

UNIVERSITAS INDONESIA

APLIKASI SECURE FILE TRANSFER PROTOKOL PADA MOBILE IPV6 DAN TUNNELING 6TO4

SKRIPSI

W A F I R 0806366472

FAKULTAS TEKNIK PROGRAM STUDI TEKNIK ELEKTRO DEPOK DESEMBER 2010

Aplikasi secure ..., W a f i r, FT UI, 2010



UNIVERSITAS INDONESIA

APLIKASI SECURE FILE TRANSFER PROTOKOL PADA MOBILE IPV6 DAN TUNNELING 6TO4

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Teknik

W A F I R 0806366472

FAKULTAS TEKNIK PROGRAM STUDI TEKNIK ELEKTRO DEPOK DESEMBER2010

Aplikasi secure ..., W a f i r, FT UI, 2010

HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya saya sendiri,

dan semua sumber baik yang dikutip maupun dirujuk

telah saya nyatakan dengan benar

Nama	: WAFIR
NPM	: 0806366472
Tanda Tangan	
Tanggal	

HALAMAN PENGESAHAN

Skripsi ini diajukan oleh : Nama : Wafir

NPM : 0806366472

Program Studi : Teknik Elektro

Judul Skripsi : Aplikasi Secure File Transfer Protokol Pada Mobile IPv6 dan Tunneling 6to4

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Teknik pada Program Studi Teknik Elektro, Fakultas Teknik, Universitas Indonesia

DEWAN PENGUJI

Pembimbing : Ir. Endang Sriningsih MT., Si

Penguji : Dr. Ir. Anak Agung Putri Ratna M.Eng

Penguji : Muhammad Salman ST., MIT

Ditetapkan di : Depok Tanggal : Januari 2011

UCAPAN TERIMA KASIH

Puji syukur saya panjatkan kepada Tuhan Yang Maha Esa, karena atas berkat dan rahmat-Nya, saya dapat menyelesaikan skripsi ini. Penulisan skripsi ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana Teknik Jurusan Teknik Elektro pada Fakultas Teknik Universitas Indonesia. Saya menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan skripsi ini, saya mengucapkan terima kasih kepada:

- Ir. A Endang Sriningsih MT.,Si., selaku dosen pembimbing yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan saya dalam penyusunan skripsi ini;
- (2) PT. Vieano Trimitra Sejahtera yang telah memberikan bantuan dukungan material dan moral; dan
- (3) SMK Telekomunikasi Tunas Harapan RSBI Kab. Semarang, yang telah menyediakan Lab. ITnya

Akhir kata, saya berharap Tuhan Yang Maha Esa berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga skripsi ini membawa manfaat bagi pengembangan ilmu

> Depok, 2010 Penulis

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Indonesia, saya yang bertanda tangan di bawah ini:

Nama	:	WAFIR
NPM	:	0806366472
Program Studi	:	Teknik Elektro
Departemen	:	Teknik Elektro
Fakultas	:	Teknik
Jenis karya	:	Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia **Hak Bebas Royalti Noneksklusif** (*Non-exclusive Royalty-Free Right*) atas karya ilmiah saya yang berjudul :

APLIKASI SECURE FILE TRANSFER PROTOKOL PADA MOBILE IPV6 DAN TUNNELING 6TO4

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Indonesia berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan memublikasikan skripsi saya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Depok Pada tanggal : Desember 2010 Yang menyatakan

(WAFIR)

APLIKASI SECURE FILE TRANSFER PROTOCOL PADA MOBILE IPv6 DAN TUNNELING 6T04 UNTUK ABSTRAK

Tujuan dari penulisan skripsi ini adalah untuk membuat jaringan Mobile Internet Protokol version 6 (MIPv6) dan Tunneling 6to4 untuk melewatkan Jaringan MIPv6 melewati Mobile Internet Protocol vesion 4 (MIPv4). Dan menerapkan aplikasi Secure File Transfer Protokol (SFTP) pada kedua konfigurasi jaringan. Proses pengambilan data menggunakan jaringan local sederhana. Dalam pengujian digunakan sebuah laptop diterapkan sebagai mobile node serta 6 unit PC sebagai router MIPv6 dan tunnel dual stack. Pengambilan data dilakukan dengan cara meng-upload dan download file yang ukurannya berbeda-beda dari mobile node ke home agent dengan perpindahan access point yang berpindah pindah selama upload-download. Parameter uji coba yang dibandingkan adalah transfer time, throughput, dan delay. Konfigurasi MIPv6 memiliki nilai transfer time, throughput, dan delay yang lebih baik dari konfigurasi MIPv6 tunneling 6to4. Untuk jaringan yang menggunakan MIPv6 secara presentasi memiliki nilai transfer time rata-rata lebih kecil pada saat upload 12% sampai 29% dan saat download 31% sampai 41% dari konfigurasi jaringan MIPv6 tunneling 6to4. Konfigorasi MIPv6 memiliki nilai throughput lebih besar pada saat upload 12% sampai 36% dan pada saat download 31% sampai 41% dibanding konfigurasi MIPv6 tunneling 6to4. Untuk delay dari konfigurasi MIPv6 lebih kecil pada saat upload 12% sampai 38% dan pada saat download 17% sampai 41% dibanding MIPv6 tunneling 6to4. Perbedaan waktu hand over dipengaruhi perangkat access point.

Kata kunci : MIPv6, SFTP, Tunneling, Transfer time, throughput, delay.

DAFTAR ISI

HALAMAN JUDUL	i	
HALAMAN PERNYATAAN ORISINALITASii		
HALAMAN PENGESAHANi		
KATA PENGANTAR	iv	
HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UN	ITUK	
KEPENTINGAN AKADEMIS	v	
ABSTRAK	vi	
ABSTRACT	vii	
DAFTAR ISI	viii	
DAFTAR GAMBAR	xi	
DAFTAR TABEL	xiii	
BAB 1 PENDAHULUAN		
1.1 Latar Belakang		
1.2 Tujuan Penulisan	2	
1.3 Batasan Masalah	2	
1.4 Metodologi Penulisan	2	
1.5 Sistematika Penulisan		
BAB 2 MOBILE IPV6 DAN FILE TRANSFER PROTOKOL (FTP)	4	
2.1 Mobile Internet Protokol	4	
2.1.1 Latar Belakang Perkembangan Mobile IP	4	
2.1.2 Protokol Mobile IPV6	6	
2.1.3 Perbandingan Mobile IPV4 dengan Mobile IPV6	9	
2.2 Interkoneksi IPV6 ke IPV4 dengan Mekanisme Automatic Tunneling		
2.2.1 Implementasi Automatic Tunneling		
2.3 Secure File Transfer Protokol (SFTP)		

BAB III PERANCANGAN TOPOLOGI JARINGAN...... 19

3.1 Perancangan Topologi Jaringan		
3.2 Kont	figurasi Jaringan Mobile IPv6 dengan Debian	. 21
3.2.1	Topologi	. 21
3.2.2	Konfigurasi Home Agent	. 21
3.2.3	Konfigurasi Foreign Agent 1	. 22
3.2.4	Konfigurasi di Foreign Agent 2	. 24
3.3 Kont	figurasi Mobile Internet Protocol versi 6 (MIPv6) Tunneling 6to4	. 27
3.3.1	Topologi	. 27
3.3.2	Konfigurasi Router IPv4	. 27
3.3.3	Konfigurasi di Home Agent	. 28
3.3.4	Konfigurasi di Foreign Agent 1	. 29
3.4 Metode Pengambilan Data		

BAB IV	ANALISA DATA	
4.1 Ana	isa Konfigurasi Jaringan	
4.1.1	Konfigurasi IPv6	
4.1.2	Konfigurasi Mobile IPv6 dengan Tunneling 6to4	
4.2 Anal	isa Performa Jaringan Pada SFTP	
4.2.1	Analisa Transfer Time	
4.2.2	Analisa Troughput	
4.2.3	Analisa <i>Delay</i>	

BAB V KESIMPULAN

..... 50

DAFTAR REFERENSI

DAFTAR LAMPIRAN

DAFTAR TABEL

Tabel 4.1	Transfer time MIPv6	. 34
Tabel 4.2	Transfer time MIPv6 tuneling 6to4	. 43
Tabel 4.5	Troughput MIPv6	. 45
Tabel 4.6	Troughput MIPv6 tunneling 6to4	. 45
Tabel 4.7	Delay pada Jaringan MIPv6	. 47
Tabel 4.8	Delay MIPv6 tunneling 6to4	. 47



DAFTAR GAMBAR

Gambar 2.1	Dari Coresponden Node ke Mobile Node	8
Gambar 2.2	Dari mobile node ke koresponden node	9
Gambar 2.3	Dari koresponden node ke mobile node	10
Gambar 2.4	interkoneksi IPv6 melewati IPv4	16
Gambar 3.1	Topologi jaringan Mobile Internet Protokol versi 6 (MIPv6)	21
Gambar 3.2	Topologi MIPv6 tunneling 6to4	27
Gambar 4.1	Tampilan Tracerouter dari Home Agent	35
Gambar 4.2	Tampilan Tracerouter dari Foreign agent	35
Gambar4.3	Tampilan aplikasi WinSCP	37
Gambar 4.4	Tampilan file yang tedapat pada MN dan HA	37
Gambar 4.5	Tampilan eksekusi upload/download	38
Gambar 4.6	Tampilan donload/upload berlangsung	38
Gambar 4.7	Tampilan pindah access point	39
Gambar 4.8	Tampilan proses koneksi acces point baru	40
Gambar 4.9	Tampilan proses hand over	40
Gambar 4.10	Tampilan proses upload/download setelah perpindahan	
	koneksi dengan Acess point baru	41
Gambar 4.11	Pengambilan nilai Transfer time	43
Gambar 4.13	Pengambilan Data Troughput	45
Gambar 4.14	Diagram Perbandingan Throughput	46
Gambar 4.15	Diagram Perbandingan Delay	48

BAB 1 PENDAHULUAN

1.1 LATAR BELAKANG

Seiring dengan berkembangnya teknologi pada zaman sekarang teknologi komunikasi berbasis *Mobile Internet Protokol* (MIP). Sehingga memungkinkan banyaknya penggunaan *Mobile Internet Protokol version 4* (MIPv4) yaitu teknologi yang digunakan saat ini akan mengalami masalah pengalamatan yang semakin terbatas. Karena keterbatasan jumlah pengalamatan pada MIPv4 ini, sehingga dibutuhkan suatu standart baru pada routing protocol yang mampu mengakomodasi jumlah pengalamatan yang lebih banyak. Berangkat dari masalah ini, *Mobile Internet Protokol version 6* (MIPv6) kemudian dikembangkan dan dijadikan standart baru yang kelak akan mengakomodasi pengalamatan yang lebih banyak.

MIPv6 adalah protocol baru yang didisain untuk menggantikan MIPv4. Alamat MIPv4 pada dasarnya menggunakan metode pengalamatan berbasis 32 bit, yang berarti mampu mengakomodasi jumlah pengalamatansampai dengan 2 pangkat 32 atau sekitar 4,294 x 10 pangkat 9. Sedangkan IPv6 menggunakan metode pengalamatan berbasis 128 bit, yang berarti mampu mengakomodasi jumlah pengalamatan sampai dengan 2 pangkat 128 atau sekitar 3,402 x 10 pangkat 38. Dengan perbandingan jumlah pengalamatan yang begitu besar inilah, yang mendasari perubahan dari MIPv4 menjadi MIPv6.

MIPv6 merupakan MIP generasi berikutnya atau disebut juga *Internet Protocol Next Generation* (IPng). MIPv6 dirancang sedemikian rupa agar memiliki kinerja yang lebih handal bila dibandingkan dengan IPv4 seperti dalam pengiriman paket, *security*, *authentication* dan QoS (*Quality Of Service*). Selain itu diharapkan MIPv6 juga mampu memberikan fitur-fitur lain yang lebih kompleks yang akan dikembangkan lagi.

Sampai saat ini, secara umum jaringan masih menggunakan IPv4 sehingga implementasi jaringan MIPv6 dilakukan secara bertahap dan diusahakan tidak akan mengganggu jaringan MIPv4 yang sudah ada saat ini. Oleh karena itu, diperlukan suatu mekanisme transisi untuk mengganti penggunaan jaringan MIPv4 menjadi jaringan MIPv6 secara keseluruhan. Untuk melakukan proses transisi dari MIPv4 ke MIPv6 maka diperlukan suatu metode yang mampu menunjang mekanisme transisi tersebut. Beberapa metode telah diteliti dan diantaranya yaitu metode *Tunneling* dan *Translation*.

Salah satu aplikasi yang akan diimplementasikan sekaligus menjadi uji coba dalam MIPv6 dan MIPv6 *tunneling 6to4* adalah *transfer file*, yang menggunakan *protocol* yang disebut Secure File Transfer Protocol (SFTP). Kebutuhan akan proses *upload* dan *download* ke suatu *Home Agent* menjadikan aplikasi ini sering dipergunakan.

1.2 TUJUAN SKRIPSI

Tujuan dari skripsi ini adalah sebagai berikut.

- 1. Merancang sebuah jaringan Mobile Internet Protocol version 6 (MIPv6)
- Membuat jaringan Tunneling 6to4 untuk melewat MIPv6 dalam jaringan IPv4 yang sudah ada saat ini.
- 3. Aplikasi Secure Transfer File Protocol (SFTP) untuk uji coba transfer time, throughput dan delay MIPv4 dan MIPv6 tunneling 6to4.

1.3 BATASAN MASALAH

Pada skripsi ini hanya akan membahas pada Mobile Internet Protokol Internet version 4 (MIPv6) dan MIPv6 dengan tunneling 6to4.

Rancangan jaringan sederhana yang akan dibangun adalah jaringan lokal yang menggunakan Router PC dengan system operasi Debian Leny 5.

Aplikasi yang akan diimlementasikan pada jaringan test bed adalah aplikasi WinSCP pada router PC dan *Mobile Node*.

1.4 METODOLOGI PENULISAN

1. Studi Literatur

Mengumpulkan dan memelajari referensi tentang jaringan MIPv6, tunneling, SFTP, Aplikasi Wireshark.

2. Perancangan Sitem

Pada skripsi ini dirancang system perangkat keras yang diperlukan dapat berjalan lancar dengan perangkat lunak yang diaplikasikan dalam perangkat keras tersebut.

3. Pembuatan Sistem

Pembuatan sistem dapat dilakukan setelah semua perangkat keras dan lunak telah terpenuhi. Permasalahan perangkat keras berupa router PC.

4. Pengambilan dan analisa data

Setelah dilakukan imlementasi, akan dicatat data-data yang berhubungan dengan *Secure File Transfer Protocol* pada masing-masing jaringan. Dan parameter yang dambil adalah *transfer time, throughput*, dan *delay*.

5. Penarikan kesimpulan

Penarikan kesimpulan dapat diambil dari topologi masing-masing jaringan yang akan dibuat.

1.5 SISTEMATIKA PENULISAN

Dalam penulisan skripsi ini akan disusun secara sistematis yang terdiri atas bagian-bagian yang saling berhubungan sehingga diharapkan akan mudah dipahami dan dapat diambil manfaatnya. Bab satu berisi latar belakang, tujuan skripsi, batasan masalah, dan sistematika penulisan. Bab dua berisi tentang pengenalan tentang *Jaringan Mobile internet Protokol*, tunneling dual stack, dan uraian pendukung jaringan. Bab tiga menjelaskan perancangan *Topologi jaringan* dan konfigurasi jaringan. Bab empat analisa data berisikan tentang pengambilan data dan analisa data masing masing jaringan untuk aplikasi *Secure File Transfer Protocol* (SFTP). Kemudian bab lima sebagai penutup berisikan beberapa kesimpulan dari skripsi yang dilakukan.

BAB 2

MOBILE IPv6 DAN SECURE FILE TRANSFER PROTOCOL (FTP)

2.1 Mobile Internet Protocol

2.1.1 Latar Belakang Perkembangan Mobile Internet Protocol

Semakin pesat perkembangan teknologi komunikasi dan informasi terutama dalam bidang komunikasi *wireless* sehingga kebutuhan akan *mobile* semakin tinggi. Sedangkan untuk setiap perpindahan jaringan terjadi perubahan nomer IP (*internet protocol*). Dengan demikian diperlukan teknologi yang bisa melakukan fungsi untuk tidak merubah alamat IP meskipun berpindah dari suatu jaringan dengan jaringan lainnya. Teknologi yang bisa melakukan fungsi ini adalah *mobile* IP. Dimana dalam teknologi ini ketika sebuah *mobile node* berpindah dari jaringan satu ke lainnya maka tidak mengalami perubahan IP. Dengan kata lain sebuah *mobile node* akan mempunyai alamat yang tetap meskipun selalu berpindah jaringan.

Semakin bertambah *mobile node* yang berbeda pada suatu jaringan computer mengakibatkan kebutuhan akan IP semakin meningkat sehingga untuk memenuhi kebutuhan ini diperlukan adanya alokasi IP yang lebih banyak. Dalam teknologi *Mobile Internet Protocol* (MIP) terdapat dua model : yaitu model IP versi 4 dan mobile IP versi 6. Mobile IP versi 6 ini mendukung adanya koneksi yang lebih cepat karena didukung adanya teknologi *tunneling*. Yaitu *biderectional tunnel* dan *route potimation*. Dengan MIP ini diharapkan akan lebih memudahkan dalam pengaturan IP.

Dalam jaringan internet yang mengunakan kabel, ditetapkan bahwa alamat IP mengidentifikasi secara unik titik node yang terhubung pada internet. Karena itu sebuah *node* harus ditempatkan pada jaringan yang diidentifikasikan oleh alamat IPnya dalam rangka untuk menerima datagram yang ditunjukkan kepadanya jika tidak, datagram yang ditunjukkan kepada *node* tidak terkirim. Untuk sebuah *node* yang merubah *point of attachment* tanpa kehilangan kemampuan untuk berkomunikasi, maka salah satu dari mekanisme berikut harus dilakukan:

- 1. *Node* harus merubah alamat IP nya ketika *node* merubah titik hubungnya ke internet.
- 2. Route tertentu *node* harus disebarkan ke seluruh penyedia internet

Kedua alternatif ini sering tidak dapat diterima , alternatif pertama tidak mungkin bagi sebuah node untuk menjaga sambungan layer transport dan layer yang lebih tinggi ketika node merubah lokasinya. Alternatif kedua jelas akan menjadi masalah karena diperlukan mekanisme baru untuk mengakomodasikan *mobilitas node* dalam internet yang memungkinkan node merubah alamat IPnya.

Fitur dari mobile IP ini diantaranya yaitu:

- 1. Support host yang berpindah-pindah
- 2. Tidak ada batasan geografis
- 3. Tidak ada modifikasi terhadap nomor IP
- 4.Keamanan jaringan terjamin

Mobile IP yang telah disetujui oleh *Internet Enginering* Steering Group (IESG) pada bulan juni 1996 dan dipublikasikan sebagai Proposed Standart pada november 1996, Proposed Standart merupakan langkah signifikan pertama pada evolusi sebuah protokol dari draft internet menjadi standart internet penuh.

MIP dibuat oleh IP Routing untuk *wireless/mobile node* yang merupakan kerjasama dengan IETF yang terbentuk pada juni 1992. Dokumen standart dari MIP mengikuti RFC antara lain:

- RFC 2002 yang merupakan protokol dari mobile itu sendiri
- RFC 2003, 2004, dan 1701, yang masing-masing mengidentifikasi tipe tunneling yang digunakan dalam MIP.
- RFC 2005, yang menjelaskan tentang applicability dari MIP
- RFC 2006 yang menjelaskan tentang mobile IP Management information Base (MIB). Mobile IP MIB adalah sekumpulan

variabel dalam sebuah *node* yang mengimplementasikan mobile IP yang dapat diperiksa atau dikonfigurasikan oleh sebuah maneger station dengan mengunakan Simple Network Management Protocol versi 2 (SNMPv2) yang terdapat dalam RFC 1905.

Alamat IP dari sebuah *node* terdiri dari dua bagian yaitu bit alamat yang lebih tinggi menentukan jaringan dimana *node* tersebut terletak dan bit yang lebih rendah menentukan nomer *node* tersebut. *Mobile IP* yang dirancang untuk mengijinkan setiap *mobile node* untuk memiliki dua alamat IP dan mengatur dengan baik proses binding antara dua alamat tersebut . Salah satu dari alamat IP adalah alamat permanen *home address* yang berada pada *home network* dan digunakan untuk komunikasi *endpoint* dan yang lainnya merupakan *temporary care of address* yang menunjukkan lokasi sekarang dimana host tersebut berada. Tujuan utama dari MIP adalah untuk membuat mobilitas dapat semakin mudah untuk dikenali ke level protokol yang lebih tinggi seperti TCP dan untuk menimimalisasi perubahan infrastruktur internet yang ada.

2.1.2. Protokol Mobile IPV6

Mobile IPV6 mendefinisikan sebuah protokol IPV6 baru berupa set pesan-pesan dan proses-proses yang digunakan untuk menetapkan hubungan antara node-node yang berdekatan. Protokol tersebut adalah *Neigbor Discovery*.

Proses-proses yang dilakukan oleh *Neighbor Discovery* adalah sebagai berikut :

- 1. *Router Discovery*, proses dimana sebuah host menelusuri routerrouter pada sebuah *link*.
- 2. *Prefix Discovery*, proses dimana host-host menelusuri *perfix-perfix netwok* untuk link-link local
- 3. Parameter Discovery, proses dimana host-host menelusuri

parameter-parameter operasi tambahan .

- 4. *Address autoconfiguration*, proses pengkonfigurasi IP address untuk interface-interface secara otomatis.
- Neighbor Unreachabilty detection, proses dimana sebuah node memastikan sebuah node memastikan bahwa layer IPv6 suatu node tetangga tidak lagi menerima paket-paket.
- 6. *Neighbor Unreachability detection*, proses dimana sebuah node memastikan bahwa sebuah address yang akan digunakan belum pernah dipakai oleh tetangga.

Mobile node selalu diharapkan untuk dialamatkan pada *home* addressnya, meskipun ia berada pada *home linknya* atau jauh dari *home*. *Home address* adalah alamat IP yang diberikan pada mobile node dengan *home subnet* perfiknya pada *home link*. Sementara mobile node berada dalam *home*, paket dialamatkan pada *home* addressnya kemudian dirutekan ke sambungan *mobile node* menggunakan mekanisme routing.

Sementara mobile node menempel pada beberapa foreign link yang jauh dari home, ia juga dapat dialamatkan pada satu atau lebih care of address yang merupakan sebuah alamat IP yang dihubungkan dengan mobile node yang mempunyai subnet perfix dari sebuah foreign link tertentu merupakan. Mobile node dapat memperoleh care of addressnya melalui mekanisme IPv6 konvensional seperti stateless atau statfull autoconfiguration. Selama mobile node tinggal pada lokasi ini paket dialamatkan pada care of address ini untuk kemudian dirutekan ke mobile node. Mobile node dapat juga menerima paket-paket dari beberapa care of address, seperti ketika ia sedang bergerak tetapi masih dapat dicapai pada *link* sebelumnya.

Hubungan antara mobile node, *home address* dan *care of address dikenal sebagai corespondent node*. Sementarta ketika jauh dari *home*, sebuah *mobile node* meregristasi *care of address* secara utama dengan *router* pada *home linknya*, permintaan kepada *router* ini berfungsi sebagai *home agent* untuk *mobile node*. Ada dua mode komunikasi yang mungkin antara mobile node dan correspondent node yaitu :

1. Mobile node ini membuat regristasi binding dengan mengirimkan pesan *binding update* ke *home agent*. *Home agent* akan membalas *mobile node* dengan mengambalikan pesan ke binding acknowledgement node. Paket-paket dari corespondent node dan bahkan tersedia jika mobil node tidak meregristasi bindingnya yang terbaru dengan coresponden node. Paket-paket dari corespondent mode dirutekan ke home agent dan kemudian disalurkan dari mobile node ke home agent (reserve tunneled) dan kemudian secara normal dari home network ke coresponden node. Pada mode ini, home agent menggunakan proxy Neighbor Discovery untuk menahan beberapa paket IPV6 yang dialamatkan ke mobile node home address pada home link. Setiap paket yang ditahan disalurkan ke mobile node home address pada home link. Setiap paket yang ditahan disalurkan ke mobile node primary care of address. Penyaluran ini menggunakan enkapsulisasi IP6.



Gambar 2.1 Dari Coresponden Node ke Mobile Node [1]

2. Mode kedua adalah route optimazation. Mode ini memerlukan dukungan mobile untuk meregristasi bindingnya pada corespondent node. Paket-paket dari corespondent node dapat dirutekan secara langsung ke care of address dari mobile node. Ketika mengirimkan sebuah paket ke beberapa tujuan coresponden node mengecek binding yang tertahan untuk masukan untuk paket destination address. Jika binding yang tertahan untuk alamat tujuan ditemukan, node menggunakan sebuah dari tipe dari IPv6 routing header yang baru untuk meroutekan paket secara langsung ke mobile node care of address membolehkan penggunaan jalur komunikasi terpendek. Ini juga menghilangkan congestion pada mobile node home agent dan home link. Sebagai tambahan dampak dari kemungkinan kegagalan dari home agent atau network pada jalur dapat dikurangi. Ketika peroutingan paket secara langsung ke mobile node, corespondent node menyesuaikan destination address pada IPv6 header ke node care of address dari mobile node. Tipe routing IP6v6 header yang baru juga ditambahkan ke paket untuk dibawa ke home address yang ditentukan, mobile node menyesuaikan source address dalam IPV6 paket header ke care of addressnya yang baru. mobile node menambahkan pilihan tujuan IPv6 home address yang baru untuk membawanya ke home address. Pencantuman home address pada paket-paket ini membuat penggunaan care of address transparan diatas network layer.



Gambar 2.2 Dari mobile node ke koresponden node [1]



Gambar 2.3 Dari koresponden node ke mobile node [1]

2.1.3 Perbandingan Mobile IPV4 dengan Mobile IPV6

Ada perbedaan utama antara mobile IPV4 dengan mobile IPV6

- Pada mobile IPV6 tidak ada keharusan untuk menggunakan router khusus sebagai *foreign agent* seperti di mobile IPv4. Mobile IPv6 beroperasi dibeberapa lokasi tanpa kebutuhan khusus dari router local.
- 2. Mobile IPv6 mendukung untuk optimasi rute yang menjadi bagian dasar protokol, daripada perluasan yang standar.
- 3. Optimasi *route mobile* IPv6 dapat beroperasi secara aman bahkan tanpa *pre-anggered security association*. Ini diharapkan bahwa *optimasi router* tersebut dapat dilakukan skala global antara seluruh *mobile node* dan *coresponden node*.
- Kebanyakan paket dikirimkan ke mobile node sementra jauh dari home dalam mobile IPv6 dikirim menggunakan IPv6 routing header daripada enkapsulasi IP, mengurangi apa yang dikerjakan dalam mobile IP44.
- 5. Mobile IPV6 dipisahkan dari beberapa bagian *link layer*, sebagaimana digunakan pada *neigbor Discovery*. Ini juga meningkatkan kekuatan dari protokol.
- 6. Penggunaan *enkapsulasi* IPv6 memindahkan kebutuhan dalam mobile IPv6 untuk mengatur *tunnel soft state*.
- 7. Mekanisme penemuan *home agent address dinamis* dalam mobile IPv6 mengembalikan balasan tunggal ke mobile node.

Pendekatan *directed broadcast* digunakan dalam IP V4 untuk mengembalikan balasan yang terpisahke setiap home.

2.2 Interkoneksi IPv6 ke IPv4 dengan Mekanisme Automatic Tunneling

IPv6 mempunyai format alamat dan *header* yang bebeda dengan IPv4 sehingga tidak bisa melakukan *interkoneksi* dengan IPv4 secara langsung karena itu diperlukan suatu mekanisme transmisi IPv6 agar paket IPv6 dapat dilewatkan pada jaringan IPv4 yang telah ada atau sebaliknya. Salah satu metode transisi adalah metode *tunneling*.

Panjang alamat IPv4 sebesar 32 bit , alamat IPv4 pada dasarnya terdiri dari dua bagian utama , yaitu identitas jaringan *(network ID)* dan identitas komputer *(host ID)* . *Netwok ID* menyatakan identitas dari jaringan dimana komputer tersebut berada, sementara *host ID* menyatakan identitas jaringan dimana komputer itu sendiri.

Pembagian kelas IPv4

Kelas A = 00000000 s/d 01111111 = 0 s/d 127

Kelas B = 10000000 s/d 10111111 = 128 s/d 191

Kelas C = 11000000 s/d 11011111 = 192 s/d 223

Kelas D = 11100000 s/d 11101111 = 224 s/d 239

Kelas E = 11110000 s/d 11111111 = 240 s/d 255

Penulisan Alamat IPv4 *Tunneling* : 202.149.240.66 dengan menggunakan contoh ini , jika administrator men-setup jaringan dengan semua komputer yang memiliki bagian nilai yang sama. <u>202.149.240</u>.xxx angka yang bergaris bawah merupakan network ID-nya, sedangkan xxx adalah host ID-nya. Kelas pada IPV4 mewakili sebuah group alamat yang dapat dikenali *software* sebagai suatu jaringan fisik. Untuk mengetahui suatu alamat IPV4 itu termasuk kelas apa, kita harus merubah alamat IPV4 tersebut ke dalam nilai biner, contoh : 10.149.240.66

<u>000</u>01010.10010101.11110000.10000010

Dengan memperhatikan 3 nilai biner pertama kita bisa mengatakan alamat IPv4 diatas adalah kelas A.

Alamat IPV6 yang mempunyai panjang 128 bit dalam hexadesimal

tentunnya sulit dihafalkan karena itu alamat numerik jarang digunakan lebih mudah DSN memegang peranan penting. Alamat IPv6 sendiri terbagi atas beberapa macam berdasarkan RFC 3513 :

- unspeccifed dengan notasi ::/128
- Loopback dengan notasi ::1/128
- Multicast dengan notasi ff00::/8
- Link local unicast dengan notasi FE80::/8
- Site local unicast dengan notasi FECO::/8
- Global unicast

Alamat yang akan digunakan untuk berkomunikasi dengan internet adalah alamat global unicast. Pembagian alokasi alamat global berdasarkan regristrasi RFC 2928 :

- IANA 2001:000::/29 sampai 2001:01F8::/29
- APNIC 2001:200::/29 sampai 2001:03F8::/29
- ARIN 2001:400::/29 sampai 2001:05F8::/29
- RIPE NCC 2001:400::/29 sampai 2001:05F8::/29

Tunneling protokol merupakan mekanisme proses enkapsulasi atau netwok protokol yang disebut *payload* protokol ke dalam *delivery* protokol yang berbeda. Tunneling IPv6 *over* IPv4 merupakan suatu proses *enkapsulasi* paket IPv6 dengan header IPv4 sehingga paket IPv6 dapat dikirim melalui jaringan IPv4 Struktur tunneling IPv6 pada IPv4 ditunjukan gambar 2.4.



Gambar 2.4 Enkapsulasi paket pada proses tunneling [2]

2.2.1 Implementasi Automatic Tunneling

Untuk membangun sebuah sistem mekanisme transisi automatic tunneling diperlukan beberapa langkah :

- 1. Desain arsitektur sistem automatic tunneling
- 2. Implementasi 2 automatic tunneling gateway / Dualstack
- 3. Pengaturan routing IPV6 pada gateway dan client tunnel
- 4. Pengujian mekanisme automatic tunneling

Sebagai contoh implementasi mekanisme tuneling outomatic

| pinguin1 |-----| CNC 1 |------| Router / Internet IPv4 |-----| CNC 2 |------| pinguin2 |

Misalkan dengan konfigurasi seperti contoh diatas dengan kondisi sebagai berikut :

- CNC 1 adalah Personal Computer (PC) dualstack dengan
 - alokasi *perfix* IPV4 adalah :198.xxx.xxx.x ::/48 alokasi *perfix* IPV6 adalah :2002:xxxx:xxx::1/48 alokasi alamat IPV6 adalah :2002:xxxx:xxx::1/48
- Pinguin 1 adalah host IPV6 dengan alokasi IPV6:2002:xxxx:xxxx::2/48
- CNC 2 adalah PC dualstack dengan alokasi IPV4 adalah:190:xx:xx:x alokasi perfix IPV6 adalah:2002:xxxx:xxxx::/48 alokasi alamat IPV6 adalah:2002:xxxx:xxxx::1/48
- Pinguin2 adalah host IPV6 dengan alokasi alamat IPV6 : 2002:xxxx:xxxx::2/48

Implementasi gateway tunneling pada CNC 1 (Dualstack) untuk host CNC 1 harus dialokasikan dengan menggunakan alamat IPV6 global supaya dapat diroutekan pada jaringan IPV6 dan internet. Format alamat IPV6 untuk gateway tunnel adalah sebagai berikut :

2002 = perfix global

xxxx:xxxx = alamat IPv4 dalam hexa (198.xxx.xxx.x = xxxx:xxxx)

Supaya operating system kita mendukung IPV6 kita perlu instalasi modul IPv6 adapun perintah untuk aktivasi modulnya adalah : #insmod ipv6

Misalkan yang terhubung ke jaringan IPV4 adalah interface eth0 dan yang terhubung ke *client tunnel* adalah eth1. Setelah itu kita perlu konfigurasi alamat IPV4 yaitu dengan perintah :

#ifconfig eth0 198.xxx.xxx.x netmask 255.2555.255.0 up
Untuk pengecekan interface kita gunakan perintah :
#ifconfig eth0

Langkah selanjutnya adalah mengaktifkan *interface* untuk *tunneling* yang digunakan untuk membangun jembatan menembus jaringan IPV4. Aktivasinya dengan mengunakan perintah :

#ifconfig sit0 up

Dengan implementasi *gateway* tunnelingnya adalah dengan format sebagai berikut : ::address IPV4 host /prefix

Dalam implementasi gateway tunnel address IPV4 pada eth0 yang digunakan adalah 198.xxx.xxx.x maka format address yang muncul pada *interface* sit0 dan CNC 1 adalah ::198.xxx.xxx.x dengan perfix 96. Biasanya alamat ini akan terkonfigurasi secara otomatis saat kita aktifasi sit0. Untuk mengkofigurasinya dapat dilakukan dengan perintah :

#ifconfig sit0 add ::198.xxx.xxx.x/196 up
Utau untuk menghapus digunakan
#ifconfig sit0 del::198.xxx.xxx.x/96
Untuk mengecek sit0 menggunakan perintah
#ifconfig sit0

Untuk selanjutnya mengkonfigurasi alamat pada interface eth1. Alamat IPV6 untuk eth1 harus menggunakan perfik ulang telah dihitung yaitu 2002:xxxx:xxxx::1/48. Perintah yang digunakan :

#config eth1 add 2002:xxxx:xxxx::1/48 up

Untuk mengecek konfigurasinya menggunakan

#ifconfig eth1

Langkah yang terakhir yang dikonfigurasi gateway tunnel CNC 1 ini adalah dengan mengkonfigurasi entri tabel routingnya yaitu semua alamat yang bertujuan ke CNC 2 atau dengan perfik 2002:xxxx:xxxx::/48 dilewatkan ke *interface tunnel* sit0, dengan perintah

#route-A inet6 add 2002:xxxx:xxxx::/48 gw

::198.xxx.xxx.x dev sit0 supaya *gateway* dapat memforward paket IPV6 maupun IPV4 maka diperlukan aktivasi IP *forward* pada sistem operasi dengan perintah

#echo"1">/proc/sys/net/ipv4/conf/all/forwarding

#echo"1">/proc/sys/net/ipv6/conf/all/forwarding

Implementasi Gateway Tunneling pada CNC 2

Gateway Tunnel CNC 2 mempunyai prinsip konfigurasiyang sama. Untuk alamat IPv6 yang dipakai 2002 : prefix global

xxxx:xxxx : Alamat IPv4 CNC 2 dalam hexa (190.xx.xx.x = xxxx:xxxx)

Supaya operating system kita mendukung IPv6 kita perlu instalasi modul IPv6 adapun perintah untuk aktivasi modulnya adalah:

insmod ipv6

Misalkan yang terhubung ke jaringan IPv4 adalah interface eth0 dan yang terhubung ke *client tunnel* adalah eth1 .Setelah itu kita perlu konfigurasi alamat IPv4 yaitu dengan perintah :

ifconfig eth0 190.xx.xx.x netmask 255.255.255.0 up Seperti halnya konfigurasi pada gateway tunnel CNC 1 maka kita perlu aktivasi interface tunnel sit0.

#ifconfig sit0 up

Apabila inet6 address sudah terkonfigurasi alamat IPv6 compatibel IPv4 maka kita tidak perlu melakukan penambahan alamat pada interface sit0.



#ifconfig sit0 up

Gambar 2.5 interkoneksi IPv6 melewati IPv4 [2]

Sebuah perusahaan memiliki topologi jaringhan seperti gambar diatas dengan kondisi sebagai berikut :

> - PC 1 adalah PC dualstack dengan alokasi IPv4 adalah 202.120.120.1 Alokasi prefix IPv6 adalah : 2002:ca78:7801::/48

Alokasi alamat IPv6 adalah : 2002:ca78:7801::1/48

- HOST 1 adalah host IPv6 dengan alokasi IPv6 2002:ca78:7801::2/48
- PC 2 adalah PC dualstack dengan alokasi IPv4 adalah 202.81.81.2 Alokasi prefix IPv6 adalah : 2002:ca51:5102::/48 Alokasi alamat IPv6 adalah : 2002:ca51:5102::1/48
- HOST 2 adalah host IPv6 dengan alokasi alamat IPv6 2002:ca51:5102::2/48
- PC 1 & PC 2 terhubung ke jaringan IPv4 menggunakan interface eth0.
- PC 1 terhubung ke HOST 1 dan PC 2 terhubung ke HOST 2 menggunakan interface eth1.

Pada PC 1 alamat IPv4 nya harus dialokasikan dengan menggunakan alamat IPv6

global supaya dapat di routekan pada jaringan IPv6, pengalokasiannya adalah sebagai berikut :

Prefix Global :	Alamat IPv4 dalam hexadesimal
2002:ca78:7801::/48	

Ket: 2002 = Prefix global

ca78:7801 = Alamat IPv4 PC 1 dalam hexa (202.120.120.1 = ca78:7801)

ifconfig eth0 202.120.120.1 netmask 255.255.255.0 up {
Pengkonfigurasian alamat IPv4 pada PC 1 }

ifconfig sit0 up { Mengaktifkan interface untuk tunneling yang
digunakan untuk membangun jembatan menembus jaringan IPv4 }

Alamat IPv4 pada eth0 yang digunakan adalah 202.120.120.1 maka format alamat yang dimunculkan pada *interface tunneling* (sit0) PC 1 adalah ::202.120.120.1 dengan prefix 96.

Alamat IPv6 pada eth1 yang digunakan adalah 2002:ca78:7801::1/48 # ifconfig eth1 add 2002:ca78:7801::1/48 up

{ Pengkonfigurasian alamat IPv6 pada interface eth1 (HOST 1) }

route -A inet6 add 2002:ca51:5102::/48 gw ::202.120.120.1 dev sit0
{Pengkonfigurasian entry table routing / semua alamat yang bertujuan ke
PC 2 akan dilewatkan ke interface tunneling (sit0)}

HOST 1 berada dibawah layanan PC 1, maka harus dibuat alamat *prefix* dari HOST 1 ini sama dengan alamat *prefix* dari PC 1. Alamat Prefixnya yaitu 2002:ca78:7801::/48, maka dapat dialokasikan alamat untuk HOST1 yaitu : 2002:ca78:7801::2/48. Semua paket yang bertujuan ke *prefix* PC 2 harus dilewatkan ke eth0 dengan perintah konfigurasi sebagai berikut :

#ifconfig eth0 add 2002:ca78:7801::2/48 up

#route -A inet6 add 2002:ca51:5102::/48 gw 2002:ca78:7801::1 dev eth0

Sama halnya juga dengan *HOST* 2 berada dibawah layanan PC 2, maka harus dibuat alamat *prefix* dari *HOST* 2 ini sama dengan alamat prefix

dari PC 2. Alamat Prefixnya yaitu 2002:ca51:5102::/48, maka dapat dialokasikan alamat untuk *HOST* 2 yaitu : 2002:ca51:5102::2/48. Semua paket yang bertujuan ke *prefix* PC 2 harus dilewatkan ke eth0 dengan perintah konfigurasi sebagai berikut:

#ifconfig eth0 add 2002:ca51:5101::2/48 up

#route -A inet6 add 2002:ca78:7801::/48 gw 2002:ca51:5102::1 dev eth0

2.3 Secure File Transfer Protokol (SFTP)

Secure Shell atau SSH adalah protokol jaringan yang memungkinkan pertukaran data melalui saluran aman antara dua perangkat jaringan. Terutama banyak digunakan pada sistem berbasis Linux dan Window untuk mengakses akun shell, SSH dirancang sebagai pengganti Telnet dan *shell remote* tak aman lainnya, yang mengirim informasi, terutama kata sandi, dalam bentuk teks sederhana yang membuatnya mudah untuk dicegat. Enkripsi yang digunakan oleh SSH menyediakan kerahasiaan dan integritas data melalui jaringan yang tidak aman seperti Internet. standar TCP port 22 telah ditetapkan untuk menghubungi server SSH.

Dalam semua versi SSH, penting untuk memverifikasi kunci publik sebelum menerimanya secara valid. Menerima seorang kunci publik *atttacker* sebagai kunci publik yang valid memiliki efek membuka password yang ditransmisikan dan memungkinkan serangan *man in-the-middle*. Dalam komputasi, *SSH File Transfer Protocol* (kadang-kadang disebut *Secure File Transfer Protocol* atau SFTP) adalah protokol jaringan yang menyediakan akses file, transfer file , dan file manajemen fungsionalitas atas setiap diandalkan data stream. Hal ini dirancang oleh *Internet Engineering Task Force* (IETF) sebagai perluasan dari *Secure Shell protocol* (SSH) versi 2.0 untuk menyediakan kemampuan transfer file aman. IETF dari Internet Draft menyatakan bahwa meskipun protokol ini dijelaskan dalam konteks protokol SSH2, protokol ini bersifat umum dan independen . Ini bisa digunakan dalam beberapa aplikasi yang berbeda, seperti transfer file aman selama *Transport Layer Security* (TLS) dan transfer informasi manajemen <u>VPN</u> aplikasi.

BAB III

PERANCANGAN TOPOLOGI JARINGAN

3.1 Perancangan Topologi Jaringan

Pada perancangan topologi jaringan *test-bed* terdiri dari 2 tipe jaringan yang diklasifikasikan menurut teknik konfigurasi pengalamatannya, yaitu jaringan Mobile IPv6, dan jaringan Mobile IPv6 *tunneling 6to4*.

Pada kedua tipe jaringan tersebut akan dilakukan pengamatan mengenai kualitas *Security File Transfer Protokol* masing-masing tipe jaringan (SFTP) dari masing-masing tipe jaringan dan memperoleh informasi mengenai kelebihan dan kekurangan dari jaringatn tersebut.

Sebagai perangkat pendukung utama dalam test bed akan digunakan PC yang bertindak sebagai router IPv4 – *Tunneling Dual Stack* sebagai solusi dari permasalahan keterbatasan router yang tidak dimiliki, karena keterbatasan biaya . Berikut ini spesifikasi perangkat keras yang diperlukan dalam jaringan test-bed :

1. Home Agent (PC Intel Atom)

- Sistem operasi Linux Debian Lenny 5 aplikasi WinSCP
- ▷ Intel Centrino CPU 2.00 GHz
- \boxtimes 1 GByte RAM
- Ethernet 10/100 Mbp
- 2. Mobile Node (laptop Axioo Neon M740SUN)
 - Sistem operasi Windows 7 aplikasi WinSCP dan WireShark
 - ▷ Intel Core 2 Duo CPU 2.00 GHz
 - ≥ 2 GByte RAM
 - \boxtimes Ethernet 10/100 Mbps1.
- 3. Foreign Agent 1 (PC Intel Atom)
 - Sistem operasi Linux Debian Lenny 5 aplikasi WinSCP
 - ▷ Intel Centrino CPU 2.00 GHz
 - ≥ 1 GByte RAM
 - Ethernet 10/100 Mbps
- 4. Foreign Agent 2 (PC Intel Atom)
 ☑ Sistem operasi Linux Debian Lenny 5 aplikasi WinSCP

- ▷ Intel Centrino CPU 2.00 GHz
- ≥ 1 GByte RAM
- Ethernet 10/100 Mbps
- 4. Router IPv4 (PC Intel Atom)
 - Sistem operasi Debian lenny 5
 - ▷ Pentium 4 CPU 2.00 GHz
 - \boxtimes 1 GByte RAM
 - \boxtimes Ethernet 10/100 Mbps4.
- 5. Dual Stack 1 (PC Intel Atom)
 - Sistem operasi Linux Debian Lenny 5 Aplikasi WinSCP
 - ▷ Intel Centrino CPU 2.00 GHz
 - ≥ 1 GByte RAM
 - Ethernet 10/100 Mbps
- 5. Dual Stack 1 (PC Intel Atom)
 - Sistem operasi Linux Debian Lenny 5 aplikasi WinSCP
 - ☑ Intel Centrino CPU 2.00 GHz
 - ≥ 1 GByte RAM
 - Ethernet 10/100 Mbps
- 6. Enam unit LAN Card (TP-Link)
 - Supports 10/100 Mbps
 - Integrated Fast Ethernet MAC
- 7. Enam unit *Wireless router* (Linksys)
 - Supports 802.11b/g/n standars
 - i Kecepatan hingga 300 Mbps
 - ⊠ Maximum 100 m indoor dan 300 m outdoor
- 8. Swich (TP-Link)
- 9. Dua Kabel UTP Cross
- 10.Delapan Kabel UTP Straigh

3.2 Konfigurasi Jaringan Mobile IPv6 dengan Debian

3.2.1. Topologi



Gambar 3.1 Topologi jaringan Mobile Internet Protokol version 6 (MIPv6)

Pada gambar 3.1 merupakan gambaran topologi jaringan Mobile IPv6, eth0 Home Agent (HA) dihubungkan dengan swich, sementara eth1 HA dihubungkan dengan accespoint HA (wireless router 0). Eth0 Foreign Agent 1 (FA1) dihubungkan dengan switch, sementara eth1 dihubungkan dengan accespoint FA1 (wireless FA1). Eth0 Foreign agent 2 (FA2) dihubungkan dengan switch, sementara eth1 FA2 dihubungkan accespoint FA2 (wireless FA2).

3.2.2. Konfigurasi Home Agent

- 1. Login sebagai root
- 2. Lalu ketikan modprobe ipv6

HomeAgent:~# modprobe ipv6

3. Setelah itu ditambahkan IP address sesuai dengan topologi

HomeAgent:~# nano /etc/network/interfaces

4. Tambahkan baris seperti berikut

auto lo

iface lo inet loopback

auto eth0

iface eth0 inet6 static

address 2001:0:0:b::1

netmask 64

auto eth1

iface eth1 inet6 static

address 2001:0:0:a::1

netmask 64

(lalu keluar dengan menekan tombol ctrl + x jawab y lalu enter) 5.

Setelah itu tambahkan proses networknya dengan perintah

HomeAgent:~# /etc/init.d/networking restart

echo 1 > /proc/sys/net/ipv6/conf/all/forwarding

route - A inet6 add 2001:0:0:c::/64 gw 2001:0:0:b::2 dev eth0

route -A inet6 add 2001:0:0:d::/64 gw 2001:0:0:b::3 dev eth0

3.2.3 Konfigurasi Foreign Agent 1

- 1. Login sebagai root
- 2. Mount Paket dari CD/DVD

apt-cdrom add

3. Install Paket ssh-server

apt-get install ssh-server

 Berikan IPv4 terlebih dahulu untuk menambah packet yang tidak ada di CD/DVD

ifconfig eth0 192.168.0.1 netmask 255.255.255.0 up

5. Koneksikan PC client ke Foreign Agent lalu berikan ip pada LAN

ip address 192.168.0.2

Tambahan packet yang belum ada di CD/DVD menggunakan WinScp

radvd

6. reboot PC Foreign Agent

Setelah proses reboot selesai lakukan konfigurasi

1. Login sebagai root

2. Lalu ketikan modprobe ipv6

ForeignAgent:~# modprobe ipv6

3. Setelah itu tambahkan IP address sesuai dengan topologi

ForeignAgent:~# nano /etc/network/interfaces

4. Tambahkan baris seperti berikut

auto lo

iface lo inet loopback

auto eth0

iface eth0 inet6 static

address 2001:0:0:b::2

netmask 64

gateway 2001:0:0:b::1

auto eth1

iface eth1 inet6 static

address 2001:0:0::c::1

netmask 64

(lalu keluar dengan menekan tombol ctrl + x jawab y lalu enter)

5. Setelah itu tambahkan proses networknya dengan perintah

ForeignAgent:~# /etc/init.d/networking restart

echo 1 > /proc/sys/net/ipv6/conf/all/forwarding

route -A inet6 add 2001:0:0:a::/64 gw 2001:0:0:b::1 dev eth0

route -A inet6 add 2001:0:0:d::/64 gw 2001:0:0:b::3 dev eth0

6. Kemudian lakukan instalasi paket radvd yang telah ditambahkan tadi

ForeignAgent:~# dpkg -i radvd.deb

7. Lalu buat konfigurasi radvd.conf di /etc dengan cara

ForeignAgent:~# nano /etc/radvd.conf

8. Lalu tambahkan baris berikut

interface eth1

{

2;

AdvSendAdvert on; prefix 2001:0:0:c::/64

9. Lalu restart radvd dengan perintah

ForeignAgent:~#/etc/init.rd/radvd restart

3.2.4 Konfigurasi di Foreign Agent 2

- 1. Login sebagai root
- 2. Mount Paket dari CD/DVD

apt-cdrom add

3. Install Paket ssh-server

apt-get install ssh-server

4. Berikan IPv4 terlebih dahulu untuk menambah packet yang tidak ada di CD/DVD

ifconfig eth0 192.168.0.1 netmask 255.255.255.0 up

5. Koneksikan PC client ke Foreign Agent 2 lalu berikan IP pada LAN

ip address 192.168.0.2

6. Tambahan packet yang belum ada di CD/DVD menggunakan WinSCP

radvd

7. reboot PC Foreign Agent 2

Setelah proses reboot selesai lakukan konfigurasi

1. Login sebagai root

2. Lalu ketikan modprobe ipv6

ForeignAgent2:~# modprobe ipv6

3. Setelah itu tambahkan IP address sesuai dengan topologi

ForeignAgen2t:~# nano /etc/network/interfaces

4. Tambahkan baris seperti berikut

auto lo

iface lo inet loopback

auto eth0

iface eth0 inet6 static

address 2001:0:0:b::3

netmask 64

gateway 2001:0:0:b::1

auto eth1

iface eth1 inet6 static
address 2001:0:0::d::1

netmask 64

(lalu keluar dengan menekan tombol ctrl + x jawab y lalu enter)
5. Setelah itu restart proses networknya dengan perintah *ForeignAgent2:~# /etc/init.d/networking restart echo 1 > /proc/sys/net/ipv6/conf/all/forwarding route -A inet6 add 2001:0:0:a::/64 gw 2001:0:0:b::1 dev eth0 route -A inet6 add 2001:0:0:c::/64 gw 2001:0:0:b::2 dev eth0*6. Kemudian lakukan instalasi paket *radvd* yang telah ditambahkan tadi *ForeignAgent2:~# dpkg -i radvd.deb*7. Lalu buat konfigurasi *radvd.conf* di */etc* dengan cara

ForeignAgen2t:~# nano /etc/radvd.conf

8. Lalu tambahkan baris berikut

interface eth1

};

```
AdvSendAdvert on;
prefix 2001:0:0:d::/64
{
};
```

9. Lalu restart radvd dengan perintah

ForeignAgent2:~#/etc/init.rd/radvd restart

Jika semua langkah di atas sudah selesai tinggal di coba melakukan test ping ke masing – masing PC

3.3 Konfigurasi Mobile Internet Protocol versi 6 (MIPv6) Tunneling 6to4

3.3.1 Topologi



Gambar 3.2 Topologi MIPv6 tunneling 6to4

Pada gambar 3.2 merupakan gambaran topologi jaringan mobileIPv6 tunelling 6to4 .Pada Eth0 router IPv4 dihubungkan dengan Eth0 dari *dualstack* 1 menggunakan kabel UTP cross, sementara Eth1 diubungkan dengan Eth0 menggunakan *dualstack* 2. Pada Et1 dualstack 1 dihubungkan dengan *acces point home* (*wireless home*). Dan pada Eth1 dualstack 2 dihubungkan dengan *foreign* (*wireless foreign*).

3.3.2 Konfigurasi Router IPv4

- 1. Login sebagai root
- 2. Setelah itu tambahkan IP address sesuai dengan topologi

nano /etc/network/interfaces

3. Tambahkan baris seperti berikut

auto lo

iface lo inet loopback

auto eth0

iface eth0 inet static

address 192.168.10.1

netmask 255.255.255.0

network 192.168.10.0

broadcast 192.168.10.255

auto eth1

iface eth1 inet static

address 192.168.100.1

netmask 255.255.255.0

network 192.168.100.0

broadcast 192.168.100.255

(lalu keluar dengan menekan tombol ctrl + x jawab y lalu enter)

4. Setelah itu restart proses networknya dengan perintah

/etc/init.d/networking restart

echo 1 > /proc/sys/net/ipv4/ip_forward

3.3.3 Konfigurasi di Home Agent

1. Login sebagai root

2. Setelah itu tambahkan IP address sesuai dengan topologi

nano /etc/network/interfaces

3. Tambahkan baris seperti berikut

auto lo

iface lo inet loopback

auto eth0

iface eth0 inet static

address 192.168.100.2

netmask 255.255.255.0

network 192.168.100.0

broadcast 192.168.100.255

gateway 192.168.100.1

auto eth1

iface eth1 inet6 static

address 2001:0:0:a::1

netmask 64

(lalu keluar dengan menekan tombol ctrl + x jawab y lalu enter)

4. Setelah itu tambahkan proses networknya dengan perintah

ifconfig sit0 add ::192.168.100.2/96 up
/etc/init.d/networking restart
echo 1 > /proc/sys/net/ipv4/ip_forward

echo 1 > /proc/sys/net/ipv6/conf/all/forwarding

route -A inet6 add 2001:0:0:b::/64 gw ::192.168.10.2 dev sit0

3.3.4 Konfigurasi di Foreign Agent 1

- 1. Login sebagai root
- 2. Mount Paket dari CD/DVD

apt-cdrom add

3. Install Paket ssh-server

apt-get install ssh-server

 Berikan IPv4 terlebih dahulu untuk menambah packet yang tidak ada di CD/DVD

ifconfig eth0 192.168.0.1 netmask 255.255.255.0 up

5. Koneksikan PC client ke Foreign Agent lalu berikan IP pada LAN

ip address 192.168.0.2

6. Tambahan packet yang belum ada di CD/DVD menggunakan WinSCP *radvd*

7. reboot PC Foreign Agent

Setelah proses reboot selesai lakukan konfigurasi

5. Login sebagai root

6. Setelah itu tambahkan IP address sesuai dengan topologi

nano /etc/network/interfaces

7. Tambahkan baris seperti berikut

auto lo

iface lo inet loopback

auto eth0

iface eth0 inet static

address 192.168.10.2

netmask 255.255.255.0

network 192.168.10.0

broadcast 192.168.10.255

gateway 192.168.10.1

auto eth1

iface eth1 inet6 static

address 2001:0:0:b::1

netmask 64

(lalu keluar dengan menekan tombol ctrl + x jawab y lalu enter)

8. Setelah itu tambahkan proses networknya dengan perintah

Ifconfig sit0 add :: 192.168.10.2/96 up

/etc/init.d/networking restart

echo 1 > /proc/sys/net/ipv4/ip_forward

echo 1 > /proc/sys/net/ipv6/conf/all/forwarding

route -A inet6 add 2001:0:0:a::/64 gw ::192.168.100.2 dev sit0

9. Kemudian lakukan instalasi paket *radvd* yang telah ditambahkan sebelumnya

dpkg –i radvd.deb

10. Lalu buat konfigurasi radvd.conf di /etc dengan cara

nano /etc/radvd.conf

11. Lalu tambahkan baris berikut

interface eth1

{

AdvSendAdvert on;

prefix 2001:0:0:b::/64

{ };

};

12. Lalu kita restart radvd dengan perintah

/etc/init.rd/radvd restart

Jika semua langkah di atas sudah selesai tinggal di coba melakukan test ping

3.4 Metode Pengambilan Data

Pengambilan data dilakukan dengan cara :

- 1. Pada konfigurasi Mobile IPV6
 - a. Melakukan upload file dalam bentuk Win Rar dari Mobile (MN) node ke home agent (HA) pada saat MN terhubung dengan *access point* HA selanjutnuya dipindah ke Acces point Foreign agent (FA).
 - b. Melakukan download file dalam bentuk Win Rar dari MN ke HA pada saat MN terhubung dengan *acces point* HA kemudian kita pindah ke *access point* FA.
- 2. Pada konfigurasi tunneling 6to4 mobile IPv6
 - a. Melakukan upload file dalam bentuk Win Rar dari MN ke HA (*dualstack 1*) pada saat MN terhubung dengan *access point* HA selanjutnya dipindah ke *access point* FA.
 - b. Melakukan download file dalam bentuk Win Rar dari MN ke HA pada saat MN terhubung dengan *access point* HA selanjutnya dipindah ke *acces point* FA (dual Stack 2).

Untuk proses pengambilan data akan dilakukan penangkapan paket-paket yang lewat dari sisi *mobil node* dengan menggunakan aplikasi *Wireshark*.

Terdapat tiga parameter yang akan diambil dalam pengambilan data yaitu *transfer time, trougput,* dan *delay.* Parameter tersebut dianggap dapat mewakili unjuk kerja dari SFTP dalam melakukan proses upload dan download data. Jika dilihat dari ketiga parameter tersebut memiliki ketrkaitan satu dengan lainnya.

File yang diupload dan download pada SFTP dibedakan menjadi dalam bermacam ukuran, yaitu 190Mbyte, 260Mbyte, dan 440Mbyte. Perbedaan ukuran file ini bertujuan untuk mengamati hubungan antara ukuran file ini bertijuan untuk mengamati hubungan antara ukuran file dengan parameter-parameter yang diuji.

Pada sekripsi ini dilakukan pengambilan data melalui IPv6 murni dan IPv6 dengan tunneling 6to4.

Penangkapan-penangkapan data melalui aplikasi *Wiresark* pada sisi mobile node . Pada proses penangkapan (*capture*) data tersebut akan

menampilkan banyak paket yang diterima, maka dari itu dilakukan proses filtering, sehingga yang akan terlihat hanya paket-paket secure file transfer protocol (SFTP) saja. Kemudian dapat dilihat pada *summary* dan mendapat parameter-parameter yang diinginkan, yaitu *transfer time, trougput* dan *delay*.



BAB IV ANALISA DATA

4.1 Analisa Konfigurasi Jaringan

Pengambilan data dilakukan dengan menggunakan jaringan sederhana pada setiap konfigurasi jaringan yang diujikan. Secara keseluruhan untuk topologi yang digunakan sebuah laptop sebagai host/node mobile dan enam buah PC router sebagai *home agent-foreign agent* serta *router tunneling 6 to 4*. Masing-masing laptop di tambahkan aplikasi WinSCP dan Wireshark.

Pada penelitian ini dilakukan 2 percobaan yaitu menggunakan jaringan mobile IPv6 dan Mobile Ipv6 dengan tunneling dual stack .

4.1.1 Konfigurasi IPv6

Pada konfigurasi jaringan mobile IPv6 seluruh perangkat baik router PC maupun mobile node diberikan alamat IPv6. Dalam konfigurasi routing yang digunakan adalah static routing, dikarenakan semua konfigurasi menggunakan alamat IPv6 maka proses transmisi data yang terjadi pada saat melalui router hanya routing dan forwarding paket seperti jaringan pada umumnya . Untuk konfigurasi lengkapnya dapat dilihat pada bab 3.

Hasil traceroute konfigurasi MIPv6 ditunjukkan pada Gambar 4.1 dari home agent ke foreign agent, dan untuk sebaliknya dari foreign agent ke home agent ditunjukkan pada Gambar 4.2 .Pada hasil tracerouter tersebut terlihat bahwa seluruh hop yang dilewati merupakan alamat IPv6.



Gambar 4.2 Tampilan Tracerouter dari Foreign agent

4.1.2 Konfigurasi Mobile IPv6 dengan Tunneling 6to4

Pada konfigurasi jaringan tunnelling 6to4 juga memiliki topologi sama dengan mobile IPv6 sehingga tidak ada perbedaan jumlah hop. Pada konfigurasi ini menggunakan mekanisme tunnelling 6to4 sehingga router perlu ditambahkan interface tunnel yang di-setting menjadi mode 6to4.

Peran router pada konfigurasi ini selain dirouting, juga berfungsi untuk proses enkapsulasi dan dekapsulasi paket. Konsep tunneling adalah melewatkan IPv6 melalui jaringan IPv4. Akan tetapi alamat dari IPv4 diubah dahulu sesuai format alamat dari tunneling 6to4. Proses enkapsulasi ini berlangsung pada waktu melewatkan IPv6, melalui jaringan IPv4, dan setelah tiba di sisi seberang akan didekapsulasi agar tersisa alamat IPv6 saja sesuai dengan awal. Untuk konfigurasi lengkap jaringan tunneling 6to4 dapat dilihat pada bab 3.

Hasil *traceroute* dilakukan dari sisi host ke host melalui tunnel. Dapat dilihat pada hasil *traceroute* bahwa pada hop kedua terdapat alamat IPv6. Alamat IPv6 pada hop kedua tersebut menunjukkan alamat *identifier* dari tunneling 6to4 sehingga dipastikan bahwa data yang dikirim dari host ke host melalui mekanisme tunneling 6to4 terlebih dahulu.

4.2 Analisa Performa Jaringan Pada SFTP

Secure File Transfer Protocol (SFTP) merupakan aplikasi yang digunakan untuk memindahkan suatu file data dari host/mobile node . SFTP merupakan suatu jenis protokol yang bekerja dengan memanfaatkan protokol TCP/IP yang pada umumnya menggunakan port 22.

SFTP dibedakan jadi 2, yaitu proses upload dan download yang dilakukan mobile node.

Pada skripsi ini digunakan aplikasi WinSCP Pada semua PC dan mobile node. MIPv6 murni dan jaringan *tunneling* 6to4 akan diimplementasikan penggunaan aplikasi tersebut. Secara otomatis WinSCP dapat mendeteksi *address* yang ada pada masing-masing jaringan tersebut. Gambar 4.3 adalah aplikasi WinSCP.

Recycle Bin	near Films PDFCreator				
Adobe Reader 9	PrimoPDF - Drop Files	WinSCP Login		?	
Join Air		Session 	Session Host name: 2001;0:0:b::1 User name: Passw root eeee	Pot number:	
ebay	Support		Private key file: Protocol Ele protocol: SFTP • Ø/	4low SCP falback	
Foxit Reader	Kinamp (Advanced options About Langu	Jages Login	Select color Save Close	
WinSCP- Shortcut					
Mozilla Freitex					
3				· W. ACD	← 隆 健 🚽 🌵 3:38 AM 12/12/2010

Gambar4.3 Tampilan aplikasi WinSCP

Setelah mobile node terhubung dengan accespoint home agent, maka selanjutnya akan diminta nomer IP Eth 0, user name dan password home agent, setelah dimasukkan, pilih login. Apabila alamat yang dituju benar maka akan ditampilkan Gambar 4.4.

	-			1		
Recycle Bin PDFCreator	y root - root@2001:0:0:b::1	- WinSCP				
	Local Mark Files Comm	nands Session Options Rem	ote Help - ∀ ¢ ⊗ ?	Default - 🕼	1.	
	My documents	• 🗃 🕼 • 🔿 • 🕅 1	1 🚮 🖗 📴	i 🔐 root	• 🗃 🖕 • 🔿 • 👔 🕅	10 B
Adobe PrimoPDF -	C:\Users\Zuha\Documents			/root		
Reader 9 Drop Files	Name Êxt	Size Type	Changed A	Name Êxt	Size Changed Ri	ghts C
See See asy Sepont asy Sepont courtecter Vinamp	Fax Fax Fax My Music My Pictures My Videos My Videos Soned Documents Gestrop.ini MA Card docx Gyshdocx MysCP.ine WinSCP.ini	Parent directory Fiel folder Fiel folder Fiel folder Fiel folder Fiel folder Fiel folder 2001 (Starsoft Offic 8,888 Microsoft Offic 6,365,696 Application 579 Configuration	12/12/2010 r 12/9/2010 r 12/6/2010 s 12/6/2010 s 12/6/2010 s 12/9/2010 r 12/12/2010 s 12/12/2010 s 12/12/2010 s 12/9/2010 s 12/9/2010 s 12/9/2010 s	Si aptitude 	12/12/2010 85 rv 12/12/2010 85 rv 12/12/2010 85 rv 12/12/2010 85 rv 412 12/15/2004 25 rv 140 11/19/2007 9.5 rv	<u>197973 (</u> X () () ()
Wasep- Startes	 ✓ Ø B of 7,091 KB in 0 of 12 I p# F2 Rename F4 Edit 	배 태출 F5 Copy : 🗟 F6 Move 💣	F7 Create Directory	・ DBdf 552 Bin 0 of 4 X F8 Delete 雪 F9 Properti	™ ≝ jī, F10 Quit A SFTP-3 @	0.00.39
		1				▲ 🖹 🛱 📲 🕂 3:40 AM 12/12/2010

Gambar 4.4 Tampilan file yang tedapat pada MN dan HA

Selanjutnya proses apload maupun download dengan menekan file yang akan dipindahkan ,baik dari mobile node maupun dari home agent dengan menekan menu copy seperti Gambar 4.5.



Gambar 4.5 tampilan eksekusi upload/download

Home Insert Page Layout	References Mailings Review	View	0		X
Calibri (Body) + 11 + 1 B Z U - date X, x ² + 2 B Z V - Ax + (A × A × A × A × A × A × A × A × A × A	CA - root@2001.00bet - WinSCP Local Mark Files Commands Sess @ @ @ @ @ @ @ @ @ @ @ @ @ @ @	ion Options Remote Help	Cot Cot And Co		Tr
Recti and discussion of the second se	bocuments and Settin bocuments and Settin boccuments and Settin boccuments and Settin boccuments boccume	Fie: C:_\Access enus\Access e	Append: 0.0008 1.455 KB/s Speed (VE/s) Unimited v	0 11/19/2007 9:5 nor-r	
ge: 2 of 2 Words: 0 🧭	Stattosec.bat 22 © config.sys 11 © hiberfil.sys 1,608,388 INSTALLLOG 636 ® NetworkCfg.xml 1,103 © pagefile.sys 2,144,518 m 0B of 3.579 MB in 0 of 21	4 Windows Batc 6/10/2009 e 0 System file 6/10/2009 e System file 12/11/2010 e 7 Erct Document 12/11/2010 e 3 XML Document 12/11/2010 e System file 12/11/2010 e	4m 0 8 of 552 B in 0 of 4		_
ozilis celor	🛿 🧬 F2 Rename 📝 F4 Edit 🗳 F5 Cop	ay 🏦 F6 Move 🍟 F7 Create Directory	r 🗙 F8 Delete 💣 F9 Properties 🦹	F10 Quit A SFTP-3 🥥 0:01:5	6

Proses upload dan download berlanjut seperti gambar 4.6

Gambar 4.6 Tampilan download/upload berlangsung

Proses selanjutnya mobil node pindah access point ke foreign agent dan diamati dan ditunggu prosesnya maka akan terjadi proses penghentian upload / download setelah tersambung lagi dan terkoneksi dengan foreign agent maka download /upload akan berlanjut.

Proses dari berhentinya upload/download sampai berlanjutnya upload/download kembali, biasa disebut *Hand Over*. Waktu yang dibutuhkan untuk *hand over* berlangsung sekitar 10-15 detik, sebagai referensi dalam skripsi ini apabila mengunakan access point pada sisi *access point home agent* (AH) 300Mbs dan sisi access point foreign agaent (AH) 54 Mbps maka akan mengasilkan *hand over* pada sisi AH lebih cepat sekitar 3detik dibanding pada sisi AF.

Side Displation Side Displation Side Displation Side Displation Side Displation Side Side Side Side <th>cle Bin PDFCreator</th> <th>C:\ - root@2001:0:0:b::1 - W</th> <th>/inSCP</th> <th></th> <th></th> <th>- • ×</th>	cle Bin PDFCreator	C:\ - root@2001:0:0:b::1 - W	/inSCP			- • ×
Note Note Note Note Note Note Note Note Note Note Note Note Note Note Note Note Note Note Note Note Note Note Note Note Note <t< td=""><td></td><td>Local Mark Files Comman</td><td>nds Session Options Re</td><td>mote Help</td><td></td><td></td></t<>		Local Mark Files Comman	nds Session Options Re	mote Help		
And And And And And Name C Local Disk C Local Disk C Local Disk And Name C Local Disk C Local Disk Name Name C Local Disk Name C Local Disk Name C Local Disk Name C Local Disk Name Data Data Data Documents and Setting Program Dist Progra				Default	. 16.	
Bible Clocal Dia Content of the state of the sta						
BBCP Primosibilities BBCP Primosibilities SBCP System Volume Infort SBCP Primosibilities SBCP System Volume Infort SBCP System Volume Infort System Volume Infort System Relia Unicetal System Relia SBCP System Relia SBCP <		C: Local Disk	• 🔄 🔶 • 🖓 • 🖾	in in in is in root	• • • • • • • •	
Size Changed Name Ext Size Type Changed Name Ext Size Changed Name Ext Name Ext Name Ext Size Changed Name Ext Name Ext Name Ext Name Ext Name Ext Name Ext Name Ext <t< td=""><td>dobe PrimoPDF - ader 9 Drop Files</td><td>UN C</td><td>1000</td><td>Troot</td><td></td><td></td></t<>	dobe PrimoPDF - ader 9 Drop Files	UN C	1000	Troot		
Sitespide File folder 12/2/2010 aptitude Data 12/25 File folder 12/2/2010 aptitude Data 256 File folder 0.0518 Time elapsed: 0.0103 Data 256 Bat 256 not 4 Windows 100 State aptitude Data 256 Bat 256 not 4 State 256 not 4 NULL m2 Windows 34 Windows 8 4 Windows 8 Aptitude <td></td> <td>Name Ext</td> <td>Size Type</td> <td>Changed A Name Ext</td> <td>Size Changed</td> <td>Rights C</td>		Name Ext	Size Type	Changed A Name Ext	Size Changed	Rights C
Image: Second state in the		SRecycle.Bin	File folder	12/6/2010 s 🛀	12/12/2010 8	:5 rwxr-xr-x r
Starting Data 2,35 Distributed	C BI	Data 1,22G	File folder	12/12/2010	12/12/2010 8	:5 rwx r
and Windys Bay Decements and Settin. MOC define Program Files Program Data By Program Data Program Data Pr		Data 2,50	File tolder	12/12/2010 11 debtads	8 8 2 12/12/2010	S PWXF-XF-X
MSOCache Pertogs Program Files Program Files Pr	n Aur WinZip	Documents and Settin	Love Copying		0 11/19/2007	5 pw-rr
Stopping		MSOCache			Cancel	
Suppart Documental Program Files Program Data File: C:Data 550M Enterptee WW.EnterWW cab Farget: Once [mained: System Volume Inform. Windows System Volume Inform. The left: 0.05 16 The sloped: 0.0103 Windows Windows System file: 0.10200 - ± Unimed Windows Windows Statutoeec.bat 24 Windows Statutoeec.bat 24/Windows Windows 1.606,288 System file: 12/11/2010 ± Image:		PerfLogs				
Supparie By Supparie By Supparie By Supparie By Supparie System Volume Infor Universe System Volu	W	Program Files			Minimize	
Big Discussion Percovery Image: /root/ Once femined: Disk-up and VPN Number Signification Signification Signification Signification Signification Disk-up and VPN Number Signification Signification Signification Signification Signification Disk-up and VPN Number Signification Signification Signification Signification Signification Null m2 See		🎉 ProgramData	File: C:\Da	ta 550M\Enterprise.WW\EnterWW.cab		INO INTERNET ACCESS
Sophitesi Sophitesi	Bay Support	Accovery	larget: /root/		Once tinished:	Dial-up and VPN
wrapped urupped Urupped 00516 Time elapsed: 00103 Windows Urussel 00516 Time elapsed: 00103 00103 Windows Urussel 01505 KB/s Speed (KBA): Urumed - Windows Secular Windows 3utoexec.bat 24 Windows Elastic 6/0/2000 elastic 0 Secular Windows 3utoexec.bat 24 Windows Elastic 6/0/2000 elastic 0 NSTALLLOG 636 Test Document 12/11/2010 elastic 103 XML Document 12/11/2010 elastic 1103 XML Document 12/11/2010 elastic 11155 KB/s 11155 KB/s NSTALLLOG 636 Test Document 12/11/2010 elastic million 1103 XML Document 12/11/2010 elastic 11155 KB/s 11155 KB/s 11155 KB/s NSTALLLOG 636 Test Document 12/11/2010 elastic million million 11155 KB/s 11155 KB/s 11155 KB/s Note million million million million million 11155 KB/s 11155 KB	Discument	System Volume Infor			Stay idie 💌	
Realer Winauge Realer Winauge Realer Windows Realer Windows		unzipped	Time left:	0:05:16 Time elapsed: 0:01:03		NULL
Reade Windows Windows Windows Windows Windows Windows Status 600 / 000 ···· 600 / 000 ···· Reade Windows Windows 600 / 000 ···· 600 / 000 ···· 600 / 000 ···· Windows Windows System file 600 / 000 ···· <td></td> <td>UserData</td> <td>Bytes transferred:</td> <td>91,/50 KiB Speed: 1,516 KiB/s</td> <td>Speed (KiB/s):</td> <td>m2</td>		UserData	Bytes transferred:	91,/50 KiB Speed: 1,516 KiB/s	Speed (KiB/s):	m2
Reader Winaup Image: Autoore Connection Virreles: Network Connection Image: Autoore Connection Image: Autoore Connection Virreles: Network Connection Image: Autoore Connection Image: Autoore Connection Home: Agent Image: Autoore Connection Image: Autoore Connection Image: Autoore Connection Image: Autoore Connection Image: Autoore Connection Image: Autoore Connection Image: Autoore Connection Image: Autoore Connection Image: Autoore Connection Image: Autoore Connection Image: Autoore Connection Image: Autoore Connection Image: Autoore Connection Image: Autoore Connection Image: Autoore Connection Image: Autoore Connection Image: Autoore Connection Image: Autoore Connection Image: Autoore Connection Image: Autoore Connection Image: Autoore Connection Image: A		Windows			Unimited •	100 V 100 V
Sep. System file 6/10/2009 + Home Agent Connected InstalLLOG 635 Tst Document 12/11/2010 + Tst St Home Agent Tst St Home Agent Sep. InstalLLOG 635 Tst Document 12/11/2010 + Tst St Home Agent Tst	Reader Winamp	autoexec.bat	24 Windows Batc.	6/10/2009 e		Wireless Network Connection
Sopplete 1608,388 System file 12/11/2010 ITNS-15 Sopplete TELSA, HOTSPOT TELSA, HOTSPOT TELSA, HOTSPOT Bed 3573 MB n 0 of 21 0B of 552 B n 0 of 4 Image: First Beam First Beam First Beam First Create Directory First Belete FIP Properties FIP O Cutt		Config.sys	10 System file	6/10/2009 a		Home_Agent Connected
Sep- rites Sep- Result LOG Bis Text Document 12/11/2010.		🗟 hiberfil.sys 1,	608,388 System file	12/11/2010 e		ITNC 15
Metwork(fgsml 1.03 XML Document 12/11/2010 ¢ Image: Constraint of the state of t		INSTALL.LOG	636 Text Document	12/11/2010 a		11140-10
depugnicus 2/14/38 System file 1/2/11/2010 Image: Constraint of the state	2	MetworkCfg.xml	1,103 XML Document	: 12/11/2010 г		TELSA_HOTSPOT
Image: Contract of the second seco	SCP -	Dagefile.sys 2,	144,518 System file	12/11/2010 z		Foreign Agent
UB of 35/39 MB IN UF 21 UB of 35/39 MB IN UF 21 UB of 35/39 MB IN UF 21 Information sent over this network might be visible to others. If p F2 Rename F2 Rename F3 ESC Opy F6 Move F7 Create Directory K F8 Delete F9 Properties In F10 Quit If p F2 Rename F8 Eds F5 Copy F6 Move F7 Create Directory K F8 Delete F9 Properties In F10 Quit Information sent over this network might be visible to others.	iteut					
Connect automatically Connect automatic		U B of 3,5/9 MiB in 0 of 21	200 200	0 B of 552 B in 0 of 4		Information sent over this network might be visible to others
SFTP-3 Connect automatically Conne		FZ Rename Eg F4 Edit H	B F5 Copy IB F6 Move	r F7 Create Directory 🗙 F8 Delete 📺 🛙	-9 Properties IL F10 Quit	
					🔒 SFTP-3	Connect automatically
	zilla					

Gambar 4.7 Tampilan pindah accesspoint

le Bin P	DFCreator	C:\ - root@2001:0:0:b::1	- WinSCP					- 🗆 🗙	
		Local Mark Files Com	mands Session Opt	ions Remote Help					
		🚺 \land 🔠 🕲 • 🔛 📽	📀 🔤 🧬 😤		O Default	- 1 🌆 -			
∼.		a. C: Local Disk	• 😋 🖛 • 🔿	- 🗈 🖬 🚮 👩 隆	🔒 root	• 😁 🕴	⊨ • ⇒ • ≦	🗀 🖪 🔂 🖻	2
ibe P	rimoPDF -	C:V			/root				
ler9 D	Drop Files	Name Êxt	Size Type	Changed	Name Êxt	Size	Changed	Rights	C
		SRecycle.Bin	File fol	lder 12/6/2010	s 🔒		12/12/2010 8:5	rwxr-xr-x	10
2		퉬 Data 1,22G	File fol	lder 12/12/2010	🌗 .aptitude		12/12/2010 8:5	rwx	r -
	7 3.	bata 2,5G	File fol	der 12/12/2010	debtags	9 9 1	12/12/2010 8:5	rwxr-xr-x	an a
Air	WinZip	Data 550M	19% Cop	ying		8 25 2	12/15/2004 2:5	rw-rr	r.
		Documents and Settin.				Cancel	11/19/2007 9:5	rw-rr	r
		Defl ess				Cancer			
7		Program Files				Minimize			
U		ProgramData	File:	C:\Data 550M\Enterprise.V	/W\EnterWW.cab				
v	Support	Recovery	Target:	/root/		Once finished:			
í (Document	System Volume Infor		and the second se		Stay idle 💌			
		🔒 unzipped	Time left	1: 0.06:22 Time	elapsed: 0:01:20				
		🔒 UserData	Bytes tra	ansferred: 111 MiB Spec	ed: 1,197 KiB/s	Speed (KiB/s):			
		Users			and the second second	Unlimited 👻			
adar	Winsma	Windows							
and the	unitarily	autoexec.bat	24 Windo	ws Batc 6/10/2009 a	E				
	1	lo contig.sys	10 System	n file 6/10/2009 a	2				
			1,008,388 System	12/11/2010 i					
4		NetworkCfg.xml	1 103 XMLD	locument 12/11/2010					
		a nagefile.svs	2 144 518 System	n file 12/11/2010		Connect	t to a Network		
(P -		(120 81	
		0 B of 3 579 MiB in 0 of 21			0 B of 552 B in 0 of 4	Connec	ting to Foreigr	_Agent	
		E P Rename 7 F4 Edi	ES F5 Copy	Move 🔿 F7 Create Directo	rv × F8 Delete MF F9	Prope			
		i i i i i i i i i i i i i i i i i i i			.,				
								-	
lla	1								-
OX XO									



on porcleator	20% Copying - root@2001:	U:U:b::1 - WINSCP						
	Local Mark Files Comma	nds Session Options Rem	ote Help		-			
		• 🖼 📽 🍇 🐘 🖽		Default • 0	9 •			
	C: Local Disk	• 🔄 🗣 • 🔿 • 🖾	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	📕 root	- 🔄 🗧	• • = • 🔳 🖬	2 🗗 🖾	18
e PrimoPDF - Drop Filor	C:X		/	toot				
ro oropines	Name Ext	Size Type	Changed 4	Name Ext	Size	Changed	Rights	C
	SRecycle.Bin	File folder	12/6/2010 s	5		12/12/2010 8:5	rwxr-xr-x	ar in
	Data 1,22G	File folder	12/12/2010	aptitude		12/12/2010 8:5	rwx	
	Data 2,5G	File folder	12/12/2010	debtags	52	12/12/2010 8:5	rwxr-xr-x	P.
ir WinZip	Bata SSUM	20% Copying		8	2	12/15/2004 2:5	rw-rr	
	MSOCache		-			11/19/2007 9:5	tw-tf	
	Perfloor	Confirm						
7	Program Files							
	ProgramData	Host is	not communicating for m	nore than 15 seconds. Still wait	Jing			
Support	Recovery	Wamin	g: Aborting this operation	n will close connection!				
Document	System Volume Infor							
	unzipped		Abort	Heip				
	UserData		112 1910 - 30000.	421 IVD/8 000001				
	Users			Unlimite	ed 👻			
	Windows							
ader Winamp	autoexec.bat	24 Windows Batc	6/10/2009 ē					
	🖄 config.sys	10 System file	6/10/2009 a					
	hiberfil.sys 1	608,388 System file	12/11/2010 e					
	INSTALLLOG	636 Text Document	12/11/2010 ē					
	NetworkCfg.xml	1,103 XML Document	12/11/2010 e					
p	pagefile.sys 2	144,518 System file	12/11/2010 e					
ut			+		m			•
	0 B of 3,579 MiB in 0 of 21		0	B of 552 B in 0 of 4				
	🕴 🖗 F2 Rename 📝 F4 Edit 🗎	🚡 F5 Copy 🕼 F6 Move 📸	F7 Create Directory	🗙 F8 Delete 🕋 F9 Proper	rties 🧵 F10 Q	juit		
					A	SFTP-3	0:03:28	
	<u> </u>					-		<u> </u>
6								

Gambar 4.9 tampilan proses hand over



Gambar 4.10 Tampilan proses upload/download setelah perpindahan koneksi dengan Acess point baru

Proses download dan upload file dari dilakukan oleh mobile node ke Home Agent dengan ukuran yang berbeda-beda ukuran file : 190 MB, 260 MB, dan 440 MB. Semua file dibuat sama dalam bentuk ekstensi.rar untuk menghindari pengaruh perbedaan file pada performa SFTP.

Terdapat tiga parameter yang diambil dalam pengambilan data, yaitu *transfer time, troughput,* dan *delay*. Parameter tersebut danggap mewakili unjuk kerja dari SFTP dalam melakukan proses down load dan download data. Jika dilihat dari ketiga parameter tersebut memiliki keterkaitan satu dengan yang lain. Untuk analisa data tentang ketiga parameter tersebut dijelaskan pada bagian berikut ini.

4.2.1 Analisa Transfer Time

Transfer Time adalah jumlah waktu yang dibutuhkan untuk mengirim seluruh paket dari server ke client yang dinyatakan dalam second. Pengambilan parameter tranfertime dilakukandengan cara down load dan upload data dari server ke client. Kemudian disaat yang bersamaan pada sisi client atau mobile node melakukan capture data atau penangkapan paket-paket yang masuk melalui interface ethernet dengan aplikasi wireshark. Berhubung paket-paket yang masuk pada ethernet tersebut bukan hanya paket SFTP ,maka dari itu dilakukan filtering terlebih dahulu pada hasil summary capture wiresark sehingga hanya muncul bagian-bagian yang diinginkan saja .Pengambilan nilai transfer time pada summary Wireshark pada Gambar 4.11. Pengambilan nilai *transfer time* pada *summary* Wireshark dapat dilihat padapat dilihat pada gambar diatas data yang digunakan hanya data paket yang didisplayed bukan pada captured. Data transfer time diambil dari perbedaan rentang waktu antara paket pertama sampai dengan paket terakhir. Dari tabel 3 dapat dilihat pada waktu ukuran file semakin besar kapasitas data maka semakin besar pula nilai dari transfertime.



Gambar 4.11 Pengambilan nilai Transfer time

Dapat dilihat Gambar 4.6 data yang digunakan hanya data paket yang ada pada displayed bukan pada captured. Data transfer time diambil dari perbedaan rentang waktu antara paket pertama sampai dengan paket terakhir. Dari pengujian data yang dilakukan sebanyak 5 kali pada masing-masing file dan masing-masing konfigurasi didapat rata-rata dari nilai transfer time seperti pada Tabel 4.1.

Diagram perbandingan nilai throughput ada pada Gambar 4,14.

File (Mb)	Upload (second)	Download (second)
190	180,379	116,891
260	221,416	129,261
440	331,136	225,583

Tabel 4.1 Transfer time rata-rata MIPv6

Tabel 4.2 Transfer time MIPv6 tuneling 6to4

File (Mb)	Upload (second)	Download (second)
190	202,467	165,238
260	283,252	170,346
440	427,990	300,774

Berdasarkan hasil rata rata pada Tabel 4.1 dan Tabel 4.2, didapatkan bahwa terdapat pengaruh kapasitas data terhadap nilai transfer time . Semakin besar kapasitas data maka semakin besar pula nilai dari transfer time.



Diagram perbandingan nilai transfer time dapat dilihat pada Gambar 4.12.

Gambar 4.12 Diagram Perbandingan Transfer

Untuk menghitung perbandingan transfer time saat upload dan download jaringan yang menggunakan konfigurasi MIPv6 dengan konfigurasi jaringan MIPv6 tunneling 6to4 dalam prosentase ditunjukkan rumus :

Keterangan :

%PTtU = Prosentasi Perbandingan Transfer time saat Upload NTtU = Nilai Transfer time saat Upload

 $\% \text{ PTtD } = \frac{\text{NTtD MIPv6 tunnel } 6to4 - \text{NTtD MIPv6}}{\text{NTtD } = \frac{100\%}{\text{NTtD MIPv6}}$

4.2

41

Keterangan :

%PTtD = Prosentasi Perbandingan Transfer time saat Download NTtD = Nilai Transfer time saat Download

Dari hasil perhitungan maka akan didapatkan nilai perbandingan transfer time saat upload pada konfigurasi MIPv6 lebih kecil antara 12% sampai 29% dibanding konfigurasi MIPv6 tunneling 6to4. Dan perbandingan transfer time saat download pada konfigurasi MIPv6 lebih kecil 31% sampai 41% dibanding konfigurasi MIPv6 tunneling 6to4. Hal ini dikarenakan adanya proses enkapsulasi dan dekapsulasi paket pada mekanisme tunneling. Selain routing, proses enkapsulasi dan dekapsulasi juga dapat menambah waktu transfer time suatu file.

4.2.2 Analisa Throughput

Troughput merupakan kecepatan transfer data rata-rata dari suksesnya paket yang dikirim per detiknya, pada umumnya menggunakan satuan bit per second (bps). Pengambilan parameter transfer time dilakukan dengan cara download atau upload file dari mobile ke home dengan berpindah-pindah access point. Kemudian saat bersamaan pada sisi mobile node melakukan capture data atau penangkapan paket - paket yang masuk melalui *interface ethernet* dengan aplikasi Wireshark. Berhubung paket – paket yang masuk pada *ethernet* tersebut

bukan hanya paket SFTP, maka dari itu dilakukan *filtering* terlebih dahulu pada hasil *capture* Wireshark sehingga hanya muncul paket - paket SFTP saja.

Capturing 1	from Microsoft - Wireshark	
Eile Edit V	∉iew <u>G</u> o <u>C</u> apture Analyze <u>S</u> tatistics Telephony <u></u> <u>T</u> ools <u>H</u> elp	
	😫 🕍 🖮 🖾 🗶 😂 占 🌞 🌳 🜍 😨 🛓 🗐 🗐 (भ् ६ ०. 🖂 । 🖉 🖉 🎭 💥 । 🔀
Filter: ssh	Wireshark: Summary	ar Apply
No. Tir	El.	
211047 11	News Citizen 7, het Are Debit and Translation bed WWW 00004	which response parter lengtho
211049 11	Name: C:\Osers\Zunai\AppData\Locai\Temp\wiresnarkXXXAa00024	voted response packet len=140
211050 11	Length: 215008308 bytes	voted response packet len-140
211052 11	Format: Wireshark/tcpdump/ libpcap	voted response packet len=1440
211053 11	Encapsulation: Ethernet	voted response packet len-1440
211055 11	Packet size limit: 65535 bytes	vpted response packet len=1440
211056 11		vpted response packet len=1440
211058 11	Time	vpted response packet len=1440
211059 11	First packet: 2010-12-13 00:34:29	vpted response packet len-1440
211060 11	Last packet: 2010-12-13 00:38:47	ypted request packet len=68
211061 11	Flansed: 00-04-17	ypted response packet len=1440
211062 11		ypted response packet len=1440
211064 11	Conturn	ypted response packet len=1440
211065 11	capture	ypted response packet len=1440
211067 11	Interface: Microsoft	ypted response packet len=1440
211068 11	Dropped packets: unknown	ypted response packet len=1440
211070 11	Capture filter: none	ypted response packet len-1440
211071 11		ypted response packet len=1440
211073 11	Display	ypted response packet len=1440
211074 11	Display filter: ssh	ypted response packet len=444
211076 11	Ignored packets: 0	ypted response packet len=84
211077 11		ypted response packet len=84
211079 11	Traffic Captured Displayed Marked	ypted request packet len=68
211080 11	Packets 211229 145515 0	ypted response packet len=84
211081 11	Between Gest and last and last 257 207 and 116 001 and	ypted request packet len=68
211082 11	Between first and last packet 257.797 sec 110.891 sec	ypted response packet len=68
211112 11	Avg. packets/sec 819.362 1244.873	ypted request packet len=36
	Avg. packet size 1002.176 bytes 1421.190 bytes	
Frame s Ftherne	Bytes 211688620 206804528	bick 63:eb:8f (00:24:01:63:eb:8f)
E Interne	Avg. bytes/sec 821144.519 1769201.401	Dst: 2001:0:0:b::1 (2001:0:0:b::1)
🖲 Transmi	Avg. MBit/sec 6.569 14.154	ssh (22), Seq: 1, Ack: 1, Len: 84
0000 00		p1*.
0010 00	<u>Elose</u>	
0030 00 0		.wD\$
0040 1e a	ad 50 18 00 42 6b 35 00 00 af d7 3f e7 f7 dcPBk5	····?···
Microsoft:	capture in progress> File: C: Packets: 211229 Displayed: 145515 Marked: 0	Profile: Default
📀 (0 🖉 🕑 🔼 🖉 📇	▲ No Difference 12:39 AM 12/13/2010

Gambar 4.13 Pengambilan Data Throughput

Dapat dilihat pada Gambar 4.13 data yang digunakan hanya data paket yang ada pada displayed bukan pada *captured*. Hal ini dimaksudkan agar yang ditampilkan hanya bagian – bagian yang diinginkan saja.

	51	
File (Mb)	Upload (Mbps)	Download (Mbps)
190	1,31	1,77
260	1,49	2,23
440	1,82	2,20
Rata-rata	1,54	2,06

Tabel 4.3 Throughput MIPv6

Tabel 4.4 Throughput MIPv6 tunneling 6to4

File (Mb)	Upload (Mbps)	Download (Mbps)
190	1,17	1,25
260	1,17	1,69
440	1,33	1,65
Rata-rata	1,22	1,53



Gambar 4.14 Diagram Perbandingan Throughput

Untuk menghitung perbandingan throughput saat upload dan download jaringan yang menggunakan konfigurasi MIPv6 dengan konfigurasi jaringan MIPv6 tunneling 6to4 dalam prosentase ditunjukkan rumus :

$$\% \text{ PThU} = \frac{\text{NThU MIPv6} - \text{NThU MIPv6 tunnel 6to4}}{\text{NThU MIPv6 tunnel 6to4}} \times 100\%$$
4.3

Keterangan : %PThU = Prosentasi Perbandingan Throughput saat Upload NThU = Nilai Throughput saat Upload

 $\% \text{ PThD} = \frac{\text{NThD MIPv6-NThD MIPv6 tunnel 6to4}}{\text{NThU MIPv6 tunnel 6to4}}$ 4.4

Keterangan :

%PThD = Prosentasi Perbandingan Throughput saat Download NThD = Nilai Throughput saat Download

Dari hasil perhitungan maka akan didapatkan nilai perbandingan throughput saat upload pada konfigurasi MIPv6 lebih besar antara 12% sampai 36% dibanding konfigurasi MIPv6 tunneling 6to4. Dan perbandingan throughput saat download pada konfigurasi MIPv6 lebih besar 31% sampai 41% dibanding

konfigurasi MIPv6 tunneling 6to4. Hal ini dikarenakan adanya proses enkapsulasi dan dekapsulasi paket pada mekanisme tunneling. Selain routing, proses enkapsulasi dan dekapsulasi juga dapat mengurangi througphut suatu file.

4.2.3 Analisa Delay

Delay adalah waktu tunda dari waktu yang seharusnya dari suksesnya seluruh paket yang diterima. Parameter *delay* dihitung dengan cara membagi nilai*transfer time* dengan jumlah bit data. Ditunjukkan pada rumus dibawah ini :

$$delay (sec) = \frac{transfer time (sec)}{jumlah bit}$$
4.5

Hasil pengambilan data secara keseluruhan untuk parameter *delay* dapat dilihat pada bagian lampiran sedangkan untuk hasil rata – rata dari perhitungan *delay* dapat dilihat pada Tabel 4.5.

Upload (µs)	Download (µs)
0,761	0,565
0,761	0,458
0,548	0,516
0,690	0,513
	Upload (µs) 0,761 0,761 0,548 0,690

Tabel 4.5 Delay pada Jaringan MIPv6

Tabel 4.6 Delay MIPv6 tunneling 6to4

File (Mb)	Upload (µs)	Download (µs)
190	0,854	0,799
260	0,857	0,590
440	0,754	0,606
Rata-rata	0,822	0,665

Untuk diagram perbandingan nilai delay dapat dilihat pada Gambar 4.15.



Gambar 4.15 Diagram Perbandingan Delay

Untuk menghitung perbandingan transfer time saat upload dan download jaringan yang menggunakan konfigurasi MIPv6 dengan konfigurasi jaringan MIPv6 tunneling 6to4 dalam prosentase ditunjukkan rumus :

$$\% PDU = \frac{NDU MIPv6 tunnel 6to4 - NDU MIPv6}{NDU MIPv6} 4.6$$

Keterangan : %PDU = Prosentasi Perbandingan Delay saat Upload NDU = Nilai Delay saat Upload

 $\% PDD = \frac{NDD MIPv6 tunnel 6to4 - NDD MIPv6}{NDD MIPv6} 4.7$

Keterangan : %PDD = Prosentasi Perbandingan Delay saat Download NTtD = Nilai Dealay saat Download

Dari hasil perhitungan maka akan didapatkan nilai perbandingan delay saat upload pada konfigurasi MIPv6 lebih kecil antara 12% sampai 38% dibanding konfigurasi MIPv6 tunneling 6to4. Dan perbandingan transfer time saat download pada konfigurasi MIPv6 lebih kecil 17% sampai 41% dibanding konfigurasi MIPv6 tunneling 6to4. Ini menunjukan bahwa selain proses routing juga dapat menambah delay jaringan. Hal ini dikarenakan adanya proses enkapsulasi dan dekapsulasi paket-paket pada proses tunneling.



BAB 5 KESIMPULAN

1 Untuk jaringan yang menggunakan MIPv6 secara presentasi memiliki nilai transfer time rata-rata lebih kecil pada saat upload 12% sampai 29% dan saat download 31% sampai 41% dari konfigurasi jaringan MIPv6 tunneling 6to4. Hal ini dikarenakan adanya proses enkapsulasi dan dekapsulasi paket pada mekanisme tunneling. Selain routing, proses enkapsulasi dan dekapsulasi juga dapat menambah waktu transfer suatu file.

2 Konfigorasi MIPv6 memiliki nilai throughput lebih besar pada saat upload 12% sampai 36% dan pada saat download 31% sampai 41% dibanding konfigurasi MIPv6 tunneling 6to4, hal ini dikarenakan adanya proses enkapsulasi dan dekapsulasi paket pada mekanisme tunneling. Selain routing, proses enkapsulasi dan dekapsulasi paket juga dapat mengurangi kecepatan rata-rata kirim keseluruhan paket.

3

Untuk delay dari konfigurasi MIPv6 lebih kecil pada saat upload 12% sampai 38% dan pada saat download 17% sampai 41% dibanding MIPv6 tunneling 6to4. Ini menunjukan bahwa selain proses routing juga dapat menambah delay jaringan. Hal ini dikarenakan adanya proses enkapsulasi dan dekapsulasi paket-paket yang masuk ada tunneling.

DAFTAR REFERENSI

[1]	Mobile Networking Through.
	http://Computer.Org/Internet/v2n1/perkins.htm
[2]	Data and Computer Communications, Stallings, W. Practice Hall, 2000
[3]	Ghosh, Debalina. Mobile IP. http://www.acm.org/crossroads/xrds7-
	<u>2/mobileip.html</u>
[4]	Mobile IP: Design Principles and Practice, Addison-Wesley
	Longman, Reading, Mass., 1998.
[5]	Computer Networks, Andrew S. Tanenbaum, 2003
[6]	Linux Mobile IPv6 HOWTO 2004–04–20
[7]	Wikipedia,"Tunneling Protocol", Diakses Maret 2010 dari Wikipedia.
	http://en.wikipedia.org/wiki/Tunneling_protocol
[8]	Wikipedia,"6to4", Diakses April 2010 dari Wikipedia
	http://en.wikipedia.org/wiki/6to4
[9]	en.wikipedia.org/wiki/SSH_File_Transfer_Protocol diakses Desember
	2010

1

LAMPIRAN HASIL CAPTURE WIRESARK



UPLOAD FILE 190MB PADA JARINGAN MIPv6

🕂 Capturing	from Microsoft - Wire	shark					_ 0 ×
<u>File</u> dit	<u>V</u> iew <u>G</u> o <u>C</u> apture	Analyze Statistics	Telephony Iools Help				
		XZAIQ	🔶 🔿 🖗 🛧 😓 🗐 🖬 🖓	Q Q Q 🖸 🖉 🗹 🍢 %	A		
Filter: ssh	Wireshark: Sumr	nary		ar Apply			
No. Tir	File						^
426995 19	Name:	C:\Users\Zuhal\Appl	Data\Local\Temp\wiresharkXXXXa02188	ypted request packet len=	512		
426996 19	Length:	253915624 bytes		ypted request packet len=	1440		
426999 19	Format:	Wireshark/tcpdump	/ libpcap	vpted request packet len=	512		
427000 19	Encapsulation: Dacket size limits	Unknown 65525 buter		ypted request packet len=	1440		
427001 19	Packet size infint.	00000 bytes		ypted request packet len=	96 -68		
427004 19	Time			ypted request packet len=	1440		
427005 19	First packet:	2010-12-13 00:22:31		ypted request packet len=	96		
427007 19	Last packet:	2010-12-13 00:31:33		vpted request packet len=	96		
427010 19	ciapseu:	00:09:01		ypted request packet len=	412		
427016 19	Capture			ypted response packet len	=100		
427017 19	Interface:	Microsoft		vpted response packet len	=68		
427019 19	Dropped packets	: unknown		ypted request packet len=	84		
427020 19	Capture filter:	none		ypted response packet len	=68		
427022 19	Display			ypted response packet len	=68		
427023 19	Display filter:	ssh		ypted request packet len=	58		
42/024 19	Ignored packets:	0		voted response packet len	=1284		
427026 19	Traffic	 Captured 	Displayed Marked	ypted response packet len	=84		
427027 19	Packets	427242	289780 0	ypted request packet len=	68		
427028 19	Between first and	last packet 541.640 see	c 180.379 sec	Retransmissionl Encrypte	=00 d response packet len=68		
427031 19	Avg. packets/sec	788.794	1606.509	ypted request packet len=	36		*
-	Avg. packet size	578.313 by	tes 817.446 bytes	m			•
⊕ Frame 3	Bytes	247079728	236879514	bits)			*
Etherne Interne	Avg. bytes/sec	456170.039	1313234.073	ink_63:eb:8f (00:24:01:63	:eb:8f)):0:b::1)		E
Transmi	Avg. MBit/sec	3.649	10.506	ssh (22), Seq: 1, Ack: 1	, Len: 68		*
0000 00			ALC: NAME	D1 .			
0010 00	Help		Close			A	=
0030 00				Lq=9.			
0040 /1	74 50 18 00 42 20 b7 54 d4 2d	94 e0 00 00 14	2 e0 1/ 08 0T e1 qtPB	····.no.			~
O Microsoft	: <live capture="" in="" prog<="" th=""><th>ress> File: C: Packe</th><th>ts: 427250 Displayed: 289780 Marked: 0</th><th></th><th></th><th>Profile: Default</th><th></th></live>	ress> File: C: Packe	ts: 427250 Displayed: 289780 Marked: 0			Profile: Default	
						- 🐚 🗟 📲	12:31 AM 12/13/2010
DOW	VNLOA	DFILE	190M MIPv6				
DUT		DTILL					
	(FOR						
. 🥴			root - root@2001:0:0:b::1 - WinSC	P			<u>s</u>
Recycle Bin	PDFCreator data1	upload	Local Mark Files Commands S	ession Options Remote Help			1
			👛 🛛 🗃 + 🖙 😫 📣 📼		C Default • 65 •		
							a
1			My documents •		🖌 root 🔹 🗠		18
			C:\Users\Zuhal\Documents		/root		_
Adobe	PrimoPDE -		Name Ext S	Size Type Changed	A Name Ext S	ize Changed Rights	C
Reader 9	Drop Files		*	Parent directory 12/13/2010	r 🔥	12/12/2010 8:5 rwxr-xr-x	r.
			Fax	Eile folder 12/9/2010	antitude	12/12/2010 8:5 rwx	r
			My Music	42% Copying	8 ×	12/12/2010 8:5 rwxr-xr-x	an a
3G			My Pictures		Creat	12/12/2010 1:5 rwxr-xr-x	r
Loin Air			My Videos		Cancer	12/12/2010 2:2 rwxr-xr-x	r
JOIN AU	annylb.		Scanned Documents	1	Minimize	12/12/2010 1:3 rwxr-xr-x	
			Capture.docx 7.001	File: data-1 rar		2 12/12/2010 2:5 PW	
	1		desktop.ini	Target: C:\Users\Zuhal\Document	s\ Once finished:	0 11/19/2007 9:5 rw-rr	r
ebY			LAN Card.docx 112	8	Stay idle 🔻	11/18/2010 7:2 rw-rr	r
			ssh.docx 700,	1 Time left: 0:00-41 Time	elapsed: 0:00:31		
eBay	Support		WUNIVERSITAS INDONE 81,	Bytes transferred: 81,599 KiB Spe	ed: 2,623 KiB/s Speed (KiB/s):		
	Seconden		WinSCP.exe 6,365,	6	Unlimited 👻		
-	~		WinSCP.ini 12,	7			
//							
	Ĩ.						
Foxit Reader	Winamp						
		11	•	Þ			F
		1	0 B of 14,028 KiB in 0 of 13		0 B of 185 MiB in 0 of 9		
		4/	1 / F2 Rename 17 F4 Edit 18 F5 C	Copy 🕼 F6 Move 🏕 F7 Create Directo	ry 🗙 F8 Delete 💣 F9 Properties 🖷 I	10 Quit	
data-3	data-1	1/			· · · · · · · · · · · · · · · · · · ·	A SETP.3 (1) 0.01.00	
						- JTIT'J - UUU!22	

▲ 🎼 🛱 🧋 🌵 12:35 AM 12/13/2010

Date 550M

🥹 📶 🖉 🐴

-

0

0

	tatistics Telephony <u>T</u> ools <u>H</u> elp		
	5 °, * * <mark>*</mark> 7 ½ 🗐 🖬] Q, Q, Q, 🖻 🖉 🕺 🥵 % 🎉	
ter: ssh		n Clear Apply	
Time Source	Destination Protocol	Info	
1047 112.081404 2001:0:0:b::1	2001::c:adfb:8b5d:e55Hv2	Encrypted response packet len=1440	
1049 112.081/79 2001:0:0:B::1 1050 112.082404 2001:0:0:b::1	2001::c:adfb:8b5d:eSSHV2 2001::c:adfb:8b5d:eSSHV2	Encrypted response packet Ten=1440 Encrypted response packet Ten=1440	
1052 112.082654 2001:0:0:b::1	2001::c:adfb:8b5d:eSSHv2	Encrypted response packet len=1440	
1053 112.083277 2001:0:0:b::1 1055 112.083790 2001:0:0:b::1	2001::c:adfb:8b5d:eSSHv2 2001::c:adfb:8b5d:eSSHv2	Encrypted response packet len=1440 Encrypted response packet len=1440	
1056 112.084232 2001:0:0:b::1	2001::c:adfb:8b5d:essHv2	Encrypted response packet len=1440	
1058 112.084654 2001:0:0:b::1 1059 112.085165 2001:0:0:b::1	2001::c:adfb:8b5d:eSSHv2 2001::c:adfb:8b5d:eSSHv2	Encrypted response packet len=1440 Encrypted response packet len=1440	
L060 112.085201 2001::c:adfb:8	b5d:e2001:0:0:b::1 55Hv2	Encrypted request packet len=68	
.061 112.085533 2001:0:0:b::1 062 112.086036 2001:0:0:b::1	2001::c:adfb:8b5d:eSSHv2 2001::c:adfb:8b5d:eSSHv2	Encrypted response packet len=1440 Encrypted response packet len=1440	
064 112.086540 2001:0:0:b::1	2001::c:adfb:8b5d:eSSHv2	Encrypted response packet len=1440	
065 112.087159 2001:0:0:b::1 067 112.087530 2001:0:0:b::1	2001::c:adfb:8b5d:eSSHv2 2001::c:adfb:8b5d:eSSHv2	Encrypted response packet len=1440 Encrypted response packet len=1440	
068 112.088154 2001:0:0:b::1	2001::c:adfb:8b5d:eSSHv2	Encrypted response packet len=1440	
070 112.088526 2001:0:0:b::1 071 112.089027 2001:0:0:b::1	2001::c:adfb:8b5d:eSSHv2 2001::c:adfb:8b5d:eSSHv2	Encrypted response packet len=1440 Encrypted response packet len=1440	
073 112.089404 2001:0:0:b::1	2001::c:adfb:8b5d:eSSHv2	Encrypted response packet len=1440	
074 112.089775 2001:0:0:b::1 076 112.089906 2001:0:0:b::1	2001::c:adfb:8b5d:eSSHv2 2001::c:adfb:8b5d:eSSHv2	Encrypted response packet len=444 Encrypted response packet len=84	
077 112.090275 2001:0:0:b::1	2001::c:adfb:8b5d:eSSHv2	Encrypted response packet len=84	
)79 112.091110 2001::c:adfb:8 080 112.092290 2001:0:0:b::1	b5d:e2001:0:0:b::1 S5Hv2 2001::c:adfb:8b5d:e55Hv2	Encrypted request packet len=68 Encrypted response packet len=84	
)81 112.093148 2001::c:adfb:8	b5d:e2001:0:0:b::1 SSHv2	Encrypted request packet len=68	
082 112.094299 2001:0:0:b::1	2001::c:adfb:8b5d:eS5Hv2	Encrypted response packet len=68 Encrypted request packet len=36	
to the courter and big	33112		
ame 3: 158 bytes on wire (12	264 bits), 158 bytes captured ((1264 bits)	
ternet II, Src: Azurewav_44	:31:05 (1c:4b:d6:44:31:05), Dst Src: 2001:0:0:a::2 (2001:0:0:a:	:: D-Link_63:eb:8f (00:24:01:63:eb:8f) ::2)	
ansmission Control Protocol	, Src Port: 55348 (55348), Dst	Port: ssh (22), Seq: 1, Ack: 1, Len: 84	
00 24 01 63 eb 8f 1c 4b d	l6 44 31 05 86 dd 60 00 .\$.c.	кD1`.	
00 00 00 68 06 40 20 01 00 00 00 00 00 00 00 00 00 00 00 00	0 00 00 00 00 00 0a 00 00h. 0 00 00 00 00 00 00 00	@	
00 00 00 00 00 01 d8 34 0 1e ad 50 18 00 42 6b 35 0	0 16 77 00 08 a9 44 24	4wD\$ 8k5	
cs of an od ab ac sh fe	0 56 15 21 00 1F 05 55		Destite: Default
icrosoft: «live capture in progress» File: C		.0	Pronie: Derault
	A CALL CALL CALL		12-27 ΔΝ
			▲ 🎼 🛱 📲 ♦ 12:37 AN 12/13/201
apturing from Microsoft - Wireshark			▲ 🎼 🛱 📲 🌵 12:37 AN 12/13/201 = 🗊 💈
pturing from Microsoft - Wireshark Edit View Go Capture Analyze	Statistics Telephony Iools Help		▲ 🕅 🛱 🚽 🌵 12:37 AN 12/13/201 — 🗇 🗧
pturing from Microsoft - Wireshark Edit View Go Capture Analyze S	Yatistics Telephony Iools Help 금 I 및 속 수 속 중 중 요 [문주		- 🕅 🛱 🚽 🌵 1237AM - 127J320 - 0
pturing from Microsoft - Wireshark Edit View Go Capture Analyze S Capture Analyze S	Statistics Telephony Iools Help □ ○ ◆ ↔ ↔ ☆ 중 앞 □ □] Q Q Q D 🔐 M 🍢 % 🛱 Ar Apply	- ™ Cf + + + + + 1237 Ab 1271,320 - ■ C = ■ C
pturing from Microsoft - Wireshark Edit View Go Capture Analyze S Capture Analyze S	Statistics Telephony Iools Help □ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○] Q Q Q ⊡ ₩ ⊠ 🖏 % Ξ Ar Apply yptcu - copyings - paciet - tci=1770	
pturing from Microsoft - Wireshark Edit View Go Capture Analyze S Store Capture Analyze S Wireshark: Summary File Name: C:\Users\Z	itatistics Telephony Iools Help	2 Q Q Q E M M S % E → ar Apply price response packet len=1440	
pturing from Microsoft - Wireshark Edit View Go Capture Analyze S San Wireshark: Summary Tir File Name: C.\Users/Z Length: 221008300	Valia AppData Local Temp Writeshark 2000 400	Q Q <td></td>	
pturing from Microsoft - Wireshark Edit View Go Cepture Analyze S Soft Wireshark Summary Tri Har 11 Naime: C.\Users/Z Length: 21506308 Format: Wireshark Soft Length: 21506308 Format: Wireshark	itatistics Telephony Tools Help	A company packet for 140 A company fore	
turing from Microsoft - Wireshark Edit View Go Capture Analyze S Go Capt	itatistics Telephony Iools Help	A company packet for 140 A company fore	
pturing from Microsoft - Wireshark Edit View Go Capture Analyze S Go Capture Analyze S	itatistics Telephony Iools Help	Ar Apply precer response packet len-1440 ypted response packet len-1440	
Construction of the second secon	Statistics Telephony Tools Help	ar Apply pred response packet len-1440 ypted response packet len-1440	
Source of the second seco	tuhal\AppData\Local\Temp\wiresharkXXXA00 bytes tcpdump/ libpcap 10:34:29 100:38:47	Ar Apply procer response packet len-1440 ypted response packet len-1440	
Soft Wireshark Summary Soft Wireshark Summary Soft Wireshark Summary Soft	Statistics Telephony Tools Help Statistics Telephony Tools Help	Action of the second se	
Image: Subscript of the second seco	Statistics Telephony Iools Help	Action of the second se	
pturing from Microsoft - Wireshark Edit View Go Capture Analyze S Edit View Go Capture Church Analyze S Edit Capture Church Analyze S Edit Capture Capture Church Analyze S Edit Capture Church	Statistics Telephony Iools Help	Ar Apply precer response packet len-1440 ypted response packet len-1440	
pturing from Microsoft - Wireshark Edit View Go Capture Analyze S sh Wireshark Summary Ti File Name: Cr\Users\2 Length: 21506308 Sish Wireshark Summary Tit File Name: Cr\Users\2 Length: 21506308 Sish Wireshark Summary Tit File Name: Cr\Users\2 Length: 21506308 Sish Tit Fire Packet size limit: 65335 byte Sish Time First packet: 2010-12-1: Last packet: 2010-12-1:	Statistics Telephony Iools Help	ar Apply pred response packet len-1440 ypted response packet len-1440	
sub-	Statistics Telephony Tools Help	ar Apply pred response packet len-1440 ypted response packet len-1440	
Image: Solution of the second secon	Statistics Telephony Tools Help	Ar Apply proce response packet len-1440 ypted response packet len-1440	
Image: Solution of the	tuhal/AppData\Local/Temp\wireshark0000400 bytes trcpdump/ libpcap 13 100-38-22	Action of the second se	
Image: Solution of the second secon	Statistics Telephony Iools Help Statistics Telephony Iools Help	Act Apply press response packet len-1440 ypted response packet len-844 ypted response packet len-84	
Image: Second	Eaptured 4 Displayed 4 Marked	A construction of the second s	
Image: Second	Eatistics Telephony Iools Help Eatistics Telephony Tools Help Eatistics Telephony Tools Help Eatistics Telephony Telephony Tools Eatistics Telephony Telephony Telephony Statistics Telephony Telephony Telephony Statis Telephony Tele	A construction of the second s	
Image: Second	Eaptured Displayed Marked Displayed Marked Li229 145515 0 257.797 sec 16.891 sec	ar Apply pred response packet len-1440 ypted response packet len-84 ypted response packet len-84 ypted request packet len-68 ypted response packet len-68	
Image: Second system Image: Second system Image: Second system Edit View Go Capture Analyze Second system Edit View Go Capture Analyze Second system Edit View Go Capture Analyze Second system Image: Second system Microsoft - Wireshark Summary Second system Second system Japate Microsoft - Wireshark Encapsulation: Ethernet Second system Japate Microsoft - Wireshark Encapsulation: Ethernet Packet size limit: S553 byte Japate First packet: 2010-12-11 Elapsed: 00:04:17 Japate Microsoft - Wireshark Capture Interface: Microsoft - Wireshark Japate Interface: Microsoft - Wireshark Capture filter: none Josplay Japate Japatekets: 0 Japatekets: 0 Japatekets Japatekets: 0 Japatekets: 0 Japatekets Japatekets: Jap	Captured Displayed Marked 211229 145515 0 257.797 sec 116.891 sec 19.362 1244.873	ar Apply pred response packet len-1440 ypted response packet len-84 ypted response packet len-84 ypted response packet len-84 ypted response packet len-86 ypted response packet len-88 ypted response packet len-68 ypted response packet len-68	
Image: Second	Captured	Ar Apply prot response packet len-1440 ypted response packet len-84 ypted response packet len-84 ypted response packet len-68 ypted request packet len-68 ypted request packet len-68 ypted request packet len-68 ypted request packet len-68	
Image: Second	Eaptured Displayed Marked Displayed	<pre>A comparison of the second of the secon</pre>	
Diving from Microsoft - Wireshark Edit View Go Capture Analyze S Edit View Go Capture Analyze S Shi Wireshark Summary T File Name: Cr\UserSi View Go Capture Analyze S Shi Wireshark Summary T File Name: Cr\UserSi So 11 Format Vireshark Summary T File Name: Cr\UserSi So 11 Format Vireshark Summary Time Format Vireshark Summary So 11 Format Vireshark Encapsulation: Ethernet Packets ize limit: 65335 byte So 11 So 11 So 11 So 11 Iast packet: 2010-12-11 Bapsed: 00.04:17 So 11 Iast packet: 2010-12-11 Iast packet: 2010-12-11 Iast packet: 2010-12-11 Iast packet: 00.04:17 So 11 Interface: Microsoft Display filter: sch	Captured Displayed Total AppData Local, Temp WiresharkXXXXa0 bytes tcpdump/ libpcap S Captured Displayed Marked Displayed Marked Displayed Marked Displayed Marked Displayed Displayed Displayed Displayed Displayed Displayed Displayed Displayed Displayed Displayed Displayed Dis	A Apply product response packet in-1440 ypted response packet ien-1440 ypted response packet ien-84 ypted response packet ien-84 ypted response packet ien-84 ypted request packet ien-68 ypted req	
Image: Second	Captured Displayed Marked 211229 145515 0 257.797 sec 116.891 sec 319.362 1244.873 1002.176 bytes 21142.190 bytes 20102176 bytes 1242.873 1002.176 bytes 211428 1243.190 bytes 2144.873 255.757 sec 116.891 sec 319.362 310032176 bytes 1244.873 1002.176 bytes 21144.513 1769201.401 5559	A construction of the second s	
Image: Second	Captured Displayed Marked 211229 145515 0 257.977 sec 116.891 sec 119.222 1102276 bytes 124.873 1002.176 bytes 2102176 bytes 124.137 1002.176 bytes 257.979 sec 116.891 sec 139.362 1102276 19.797 sec 116.891 sec 1102176 bytes 121.140 bytes 121.415 257.979 sec 116.891 sec 139.362 11032176 bytes 121.410 bytes 121.410 559 14.154 Cose	ar Apply price response packet len-1440 ypted response packet len-84 ypted response packet len-84 ypted request packet len-68 ypted request packet len-68 ypted response packet len-68 ypted response packet len-84 ypted response packet len-84 ypte	
Image: Second system Image: Second system Image: Second system Edit View Go Capture Analyze Second system Edit View Go Capture Analyze Second system Edit View Go Capture Analyze Second system Second system Mireshark: Summary Second system Second system View Mireshark: Summary Second system Second system Second system View Mireshark: Summary Second system Second system Second system View Mireshark: Summary Second system Second system Second system View Mireshark: Summary Second system Second system Second system Second system Signal Time First packet: 2010-12-11 Elapsed: 000417 Second system Second system <td< td=""><td>Statistics Telephony Tools Help Statistics Telephony Telephony Statistics Statistics Telephony Telephony Telephony Statistics Telephony Telephony Statistics Statistics Telephony Telephony Telephony Statistics Telephony</td><td>ar Apply price response packet len-1440 ypted response packet len-84 ypted response packet len-84 ypted request packet len-68 ypted request packet len-68 ypted response len-68 ypted response packet len-68 ypted res</td><td></td></td<>	Statistics Telephony Tools Help Statistics Telephony Telephony Statistics Statistics Telephony Telephony Telephony Statistics Telephony Telephony Statistics Statistics Telephony Telephony Telephony Statistics Telephony	ar Apply price response packet len-1440 ypted response packet len-84 ypted response packet len-84 ypted request packet len-68 ypted request packet len-68 ypted response len-68 ypted response packet len-68 ypted res	
Image: Second	Captured Displayed Marked 211229 12515 0 300:34:29 300:34:29 300:34:29 300:34:29 145515 0 257.797 sec 116:891 sec 319:362 124:4873 1002:176 bytes 145:59 211628:60 206604528 221145 1769201.401 5569 14.154	<pre>A C C C C C C C C C C C C C C C C C C C</pre>	
Image: Second	Captured Displayed Marked 211229 145515 0 200-34-29 106.891 sec 116.891 sec 1002-176 bytes 142.190 bytes 116.891 sec 11229 145515 0 257.797 sec 116.891 sec 116.891 sec 1130-362 122.48.873 1002.176 bytes 116666.20 206804528 22114.519 1002.176 bytes 141.54 Close 0 0.01 of 07 of 07 f7 dc P	<pre>A pply pictor response packet len-1440 ypted response pac</pre>	▲ No 1237 AU → 1237 AU → 10 2 →

UPLOAD FILE 260M MIPv6



🔀 Mi	crosoft - Wireshark		AND CONTRACT	- 0 X
Eile	Wireshark: Summ		Π	
		·		
-	File			
Filt	Name:	C:\Users\Zuhal\AppData\Local\Temp\wiresharkXXXXa03840	pn Clear Apply	
No	Length:	353735346 bytes	al Info	
	Format:	Wireshark/tcpdump/ libpcap	- cherypeen request packet ren-1770	
59	Encapsulation:	Ethernet	Encrypted request packet len=96	
59	Packet size limit:	65535 bytes	Encrypted response packet len=68	
59			Encrypted request packet ler=512	
59	Time		Encrypted request packet len=96	
59	First packet:	2010-12-13 00:47:37	Encrypted request packet len=1440	
59	Last packet:	2010-12-13 00:51:25	Encrypted request packet len=96	
59	Elapsed:	00:03:48	Encrypted request packet len=1440	
59			Encrypted request packet len=96	
59	Capture		Encrypted request packet len=1440	
59	Interface:	Microsoft	Encrypted request packet Ten=96	
50	Dropped packets:	: 0	Encrypted request packet len=300	
59	Capture filter:	none	Encrypted request packet len=100	
59			Encrypted response packet len=68	
59	Display		2 Encrypted request packet len=84	
59	Display filter:	ssh	: Encrypted response packet len=68	
59	Ignored packets:	0	Encrypted request packet len=68	
59			Encrypted response packet len=68	
59	Traffic	 Captured Displayed Marked 	Encrypted request packet len=68	
50	Packets	594815 403433 0	Encrypted response packet len=1412	
59	Between first and I	last packet 228.359 sec 221.494 sec	Encrypted request packet len=84	
59	Avg. packets/sec	2604.739 1821.416	Encrypted request packet len=68	
59	Aug. packet size	579 609 laster 919 074 laster	2 Encrypted response packet len=68	
59	Avg. packet size	576.050 bytes 616.074 bytes	[TCP Retransmission] Encrypted response packet len=68	
59	Bytes	344218282 330037996	Encrypted request packet len=36	
<	Avg. bytes/sec	1507357.321 1490052.651		•
÷ F	Avg. MBit/sec	12.059 11.920	(1136 bits)	A
± 6			t: D-Link_63:eb:8f (00:24:01:63:eb:8f)	
± 1	Help	Close	:::2), Dst: 2001:0:0:b::1 (2001:0:0:b::1)	<u> </u>
		6	Port: ssh (22), Seq: 1, Ack: 1, Len: 68	-
0000	00 24 01 63	eb 8t 1c 4b d6 44 31 05 86 dd 60 00 .\$.	скр1`.	
0010	00 00 00 58	06 40 20 01 00 00 00 00 00 0a 00 00	x.@	=
0020		00 02 20 01 00 00 00 00 00 00 00 00 00 00	····· 7 ······	1.224
0040	e7 6b 50 18	00 42 e1 0e 00 00 05 34 c3 9f 7e fa .kr	·	-
0050 Ei	28 ±4 oo d7	+h 52 70 55 70 84 22 Fs d2 21 F4 45 7	ked: 0 Dropped: 0	file: Default
	Contraction (Contraction)	pporte (cocart, cripting rackets options of spinoyed, 403435 Mar	Più Più Più Più	1252.044
				► 🔓 📲 🗣 12/12/2010
				12/13/2010

DOWNLOAD FILE 260 MIPV6

	🖕 root - root@2001:0:0:b::1 - WinSCP
Recycle Bin PDFCreator data1upload	Local Mark Files Commands Session Options Remote Help
	● 🗄 🗊 + 🏤 왕 관 🔤 🖗 왕 🏨 🛞 - 文 호 이 ۞ Default 🔹 🔇 •
	My documents • 😋 (↔ → →) 📾 🖾 🕼 😰 👔 🔐 root • 😋 (↔ → →) 📾 🖾 🕼 💱
	C:\Users\ZuhaNDocuments //oot
	Name Êst Size Type Changed / Name Êst Size Changed Rights C
Reader 9 Drop Files	💽 Parent directory 12/13/2010 r 😰 12/12/2010 8:5 rvvxr-xr-x r
	Fax File folder 12/9/2010 antitude 12/12/2010 8:5 rv/z r
	My Music 7% Copying 12/12/2010 8.5., novr-sr-sr r
	Inty Fictors Cancel 12/12/2010 22 VWY-WTX r
Join Air WinZip	Scanned Documents
	-Sapture.docx 11 varian2e p 12/12/2010 2:3 rv······ r
	Capture.docx 7,091,2 [File: data?ara. r
el?	Stay ide ▼ 11/19/200795 rv+r-r-r
	@LAN Card.docx 112.8 Time left: 0.0146 Time elanaed: 0.00.09 11/18/2010 7:1 rw-r-r- r
eBay Support Document	Ssh.docx 700,11 Bytes transferred: 18,708 K/B Speed: 2,310 K/B/s Speed (K/B/s):
	Universitas indone 81,8
	WinSpicke 0,30,00
oxit Reader Winamp	
	0 8 of 199 MB n 0 of 14 0 8 of 444 MB in 0 of 10
	🛛 🖉 F2 Rename 🧊 F4 Edit 🖄 F5 Copy 🍱 F6 Move 💣 F7 Create Directory 🗙 F8 Delete ङ F9 Properties 🏦 F10 Quit
data-3 data-1	B SFTP-3 □ 0.02.02
Mozilla data-2	Data 550M
Firefox	
🔊 O 🖉 🙆 🕼	第 第 第 単 0 1256 AU

Capturing from Microsoft - Wireshark	
<u>File Edit View Go Capture Analyze Statistics</u> Telephony <u>T</u> ools <u>H</u> elp	
	. Q. Q. 🖭 🌌 🖾 🥵 🧱
Eilter sch	are Apply
• Expression C	cai Appiy
No. Time Source Destination Protocol Info	spece response packee ren-sso
298656 131.389788 2001:0:0:b::1 2001:0:0:a::2 SSHv2 Enc	rypted response packet len=1440
298058 131.390104 2001:0:0:b::1 2001:0:0:a::2 SSHV2 End 208659 131 300704 2001:0:0:b::1 2001:0:0:a::2 SSHV2 End	rypted response packet ten=1440
298660 131.390819 2001:0:0:a::2 2001:0:0:b::1 SSHV2 End	rypted request packet len=68
298661 131.391047 2001:0:0:b::1 2001:0:0:a::2 S5Hv2 End	rypted response packet len=1440
298662 131.391671 2001:0:0:b::1 2001:0:0:a::2 SSHv2 End	rypted response packet len=1440
298664 131.392052 2001:0:0:b::1 2001:0:0:a::2 SSHv2 End	rypted response packet len=1440
298665 131.392438 2001:0:0:D::1 2001:0:0:a::2 S5HV2 End 298667 131 392970 2001:0:0:b::1 2001:0:0:a::2 S5HV2 End	rypted response packet len=1440
298668 131.393422 2001:0:0:b::1 2001:0:0:a::2 SSHV2 End	rypted response packet len=1440
298670 131.393922 2001:0:0:b::1 2001:0:0:a::2 55Hv2 End	rypted response packet len=1440
298671 131.394422 2001:0:0:b::1 2001:0:0:a::2 SSHv2 End	rypted response packet len=1440
2986/3 131.3946/2 2001:0:0:b::1 2001:0:0:a::2 SSHv2 End	rypted response packet len=596
298676 131, 398050 2001:0:0:b::1 2001:0:0:a::2 S5HV2 End	rypted response packet Ten=1440
298677 131.398547 2001:0:0:b::1 2001:0:0:a::2 SSHv2 End	rypted response packet len=1440
298679 131.398922 2001:0:0:b::1 2001:0:0:a::2 S5Hv2 End	ypted response packet len=1440
298680 131.399547 2001:0:0:b::1 2001:0:0:a::2 55Hv2 End	rypted response packet len=1440
298682 131.399796 2001:0:0:b::1 2001:0:0:a::2 SSHv2 End	rypted response packet len=532
298685 131 400704 2001:0:0:b::1 2001:0:0:a::2 558V2 Enc	ypted response packet tell=04
298686 131.400818 2001:0:0:a::2 2001:0:0:b::1 SSHV2 End	rypted reguest packet len=68
298687 131.401296 2001:0:0:b::1 2001:0:0:a::2 SSHv2 End	rypted response packet len=84
298688 131.401323 2001:0:0:a::2 2001:0:0:b::1 55Hv2 End	rypted request packet len=68
298689 131.401921 2001:0:0:b::1 2001:0:0:a::2 SSHv2 End	rypted response packet len=84
298090 131.402167 2001:0:0:D::1 2001:0:0:a::2 SSHV2 End 298709 136 901440 2001:0:0:a::2 2001:0:0:b::1 SSHV2 End	rypted response packet ten=08
Frame 14: 158 bytes on wire (1264 bits), 158 bytes captured (126	+ bits)
Ethernet II, Src: Azurewav_44:31:05 (1c:4b:d6:44:31:05), Dst: Tp	-LinkT_b0:9d:bf (00:27:19:b0:9d:bf)
Internet Protocol Version 6, Src: 2001::c:cde:80b4:b22:77fb (200	L::c:cde:80b4:b22:77fb), Dst: 2001:0:0:b::1 (2001:0:0:b::1)
⊞ Transmission Control Protocol, Src Port: 55353 (55353), Dst Port	: ssh (22), Seq: 1, Ack: 1, Len: 84
0000 00 27 19 b0 9d bf 1c 4b d6 44 31 05 86 dd 60 00 .'κ	D1`.
0010 00 00 00 68 06 40 20 01 00 00 00 00 00 00 0c 0c deh.@	······
0030 00 00 00 00 00 01 d8 39 00 16 ce ea 11 fe d2 699	
0040 12 16 50 18 10 ba a7 68 00 00 08 5c b6 89 7a 09h	······································
O Microsoft: <live capture="" in="" progress=""> File: C: Packets: 298740 Displayed: 206239 Marked: 0</live>	Profile: Default
	12:58 AM
	▲ 🕱 🖬 🤐 🥠 12/13/2010
Capturing from Microsoft - Wireshark	
Capturing from Microsoft - Wireshark Eile Edit View Go Capture Analyze Statistics Telephony Tools Help	- D X
Capturing from Microsoft - Wireshark Eile Edit View Go Capture Analyze Statistics Telephony Iools Help	
Capturing from Microsoft - Wireshark Elie Edit View Go Capture Analyze Statistics Telephony Iools Help Elie Edit View Go Capture Analyze Statistics Telephony Iools Help Elie Edit View Go Capture Analyze Statistics Telephony Iools Help Elie Edit View Go Capture Analyze Statistics Telephony Iools Help Elie Edit View Go Capture Analyze Statistics Telephony Iools Help Elie Edit View Go Capture Analyze Statistics Telephony Iools Help Elie Edit View Go Capture Analyze Statistics Telephony Iools Help Elie Edit View Go Capture Analyze Statistics Telephony Iools Help Elie Edit View Go Capture Analyze Statistics Telephony Iools Help Elie Edit View Go Capture Analyze Statistics Telephony Iools Help Elie Edit View Go Capture Analyze Statistics Telephony Iools Help Elie Edit View Go Capture Analyze Statistics Telephony Iools Help Elie Edit View Go Capture Analyze Statistics Telephony Iools Help Elie Edit View Go Capture Analyze Statistics Telephony Iools Help Elie Edit View Go Capture Analyze Statistics Telephony Iools Help Elie Edit View Go Capture Analyze Statistics Telephony Iools Help Elie Edit View Go Capture Analyze Statistics Telephony Iools Help Elie Edit View Go Capture Analyze Statistics Telephony Iools Help Elie Edit View Go Capture Analyze Statistics Telephony Iools Help Elie Edit View Go Capture Analyze Statistics Telephony Iools Help Elie Edit View Go Capture Analyze Statistics Telephony Iools Help Elie Edit View Go Capture Analyze Statistics Telephony Iools Help Elie Edit View Go Capture Analyze Statistics Telephony Iools Help Elie Edit View Go Capture Analyze Statistics Telephony Iools Help Elie Edit View Go Capture Analyze Statistics Telephony Iools Help Elie Edit View Go Capture Analyze Statistics Telephony Iools Help Elie Edit View Go Capture Analyze Statistics Telephony Iools Help Elie Edit View Go Capture Analyze Statistics Telephony Iools Help Elie Edit View Go Capture Analyze Statistics Telephony Iools Help Elie Edit View Go Capture Analyze Statistics Telephony Iools Help	
Capturing from Microsoft - Wireshark Elle Edit View Go Capture Analyze Statistics Telephony Iools Help Capture Analyze Statistics Telephony Iools Help Filte: Issh Wireshark Summary	- □ × . , Q, Q, ⊡ M, M ¹⁰ , % M ar Apply
Capturing from Microsoft - Wireshark Elle Edit View Go Capture Analyze Statistics Telephony Iools Help Filter ssh Wireshark Summary No. Trip	- □ ×) (Q, Q, 12) ■ ■ ■ 8 ※ Ⅲ ar Apply
Capturing from Microsoft - Wireshark Elie Edit View Go Capture Analyze Statistics Telephony Iools Help Filter Sch Wireshark Summary No. 2005 Til Filter Name CAll Jerch Zubah Applicitable (2015) Filter Statistics Telephony Iools Help Call Statistics Te	- □ X Q Q ⊡ M M N N III ar Apply proto response packet len=1440
Capturing from Microsoft - Wireshark Ele Edit View Go Capture Analyze Statistics Telephony Tools Help Wiresharke Summary No. Tir 2986551 Name: Cr\Users\Zuhal\AppData\Loca\\Temp\wiresharkOCOCka01060 Length: 200153983 bytes	Apply Ap
Capturing from Microsoft - Wireshark Elle Edit View Go Capture Analyze Statistics Telephony Iools Help Wireshark Summary No. 298655 11 298655 11 298655 12 298655 12 Ength: 201013983 Bytes Format: Wireshark Codumor, - libocap	ar Apply picto i copone packet len-1440 ypted response packet len-1440 ypted response packet len-1440
Capturing from Microsoft - Wireshark Elie Edit View Go Capture Analyze Statistics Telephony Tools Help Filter Ssh Wireshark/Summary No	Apply ar Apply pred response packet len-1440 ypted response packet len-1440 ypted response packet len-1440 ypted response packet len-1440 ypted response packet len-1640
Capturing from Microsoft - Wireshark Ele Edit View Go Capture Analyze Statistics Telephony Tools Help City of the state Summary No. Tr 298655 1 298655 1 298655 1 298655 1 298655 1 298656 1 298658 1 29868	
Capturing from Microsoft - Wireshark Elle Edit View Go Capture Analyze Statistics Telephony Tools Help Wireshark Summary No. Tr 2986551 1: Name: C:\User\Zuhal\AppData\Local\Temp\wireshark\XXX401060 Length: 300163983 bytes 2986561 1: 2986661 2986661 2: 2986661 2986661 1: 298664 C:\User\Zuhal\AppData\Local\Temp\wireshark\XXX401060 C:\User\Zuhal\AppData\Local\Temp\wireshark\XXX401060 298661 1: 298664 2986661 1: 298664 298664 1: 298664 C:\User\Zuhal\AppData\Local\Temp\wireshark\XXX401060 298664 1: 298664 C:\User\Zuhal\AppData\Local\Temp\wireshark\XXX401060 C:\User\XX401060 C:\Use	Image: Provide protect iclines ypted response packet ien-1440
Capturing from Microsoft - Wireshark Elie Edit View Go Capture Analyze Statistics Telephony Tools Help Filter: Sah Wireshark/Summary Filter: Sah Wireshark/Summary Filter: Sah Wireshark/Summary Filter: Sah Wireshark/Summary Filter: Sah Wireshark/Summary Filter: Sah Wireshark/Summary Filter: Sah Wireshark/Summary Filter: Sah Sampara Sam	Apply ar Apply ar Apply pred response packet len=1440 ypted response packet len=1440
Capturing from Microsoft - Wireshark File Edit View Go Capture Analyze Statistics Telephony Tools Help Filter sch No. 298655 11 298655 12 298656 11 298656 11 10012-1300-55:49	Apply Pred response packet len-1440
Capturing from Microsoft - Wireshark File Edit View Go Capture Analyze Statistics Telephony Tools Help Wireshark Summary No	A CONTRACTOR CONTRACTO
Capturing from Microsoft - Wireshark Elie Edit View Go Capture Analyze Statistics Telephony Tools Help Filter Sah Wireshark/Summary File Plant Ci-Users/Zuhal/AppData/Local/Temp/wireshark/000601060 Length: 201013983 bytes Pormat: Wireshark/Krpdump/Ilibpcap Encapsulation: Unknown Packet size limit: 65535 bytes Pasket Size Limit: 65535 bytes Pasket 2010-12-13 00:55:49 Last packet: 2010-12-13	Apply ar Apply prote response packet len-1440 ypted response packet len-1440
Capturing from Microsoft - Wireshark Elie Edit View Go Capture Analyze Statistics Telephony Tools Help Citizen Capture Analyze Statistics Telephony Tools Help View Go Capture Analyze Statistics Telephony Te	Apply If a point packet icn-355 ypted response packet icn-355 ypted response packet icn-1440 ypted response packet
Capturing from Microsoft - Wireshark Elie Edit View Go Capture Analyze Statistics Telephony Tools Help Capture Capture Analyze Statistics Telephony Tools Help Capture	Apply Ap
Capturing from Microsoft - Wireshark Elie Edit View Go Capture Analyze Statistics Telephony Tools Help Control	Apply ar Apply pred response packet len=1440 ypted response packet len=1440
Capturing from Microsoft - Wireshark Elie Edit View Go Capture Analyze Statistics Telephony Tools Help Cities Edit View Go Capture Analyze Statistics Telephony Tools Help View Go Capture Analyze Statistics Telephony Tools Help View Go Capture Cities 2010/12/13 00/	
Capturing from Microsoft - Wireshark Elie Edit View Go Capture Analyze Statistics Telephony Tools Help Control	Apply Ap
Capturing from Microsoft - Wireshark Elie Edit View Go Capture Analyze Statistics Telephony Tools Help Control Capture Canalyze Statistics Telephony Tools Help Wireshark/Summary No., Tri File Name: C1/Users/Zuhal/AppData/Local/Temp/wireshark/2000601060 Users/Zuhal/AppData/Local/Temp/wireshark/2000601060 Users/Zuhal/AppData/Local/Temp/wireshark/2000601060 Users/Zuhal/AppData/Local/Temp/wireshark/2000601060 Users/Zuhal/AppData/Local/Temp/wireshark/2000601060 Packet size limit: 65535 bytes Pormat: Wireshark/Rcpdump/ libpcap Encapsulation: Unknown Packet size limit: 65535 bytes Page6661 Users/Zuhal/AppData/Local/Temp/wireshark/20006011 Packet size limit: 65535 bytes Page6661 Users/Zuhal/AppData/Local/Temp/wireshark/2000601 Packet size limit: 65535 bytes Page6661 Users/Zuhal/AppData/Local/Temp/wireshark/2000601 Packet size limit: 65535 bytes Page6661 Page6661 Page6661 Page6661 Capture Interface: Microsoft Dropped packets: unknown Capture filte: none Page6861 Page6861 Page6861 Page6861 Page6861 Page6861 Page68	
Capturing from Microsoft - Wireshark Elie Edit View Go Capture Analyze Statistics Telephony Tools Help Cities Edit View Go Capture Analyze Statistics Telephony Tools Help View Go Capture Analyze Statistics Telephony Tools Help View Go Capture Cities 2 Capture Cities Cities 2 Capture Cities Cities 2 Capture Cities Cities Cities Cities Cities Cities 2 Capture Cities C	
Capturing from Microsoft - Wireshark Elie Edit View Go Capture Analyze Statistics Telephony Tools Help Control	Apply Ap
Capturing from Microsoft - Wireshark Elie Edit View Go Capture Analyze Statistics Telephony Tools Help Cities Edit View Go Capture Analyze Statistics Telephony Tools Help View Go Capture Analyze Statistics Telephony Tools Help View Go Capture Cities Cammary View Go Capture Cities Cathering Catherin	
Capturing from Microsoft - Wireshark Elie Edit View Go Capture Analyze Statistics Telephony Tools Help Filter Ish Wireshark Summary Filte Same C: User:\Zuhai\AppData\Local\Temp\wiresharkOcoca01060 Length: 2005393 Bytes 2986501 Length: 2005393 Bytes 298661 Encapsulation: Unknown Packet size limit: 5533 Bytes 298661 Encapsulation: Unknown Packet: 2010-12-13 00.55.49 Last packet: 2010-12-13 00.55.49 Last packet: 2010-12-13 00.55.49 Last packet: 2010-12-13 00.55.49 298661 Last packet: 2010-12-13 00.55.49 Last packet: 2010-12-13 00.55.49 Last packet: 2010-12-13 00.55.49 298661 Last packet: 2010-12-13 00.55.49 Last	
Capturing from Microsoft - Wireshark Elic Edit View Go Capture Analyze Statistics Telephony Tools Help Elic Edit View Go Capture Analyze Statistics Telephony Tools Help Wireshark Summary Non-out Tit Partice Statistics Wireshark Summary Non-out Tit Partice Statistics Wireshark Summary Partice Statistics Partice Statistics Partice Statistics Pomotics Partice Statistics Paris Partis Paris Partice Stati	P X Apply Protoc pactor incomes Part Part Part Part Part Part Part Part P
Capturing from Microsoft - Wireshark Elie Edit View Go Capture Analyze Statistics Telephony Tools Help Elie Edit View Go Capture Analyze Statistics Telephony Tools Help Filter Sah No	
Capturing from Microsoft - Wireshark Elic Edit View Go Capture Analyze Statistics Telephony Tools Help Capture Statistics Telephony Tele	Apply Ap
Capturing from Microsoft - Wireshark Elic Edit View Go Capture Analyze Statistics Telephony Tools Help Elic Edit View Go Capture Analyze Statistics Telephony Tools Help Wireshark: Summary No	
Capturing from Microsoft - Wireshark Elie Edit View Go Capture Analyze Statistics Telephony Tools Help Image: Statistics Telephony Tools Help Help Help Tools Help Help Help Help </td <td><pre>- • × . • • • • • • • • • • • • • • • • • • •</pre></td>	<pre>- • × . • • • • • • • • • • • • • • • • • • •</pre>
Capturing from Microsoft Wireshark Elic Edit View Go Capture Analyze Statistics Telephony Tools Help Control of the Control of	Apply Ap
Capturing from Microsoft - Wireshark Elic Edit View Go Capture Analyze Statistics Telephony Tools Help Elic Edit View Go Capture Analyze Statistics Telephony Tools Help Wireshark: Summary No	<pre>- • × - • · · · · · · · · · · · · · · · · · ·</pre>
Capturing from Microsoft - Wireshark Elie Edit View Go Capture Analyze Statistics Telephony Tools Help Filter Sah No	<pre>- • × </pre>
Capturing from Microsoft - Wireshark File Edit View Go Capture Analyze Statistics Telephony Tools Help Capture Capture Canalyze Statistics Telephony Tools Help Capture Capture Canalyze Statistics Telephony Tools Help Capture Capture Capture Canalyze Statistics Telephony Tools Help Capture Capt	<pre>Apply Apply A</pre>
Capturing from Microsoft - Wireshark File Edit View Go Capture Analyze Statistics Telephony Tools Help Wireshark: Summary Image: C. Users/Zuhal/AppData/Local/Temp/Wireshark/X00X401060 2986561 Length: 300163983 bytes 2986561 Format: Wireshark/Strokeny	<pre>Apply put it toppose packet len-1440 ypted response packe</pre>
Capturing from Microsoft - Wireshark File Edit View Go Capture Analyze Statistics Telephony Tools Help File Edit View Go Capture Analyze Statistics Telephony Tools Help File Statistics Telephony Tools Help File Statistics Telephony Tools Help Packet Statistics Telephony Tools Help Packet Statistics Telephony Tools Help Packet Statistics Telephony Tools Help Packet Statistics Tempth: 20015393 Bytes Packet Statistics Unknown Packet Statistics Tume Printer Wireshark/Captump/ libpcap Packet Statistics Display Packet Statistics Display filter: Packet Statistics Oldsad Packet Statistics Display filter:	<pre></pre>
Capturing from Microsoft - Wireshark Elle Edit View Go Capture Analyze Statistics Telephony Tools Help Filter Sah Wiresharke Summary No	Apply
Capturing from Microsoft - Wireshark Elic Edit View Go Capture Analyze Statistics Telephony Tools Help Filter Esh Wireshark Summary No	Apply precision of the set of th

UPLOAD FILE 440 MIPv6



Microsoft - Wireshark	
Eile Edit View Go Capture Analyze Statistics Telephony Tools Help	
	مَرْ اللَّهُ 🕺 💐 🗹 اللَّهُ اللَّ
Filter: ssh 🔹 Expression Clear Ap	ply
No. Time Source Destination Protocol Info	
1019264 307.4231 🖉 Wireshark: Summary	request packet len=512
1019266 307.4233 1019267 307.4233 File	request packet len=1440 request packet len=96
1019268 307.4234 Name: C:\Users\Zuhal\AppData\Local\Temp\wiresharkXXXXa02172	request packet len=1440
1019271 307.4251 Engrat: Wireshark/tendumn/libnean	request packet len=1440
1019272 307.4251 Encapsulation: Ethernet	request packet len=96 request packet len=1440
1019275 307.4252 Packet size limit: 65535 bytes	request packet len=96
1019277 307.4256 Time	request packet len=1440 request packet len=96
1019281 307. 4261 First packet: 2010-12-13 01:00:20	request packet len=1216
1019286 307.4286 Elapsed: 00:07:06	request packet len=100
1019287 307.4294 ' 1019288 307.4295	response packet len=68
1019289 307.4303 Capture	response packet len=68
1019290 307.4322 Dropped packets: 0	response packet len=68
1019292 307.4332 Capture filter: none	request packet len=68
1019293 307.4353 1019294 307.4361 Display	response packet len=84
1019296 307.4363 1019297 307.4369 Display filter: ssh	request packet len=68
1019298 307.4371 Ignored packets: 0	request packet len=68
1019299 307.4378 Traffic 4 Captured 4 Displayed 4 Marked 4 1019302 311.1360	request packet len=36
Packets 1019477 703733 0	m
B Frame 1: 142 Avg. packets/sec 2388.478 2261.818	++++++++++++++++++++++++++++++++++++++
Internet Prot Avg. packet size 579.822 bytes 806.652 bytes	001:0:0:b::1 (2001:0:0:b::1)
B Transmission Bytes 591114956 567667626	22), Seq: 1, Ack: 1, Len: 68
0000 00 24 01 Avg. bytes/sec 1384891.717 1824499.899	·
0020 00 00 00 Avg. MBit/sec 11.079 14.596	
0040 7c 26 50 0050 0b 60 41 <u>H</u> elp	•
File: "C:\Users\Zuh	Profile: Default
	▲ 📴 🗐 🕕 🚺 1308 AM 12/13/2010
DOWNLOAD FILE 440 MIPv6	
root - root@2001:0:0:b::1 - WinSCP	
Recycle Bin PDEGreator datatugload	Options Remote Help
	8 1 + - 1 0 0 0 Default - 1 3 -
	ne Channed Name Ext Size Channed Pinhtr (
Adobe PrimoPDF - Wireshark Paine Exc Size Type Reader 9 Dron Files Pai	rent directory 12/13/2010 r
Fax	• folder 12/9/2010 B antitude 12/12/2010 8:5 rwx r
My Music 5% Co	opying 12/12/2010 8:5 rwxr-xr-x r
3G BI	12/12/2010 1:5 rwxr-xr-x r
Join Air WinZip	12/12/2010 2:2 FWXT-XT-X F 12/12/2010 1:3 FWXT-XT-X F
🗐 ~ Sapture.docx 1	Minimize 9 12/12/2010 2:3 rw r
Capture.docx 7,091,2 File:	data-3.rar 2 12/15/2004 2:5 rw-rr r
data-1.rar 194,913,2	et: C:\Users\Zunar\Documents\ 0 11/19/2007 9:5 rw-rr r
data-2.rar 2/1,5/9,4	
aBay Support PLAN Card,docx 112.81 Byte	s tent: 0:02:44 Time elapsed: 0:00:09 11/10/2010 7:1 1W-1-1 1
Ssh.docx 700,1	Unlimited
MUNIVERSITAS INDONE 81,8	
WinSCP.exe 6,365,696 Ap	plication 9/24/2010 a
Event Partie Manua	miguration 12/13/2010 c
TOTAL CONTRACTOR AND	
	0.8 of 989 MB in 0 of 11
F2 Rename 12 F4 Edit 18 F5 Conv 15	F6 Move 💣 F7 Create Directory 🗙 F8 Delete 🚿 F9 Properties 🖷 F10 Ouit
data-3 data-1	A SFTP-3 000.32
Firefox Usida Story	
	 In the second sec
	12/

Microsoft - Wireshark		
e <u>E</u> dit <u>V</u> iew <u>Go</u> <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics Telephor	Iools Help	
(₩ & # # = 5 2 x 2 4 < + +	৯ 중 쏘│ 🗐 💷 │ Q, Q, Q, 🗹 │ 🖉 🗹 🥵 ※│ 💢	
ter: ssh	▼ Expression Clear Apply	
Time Source Destination	Protocol Info	
4673 179 820984 2001 0 0 0 b 1 2001 0 0 (a SSH Encrypted response packet len-1440	
675 179.821185 2001:0:0:b::1 2001:0:0	a::2 SSH Encrypted response packet len=596	
676 179.821805 2001:0:0:b::1 2001:0:0	a::2 SSH Encrypted response packet len=1440	
578 179.822179 2001:0:0:b::1 2001:0:0	a::2 SSH Encrypted response packet len=1440	
5/9 1/9.822805 2001:0:0:b::1 2001:0:0	a::2 SSH Encrypted response packet len=1440 a::2 SSH Encrypted response packet len=1440	
582 179.823686 2001:0:0:b::1 2001:0:0	a::2 SSH Encrypted response packet len=1440	
584 179.824198 2001:0:0:b::1 2001:0:0	a::2 SSH Encrypted response packet len=1440	
585 179.824688 2001:0:0:b::1 2001:0:0	a::2 SSH Encrypted response packet len=1440	
688 179.825559 2001:0:0:b::1 2001:0:0	a::2 SSH Encrypted response packet len=1440	
690 179.825934 2001:0:0:b::1 2001:0:0	a::2 SSH Encrypted response packet len=1440	
691 179.826565 2001:0:0:b::1 2001:0:0	a::2 SSH Encrypted response packet len=1440	
593 1/9.826813 2001:0:0:D::1 2001:0:0 594 179 827310 2001:0:0:b::1 2001:0:0	a::2 SSH Encrypted response packet len=596	
696 179.827810 2001:0:0:b::1 2001:0:0	a::2 SSH Encrypted response packet len=1440	
697 179.828304 2001:0:0:b::1 2001:0:0	a::2 SSH Encrypted response packet len=1440	
699 179.828439 2001:0:0:b::1 2001:0:0	a::2 S5H Encrypted response packet len=20	
700 179.828804 2001:0:0:b::1 2001:0:0	a::2 SSH Encrypted response packet len=84	
703 179.829297 2001:0:0:a::2 2001:0:0	b::1 S5H Encrypted request packet len=68	
704 179.829939 2001:0:0:b::1 2001:0:0	a::2 S5H Encrypted response packet len=84	
705 179.830635 2001:0:0:a::2 2001:0:0 705 179 826973 2001:0:0:b::1 2001:0:0	b::1 SSH Encrypted request packet len=68	
707 179.837068 2001:0:0:a::2 2001:0:0	b::1 SSH Encrypted request packet len=68	
708 179.837821 2001:0:0:b::1 2001:0:0	a::2 SSH Encrypted response packet len=68	
931 227.608595 2001:0:0:a::2 2001:0:0	b::1 SSH Encrypted request packet len=36	
ame 13: 158 bytes on wire (1264 bits), 1:	bytes captured (1264 bits) 16:44:31:05)pst: p_link_63:eb:8f (00:24:01:63:eb:8f)	
ternet Protocol Version 6, Src: 2001:0:0	1::2 (2001:0:0;a::2), Dst: 2001:0:0:b::1 (2001:0:0:b::1)	
ansmission Control Protocol, Src Port: 5	56 (55356), Dst Port: ssh (22), Seq: 1, Ack: 1, Len: 84	
00 24 01 63 eb 8f 1c 4b d6 44 31 05 86	dd 60 00	
00 00 00 68 06 40 20 01 00 00 00 00 00	0a 00 00h.@	
00 00 00 00 00 00 02 20 01 00 00 00 00 00 00 00 00 00 00 01 d8 3c 00 16 d9 c4 42	00 00 00	
82 a8 50 18 10 ba ec a0 00 00 44 73 55	9b 85 88PDsU	
e: "C:\Users\Zuhal\AppData\Local\Temp\ Packets: 514954	isplayed: 355319 Marked: 0 Dropped: 0	Profile: Default
		1:14 /
		* 🍱 🖷 📲 Y 12/13/2
icrosoft - Wireshark		
Wireshark: Summary		
	💳 🗖 🖬 I 🔍 Q 🔍 🗹 I 🖉 💹 % I 💢	and the second se
File		
Name: C:\Users\Zuhal\AppData\Local\Temp\v	reshark0000Xa03828 pn Clear Apply	
Length: 515533224 bytes	pl Info	
Format: Wiresnark/tcpdump/ IIbpcap	Encrypted response packet len=1440	
Packet size limit: 65535 bytes	Encrypted response packet len=596	
Tucket size mine obsiss bytes	Encrypted response packet len=1440	
Time	Encrypted response packet len=1440	
First packet: 2010-12-13 01:09:55	Encrypted response packet len=1440	
Last packet: 2010-12-13 01:13:46	Encrypted response packet len=1440	
Elapsed: 00:03:51	Encrypted response packet len=1440	
	Encrypted response packet len=1440	
Capture	Encrypted response packet len=1440	
Interface: Microsoft	Encrypted response packet len=1440	-
Canture filter pone	Encrypted response packet len=1440	
coprore men none	Encrypted response packet len=596	
Display	Encrypted response packet len=1440	
Display filter: ssh	Encrypted response packet len=1440	
Ignored packets: 0	Encrypted response packet len=20	
Testile 1 Contract 4 Direl 1 4	Encrypted response packet len=84	
Deskete E14054 DISplayed 4	Encrypted reguest packet len=68	
Packets 514954 355319	Encrypted response packet len=84	
Between first and last packet 231.406 sec 225.583 sec	Encrypted request packet len=68	
Avg. packets/sec 2225.323 1575.112	Encrypted response packet len=84	
Avg. packet size 985.125 bytes 1394.311 bytes	Encrypted response packet len=68	
Bytes 507293936 495425230	Encrypted request packet len=36	
Avg. bytes/sec 2192221.099 2196195.838		
Avg. MBit/sec 17.538 17.570	(1264 bits)	
	It: D-Link_63:eb:8f (00:24:01:63:eb:8f)	
Help	Close (22), Dst: 2001:0:0:b::1 (2001:0:0:b::1)	
	FULL SSIT (22), SEY. I, ACK. I, LETT. 04	
00 24 01 63 eb 8t 1c 4b d6 44 31 05 8t	dd 60 00	
00 24 01 63 eb 8t 1c 4b d6 44 31 05 8t 00 00 00 68 06 40 20 01 00 00 00 00 00 00 00 00 00 00 02 20 01 00 00 00 00 00	dd 60 00	
00 24 01 63 eb 87 1c 4b 66 44 31 05 88 00 00 00 68 06 40 20 01 00 00 00 00 00 00 00 00 00 00 02 20 01 00 00 00 00 00 00 00 00 00 1d 8 3c 00 16 d9 c4 73 55 28 28 50 18 10 b ec a0 00 00 44 73 55	add 60 00 .5.CK.D1`. 0a 00 00 80 8b 93	
00 24 01 63 eb 81 1c 4b 66 44 31 05 88 00 00 00 68 06 40 20 01 00 00 00 00 00 00 00 00 00 00 22 00 10 00 00 00 00 00 00 00 00 00 1d 83 c 00 16 d9 c4 42 82 88 50 18 10 ba c a0 00 00 47 73 55 89 07 46 41 05 26 55 42 56 42 56 42 57 56	dd 60 00	
00 24 01 63 eb 81 1 c 4b 66 44 31 05 88 00 00 00 68 66 40 20 10 00 00 00 00 00 00 00 00 68 66 40 20 10 00 00 00 00 00 00 00 00 00 02 20 01 00 00 00 00 00 00 00 00 00 01 48 c 00 16 09 c4 42 82 85 01 81 10 54 es 23 cf 46 -23 cf 88 07 4c 41 05 26 es 23 cf 46 -3 cf 88 07 4c 41 05 26 es 23 cf 46 -3 cf 88 07 4c 41 05 26 es 23 cf 46 -3 cf 88 07 4c 41 05 26 es 23 cf 46 -3 cf 88 07 4c 41 05 26 es 23 cf 46 -3 cf 88 07 4c 41 05 26 es 23 cf 46 -3 cf 88 07 4c 41 05 26 es 23 cf 46 -3 cf 88 07 4c 41 05 26 es 24 cf 80 cf	Gd 60 00	Profile: Default

UPLOAD FILE 190M MIPv6 TUNNELING 4to6


A Microsoft - Wireshark	
Eile Edit View Go Capture Analyze Statistics Telephony Iools Help	
Filter: ssh 🔹 Expression Clear	Apply
No. Time Source Destination Protocol Info	
425406 198.794762 2001::b:b5fc:1ff0:9::192.168.100.2 SSHv2 Encryp	ted request packet len=116
425408 198.795755 2001::b:b5fc:1ff0:9::192.168.100.2 S5HV2 Encryp 425409 198.795755 2001::b:b5fc:1ff0:9::192.168.100.2 S5HV2 Encryp	ted request packet len=1420 ted request packet len=116
425411 198.796995 2001::b:b5fc:1ff0:9::192.168.100.2 SSHv2 Encryp	ted request packet len=1420
425412 198.797113 2001::b:b5fc:1ff0:9::192.168.100.2 S5Hv2 Encry	ted request packet len=110
425415 198.797121 2001::b:b5fc:1ff0:9::192.168.100.2 SSHv2 Encryp	ted request packet len=116
425418 198.798268 2001::b:b5fc:1ff0:9::192.168.100.2 SSHV2 Encryp	ted request packet len=1420
425419 198.798273 2001::b:b5fc:1ff0:9::192.168.100.2 S5Hv2 Encryg 425421 198 799995 2001::b:b5fc:1ff0:9::192 168 100 2 S5Hv2 Encryg	ted request packet len=116
425422 198.800007 2001::b:b5fc:1ff0:9::192.168.100.2 SSHV2 Encryp	ted request packet len=116
425425 198.800843 2001::b:b5fc:1ff0:9::192.168.100.2 S5Hv2 Encryp 425429 198.802252 ::192.168.100.2 2001::b:b5fc:1ff0:955Hv2 Encryp	ted request packet len=508 ted response packet len=100
425430 198.802389 2001::b:b5fc:1ff0:9::192.168.100.2 S5Hv2 Encrypt	ted request packet len=100
425431 198.803447 ::192.168.100.2 2001::b:b5fc:1ff0:9S5Hv2 Encryp 425432 198.803573 2001::b:b5fc:1ff0:9::192.168.100.2 S5Hv2 Encryp	ted response packet len=68 ted request packet len=84
425433 198.804820 ::192.168.100.2 2001::b:b5fc:1ff0:955Hv2 Encry	ted response packet len=68
425434 198.805353 2001::D:D5TC:ITT0:9::192.168.100.2 S5HV2 Encry 425435 198.806322 ::192.168.100.2 2001::b:b5fc:1ff0:95SHv2 Encry	ted request packet len=68 ted response packet len=68
425436 198.806515 2001::b:b5fc:1ff0:9::192.168.100.2 SSHv2 Encryp	ted request packet len=68
425437 198.808821 ::192.108.100.2 2001::b:b5fc:1170:955HV2 Encry 425438 198.809067 2001::b:b5fc:1ff0:9::192.168.100.2 S5HV2 Encry	ted request packet len=948
425439 198.809946::192.168.100.2 2001::b:b5fc:1ff0:955Hv2 Encryp	ted response packet len=84
425441 198.810939 ::192.168.100.2 2001::b:b5fc:1ff0:955Hv2 Encryp	ted response packet len=68
425443 202.466959 2001::b:b5fc:1ff0:9::192.168.100.2 SSHv2 Encryp	ted request packet len=36
Crame 1: 142 butes on wire (1136 bits) 142 butes cantured (1136 bi	
Ethernet II, Src: Azurewav_44:31:05 (1c:4b:d6:44:31:05), Dst: Asust	ekC_e5:3f:f9 (00:11:2f:e5:3f:f9)
Internet Protocol Version 6, Src: 2001:0:0:a::2 (2001:0:0:a::2), DS Transmission Control Protocol, Src Port: 55361 (55361), DSt Port: 5	t: ::192.168.100.2 (::192.168.100.2)
0000 00 11 2f e5 3f f9 1c 4b d6 44 31 05 86 dd 60 00 / 2 K D1	·
0010 00 00 00 00 58 06 40 20 01 00 00 00 00 00 00 00 00 00	
0030 00 00 c0 a8 64 02 d8 41 00 16 56 45 a4 c6 4f 28dA[
0040 di bb 30 18 00 43 18 30 00 00 30 60 21 al 67 34	T
File: C:\Users\Zuhal\AppData\Local\Temp\ Packets: 425446 Displayed: 295464 Marked: 0 Droppe	e U Profile: Default 201 AM
	▲ 😼 🗳 📲 🌵 12/13/2010
M Microsoft - Wirechark	
File Edit View Go Capture Analyze Statistics Telephony Tools Help	
Expression Clear	Арру
125406 108 7	ed request parket log-116
425408 198.7 File	ed request packet len=1420
425409 198.7 Name: C:\Users\Zuhal\AppData\Local\Temp\wiresharkXXXXaUZU52 425411 198.7 Length: 253790347 bytes	ed request packet len=116
425412 198.7 Format: Wireshark/tcpdump/ libpcap	ed request packet len=116
425414 198.7 Encapsulation: Ethernet 425415 198.7 Backet size limit: 65535 butes	ed request packet len=1420 ed request packet len=116
425417 198.7	ed request packet len=512
425418 198. 1 425419 198. 7 Time	ed request packet len=1420 ed request packet len=116
425421 198.7 First packet: 2010-12-13 02:16:27	ed request packet len=1420
425425 198.8 Elapsed: 00:03:22	ed request packet len=10
425429 198.8	ed response packet len=100
425430 198.8 Interface: Microsoft	ed response packet len=68
425432 198.8 Dropped packets: 0	ed request packet len=84
425434 198.8 Capture filter: none	ed request packet len=68
425435 198.8 425436 198.8 Display	ed response packet len=68 ed request packet len=68
425437 198.8 Display filter: ssh	ed response packet len=948
425438 198.8 Ignored packets: 0 425439 198.8	ed request packet len=68 ed response packet len=84
425440 198.8 Traffic Captured Displayed Marked	ed request packet len=68
425443 202.4 Retween first and last nacket 202.471 car 202.467 car	ed request packet len=36
Avg. packets/sec 2101.274 1449.441	III +
Frame 1: 1 Avg. packet size S80.528 bytes S80.185 bytes	s) ^
	: ::192.168.100.2 (::192.168.100.2)
Transmissi Avg. bytes/sec 1219847.645 1171417.377	h (22), Seq: 1, Ack: 1, Len: 68
0000 00 11 Avg. MBit/sec 9.759 9.371	· `·
0020 00 00 Help	
0040 df bb	
File: "C:\Users\Zuhal\AppData\Local\Temp\ Packets: 425446 Displayed: 293464 Marked: 0 Dropped	0 Profile: Default
	▲ 18 18 - 41 - 40 - 2:21 AM
	12/13/2010

DOWNLOAD FILE 160 MIPv6 TUNNELING 6to4



Microsoft - Wireshark		
<u>File Edit View Go Capture Analyze Statistics Telephony Tools Help</u>		
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■		
Filter: ssh 💌 E	xpression Clear Apply	
Filter ssh v E No. Time Source Detination 210215 160. 340900 :192. 168. 100. 2 2001: :b:8585; f039: 5 210215 160. 3414000 :192. 168. 100. 2 2001: :b:8585; f039: 5 210216 160. 3414000 :192. 168. 100. 2 2001: :b:8585; f039: 5 210215 160. 3414000 :192. 168. 100. 2 2001: :b:8585; f039: 5 210212 160. 342995 :192. 168. 100. 2 2001: :b:8585; f039: 5 210221 160. 342977 :192. 168. 100. 2 2001: :b:8585; f039: 5 210222 160. 348152 :192. 168. 100. 2 2001: :b:8585; f039: 5 210222 160. 348152 :192. 168. 100. 2 2001: :b:8585; f039: 5 210222 160. 348152 :192. 168. 100. 2 2001: :b:8585; f039: 5 210228 160. 3514796 :192. 168. 100. 2 2001: :b:8585; f039: 5 210228 160. 3514780 :192. 168. 100. 2 2001: :b:8585; f039: 5 210238 160. 3514780 :192. 168. 100. 2 2001: :b:8585; f039: 5 210238 160. 351478 :19	spression Clear Apply Packetol SSHV2 Encrypted response packet lem=1420 SSHV2 SSHV2 Encrypted respo	
<pre></pre>	m	•
 Frame 11: 158 bytes on wire (1264 bits), 158 bytes cap Ethernet II, Src: Azurewav_44:31:05 (1c:4b:d6:44:31:05 Internet Protocol Version 6, Src: 2001:0:0:a::2 (2001: 	tured (1264 bits)), Dst: AsustekC_e5:3f:f9 (00:11:2f:e5:3f:f9) 0:0:a::2), Dst: :192.168.100.2 (::192.168.100.2)	
Transmission Control Protocol, Src Port: 55363 (55363) 0000 00 11 25 c5 25 50 1c 4b d5 44 21 05 86 dd 60 00	, Dst Port: ssh (22), Seq: 1, Ack: 1, Len: 84	
0000 00 1		I
File: "C:\Users\Zuhal\AppData\Local\Temp\ Packets: 210272 Displayed: 144940	Marked: 0 Dropped: 0	Profile: Default
		▲ 12/13/2010
Microsoft - Wireshark		_ 0 ×
Eile 📶 Wireshark: Summary		
File	🔽 🖥 I 🔍 Q. Q. 🖸 I 🖉 🕵 % I 📜 🔪	
Filt Name: C:\Users\Zuhal\AppData\Local\Temp\wiresharkXXXXa024	60 pn Clear Apply	
No. Length: 214991200 bytes Format: Wireshark/tcpdump/ libpcap	pl info	
21 Encapsulation: Ethernet	Encrypted response packet len=1420 Encrypted response packet len=1420	
21 Packet size limit: 65535 bytes	Encrypted response packet len=1420	
21 21 Time	Encrypted response packet Ten=1420 Encrypted response packet Ten=1420	
21 First packet: 2010-12-13 02:23:21 21 Last packet: 2010-12-13 02:26:08	Encrypted response packet len=1420	
21 Elapsed: 00:02:47	Encrypted response packet len=1420	
21 21 Capture	Encrypted response packet len=1420	
1 Interface: Microsoft	Encrypted response packet len=1420	
Dropped packets: 0	Encrypted request packet len=68	
21 Capture filter: none 21	<pre>Encrypted response packet len=1420 Encrypted response packet len=1420</pre>	
21 Display	Encrypted response packet len=1420	
21 Display filter: ssh 21 Innored packets: 0	Encrypted response packet len=1420 Encrypted response packet len=1420	
	Encrypted response packet len=1420	
21 Packets 210272 144940 0	 Encrypted response packet Ten=1420 Encrypted response packet Ten=1420 	
Between first and last packet 167.098 sec 165.238 sec	Encrypted response packet len=424 Encrypted response packet len=84	
Avg. packets/sec 1258.378 877.159	Encrypted response packet len=84	
Avg. packet size 1006.443 bytes 1426.503 bytes	Encrypted response packet len=100	
21 Bytes 211626824 206757398	Encrypted request packet len=36	
Avg. uytes/sec 1200480.234 12012/0.003	(1264 bits)	•
10.112 10.010	it: AsustekC_e5:3f:f9 (00:11:2f:e5:3f:f9)	
<u>H</u> elp <u>Close</u>	Port: ssh (22), Seq: 1, Ack: 1, Len: 84	
000 00 11 2T e5 3T T9 1C 4b d6 44 31 05 86 dd 60 00		
010 00 00 00 08 06 40 20 01 00 00 00 00 00 0a 00 00 020 00 00 00 00 02 00 00 00 00 00 00 00		[1
030 00 00 00 as 64 02 08 43 00 16 de 14 18 33 6e e0 040 d7 1b 50 18 00 42 80 fc 00 00 7c fc aa 57 52 c8		
File: "C:\Users\Zuhal\AppData\Local\Temp\ Packets: 210272 Displayed: 144940	Marked: 0 Dropped: 0	Profile: Default
		2:26 AM

UPLOAD FILE 260 MIPv6 TUNNELING 6to4



DOWNLOAD FILE 260 MIPv6 TUNNELING 6to4

JJL4JL L0J. JL/030 L001	c5a3:c1a2:4::192.168.100.2 55Hv2	cherypeen requese paexee ren=1420	
592453 269.927836 2001::b:		Encrypted request packet len=116	
592455 269.928529 2001::b:	c5a3:c1a2:4::192.168.100.2 SSHv2	Encrypted request packet len=1420	
592456 269.928540 2001::b: 592458 269 928717 2001b:	c5a3:c1a2:4::192.168.100.2 SSHV2	Encrypted request packet len=116	
592459 269.928723 2001::b:	c5a3:c1a2:4::192.168.100.2 SSHv2	Encrypted request packet len=116	
592461 269.929394 2001::b:	c5a3:c1a2:4::192.168.100.2 S5Hv2	Encrypted request packet len=1420	
592462 269.929400 2001::b:0	c5a3:c1a2:4::192.168.100.2 SSHV2	Encrypted request packet Ten=110	
92465 269.931663 2001::b:	c5a3:c1a2:4::192.168.100.2 SSHv2	Encrypted request packet len=116	
92467 269.931966 2001::b:(c5a3:c1a2:4::192.168.100.2 SSHV2	Encrypted request packet len=512	
92469 269.933344 2001::b:	c5a3:c1a2:4::192.168.100.2 SSHV2	Encrypted request packet len=1260	
92475 269.937574 ::192.16	8.100.2 2001::b:c5a3:c1a2:4 SSHv2	Encrypted response packet len=100	
92476 269.937755 2001::b:0	c5a3:c1a2:4::192.168.100.2 SSHV2 8 100 2 2001::b:c5a3:c1a2:4 SSHV2	Encrypted request packet len=100 Encrypted response packet len=68	
592478 269.939574 2001::b:	c5a3:c1a2:4::192.168.100.2 S5Hv2	Encrypted request packet len=84	
592479 269.941194 ::192.16	8.100.2 2001::b:c5a3:c1a2:4 SSHv2	Encrypted response packet len=68	
592480 269.941799 2001::D:0	8.100.2 2001::b:c5a3:c1a2:4 55HV2	Encrypted request packet Ten=68	
592482 269.943887 2001::b:	c5a3:c1a2:4::192.168.100.2 SSHv2	Encrypted request packet len=68	
592483 269.946325 ::192.16	8.100.2 2001::b:c5a3:c1a2:4 SSHV2	Encrypted response packet len=1060	
592485 269.947453 ::192.16	8.100.2 2001::b:c5a3:c1a2:4 55Hv2	Encrypted response packet len=84	
592486 269.947591 2001::b:	c5a3:c1a2:4::192.168.100.2 55Hv2	Encrypted request packet len=68	
592487 269.948453 ::192.16	8.100.2 2001::b:c5a3:c1a2:4 SSHV2 8.100.2 2001::b:c5a3:c1a2:4 SSHV2	Encrypted response packet len=68	
592490 283.877909 2001::b:	c5a3:c1a2:4::192.168.100.2 S5Hv2	Encrypted request packet len=36	
			•
🗈 Frame 2: 142 bytes on wi	re (1136 bits), 142 bytes captured (1136 bits)	*
Ethernet II, Src: Azurew Toternet Protocol Versio	av_44:31:05 (1c:4b:d6:44:31:05), Dst	: AsustekC_e5:3f:f9 (00:11:2f:e5:3f:f9) :2) Dsf: :192 168 100 2 (:192 168 100 2)	E
Transmission Control Pro	tocol, Src Port: 55365 (55365), Dst	Port: ssh (22), Seq: 1, Ack: 1, Len: 68	-
000 00 11 2f e5 3f f9 1c	4b d6 44 31 05 86 dd 60 00/.?.	кD1`.	
010 00 00 00 58 06 40 20 020 00 00 00 00 00 00 00 00 00 00 0	01 00 00 00 00 00 0a 00 00	a	E
030 00 00 c0 a8 64 02 d8	45 00 16 ac 92 3a ff b2 30d.	E	
040 04 00 00 10 00 42 80	20 05 02 50 50 22 fc bo 17 0 f		*
File: C:\Users\Zunai\AppData\Loca	Temp(Packets: 592503 Displayed: 409419 Marked:	: 0 Dropped: 0	Profile: Default
👩 🖸 🌔 🚺			▲ 🙀 🛱 📲 🌵 2233 AM
Filter: ssh Wireshark: Summary		ar Apply	
Filter: ssh Wireshark: Summary o. Tir		ar Apply	
Filter: ssh Wireshark: Summary	\Users\Zuhal\AppData\Local\Temp\wiresharkXXXXa04	ar Apply yptic request packet icinizato ypted request packet len=116	•
ilter: ssh Wireshark: Summary	\Users\Zuhal\AppData\Local\Temp\wiresharkXXXXa04	ar Apply pred request packet len-116 pred request packet len-1420	•
File File 92453 2 92455 2 92455 2 192456 2 92455 2 192457 2 192458 2	Ulsers\Zuhal\AppData\Local\Temp\wireshark0000ka04 3374136 bytes irreshark/tcpdump/ libpcap	ar Apply pred request packet len=116 ypted request packet len=1420 ypted request packet len=1420 ypted request packet len=1420	
File File 92455 24 92455 24 92455 24 92455 24 92455 24 92459 24 92459 24 92459 24 92459 24 92459 24 92459 24 92459 24	\Users\Zuhal\AppData\Local\Temp\wireshark0000Xa04 3574136 bytes ireshark/tcpdump/ libpcap hernet 555 haar	ar Apply pred request packet len-140 ypted request packet len-1420 ypted request packet len-1420 ypted request packet len-1420 ypted request packet len-116	,
Filter: File 192453 2C 192455 2C 192455 2C 192455 2C 192455 2C 192458 2C 192459 2C 192452 2C 1924	\Users\Zuhal\AppData\Local\Temp\wiresharkXXXXa04 3574136 bytes ireshark/tcpdump/ libpcap hernet 333 bytes	ar Apply pred request packet len=116 ypted request packet len=1420 ypted request packet len=1420 ypted request packet len=1420 ypted request packet len=1420 ypted request packet len=1420 pyted request packet len=1420 pyted request packet len=1420	ľ
Filter: ssh 592453 2c 592455 2c Length: 325 File Name: C: 592455 2c Length: 35 Format: W 592458 2c Encapsulation: Et 592461 2c Packet size limit: 65 592462 2c Time	\Users\Zuhal\AppData\Local\Temp\wireshark000Xa04 3374136 bytes ireshark/tcpdump/ libpcap henet 5335 bytes	<pre>ar Appy pred request packet len=116 ypted request packet len=1420 ypted request packet len=1420</pre>	
Iter State 02-000 Tr 192453 24 192455 Length: 192455 Length: 192455 Encapsulation: 192455 Encapsulation: 192455 Encapsulation: 192455 Encapsulation: 192452 Packet size limit: 192452 Time 192465 First packet: 20 192465 Enspekte: 20	\Users\Zuhal\AppData\Local\Temp\wireshark0000ka04 3374136 bytes ireshark/tcpdump/ libpcap henet 5335 bytes 10-12-13 0228:04 10-13 12 20-2251	<pre>ar Appy prtd request packet len-116 ypted request packet len-1420 ypted request packet len-</pre>	
Filter: ssh 592453 22 592455 22 592455 22 Length: 25 592455 22 Length: 25 592456 22 Encapsulation: Et 592456 22 592466 22 Time 592465 22 Last packet: 20 592466 22 Last packet: 20 592466 22 Last packet: 20 292466 22 Last packet: 20 292466 22 Last packet: 20 292466 22 Last packet: 20 2016 Last packet: 20 Last packet: 20 Last packet: 20 Last packet: 20 Last packet: 20 Last packet: 20	UUsers\Zuhal\AppData\Local\Temp\wireshark0000Xa04 33574136 bytes ireshark/tcpdump/ libpcap hernet 535 bytes 10-12-13 02:28:04 10-12-13 02:28:04 40-12-13 02:28:04	<pre>ar Apply prior request packet len=116 ypted request packet len=116 ypted request packet len=116 ypted request packet len=1120 ypted request packet len=1420 ypted request packet len=1420 ypted request packet len=1420 ypted request packet len=116 ypted request packet len=116 ypted request packet len=120 ypted request packet len=120 ypted request packet len=52</pre>	
Filter: ssh 592453 22 592455 22 592455 22 592456 22 592465 22 592466 20 592467 20 10 10 10 10 10 10 10 10 10 1	VUSers\Zuhal\AppData\Local\Temp\wireshark0000ka04 3374136 bytes irreshark/tcpdump/ libpcap hernet 5335 bytes 10-12-13 02:28:04 10-12-13 02:25:1 k04:47	<pre>r Apply pred request packet len=116 ypted request packet len=140 ypted request packet len=150 ypted request packet len=512 ypted request packet len=52 ypted request packet len=52</pre>	Å
Filter: ssh 592453 2 592453 2 File Format: Packet size limit: 65 592465 2 First packet: 20 592465 2 First packet: 20 592465 2 Elasped: Size First packet: 20 592465 2 Elasped: Size First packet: 20 592465 2 Elasped: Size First packet: 20 Size First packet: 20 Size	Ulsess Zuhal AppData Local Temp wireshark00004a04 13574136 bytes Irreshark102pd ump/ libpcap henet 1535 bytes 110-12-13 02:28:04 10-12-13 02:28:04 10-12-13 02:28:04	<pre>r Appy ptcl request packet len-l16 yptcd request packet len-l20 yptcd request packet len-l20 yptcd request packet len-l420 yptcd request packet len-l420 yptcd request packet len-l420 yptcd request packet len-l420 yptcd request packet len-l20 yptcd response packet len-l20 yptcd response packet len-l20 yptcd request packet len-l20 yptcd request packet len-l20 yptcd request packet len-l20 yptcd request packet len-l20 yptcd response packet len-l20 yptcd request packet len-l00 </pre>	
Filter: ssh 592455 22 592455 22 Length: 325 592455 22 Length: 325 592456 22 File S92456 22 File S92456 22 Format: We Encapsulation: Et 92466 22 First packet: 20 592466 22 First packet: 20 592466 22 Elapsed: 00 592467 22 Elapsed: 00 592477 22 First packet: 20 592477 22 First packet: 20 First packet: 20 F	VUSers/Zuhal/AppData/Local/Temp\wireshark00000404 3374136 bytes irreshark/topdump/ libpcap henet 5335 bytes 110-12-13 02:28:04 110-12-13 02:25:1 b04:47	<pre>r Appy ptcl request packet len-116 yptcd request packet len-120 yptcd request packet len-1420 yptcd request packet len-16 yptcd request packet len-16 yptcd request packet len-120 yptcd request packet len-120 yptcd request packet len-120 yptcd request packet len-120 yptcd response packet len-120 yptcd response packet len-16 yptcd response packet len-66</pre>	
Filter: Sh Wireshark: Summary 592455.2 File Name C: 592455.2 Length: 35 Signal Signal 592455.2 Length: 35 Signal Signal Signal 592456.2 Format: W Encapsulation: Et 592457.2 Signal Signal Signal Signal 592467.2 Last packet: 20 Signal Signal 592467.2 Last packet: 20 Signal Signal Signal 592467.2 Last packet: 20 Signal	VUSersi Zuhali AppData Li ocali Tempi wireshari X00004a04 3374136 bytes irreshari Xicpdump/ libpcap hernet 10-12-13 02:28:04 10-12-13 02:28:04 10-12-13 02:25:01 N04:47	<pre>r Appy r Ap</pre>	
Filter: Sh Wireshark: Summary 592455 2 File 592455 2 Format: W 592455 2 Format: W 592455 2 Format: W 592456 2 Format: W 592462 2 First packet: 20 592462 2 First packet: 20 592462 2 Elapsed: 00 592475 2 Capture 1 592475 2 Capture 0 592475 2 Capture 0 592476 2 Capture 0 592476 2 Capture 0 592476 2 Capture 0 592476 2 Capture filter: n 592476 2 Capture filter: n 592476 2 Capture filter: n 592470 2 Capture filter: n	VUSers\Zuhal\AppData\Local\Temp\wireshark00000404 33574136 bytes ireshark/tcpdump/ libpcap hernet 5355 bytes 10-12-13 02-28-04 10-12-13 02-28-04 10-12-14 02-14 10-14-14 10-14-14 02-14 10-14-14 10-	<pre>r Appy rt ar Appy</pre>	
Filter: Sth Wireshark: Summary 10: 11: File 592453 2 Name: C: 592453 2 Name: C: 592453 2 Length: 33 592452 Format: V Encapsulation: 592462 Packet size limit: 55 592462 Last packet: 20 592462 Last packet: 20 592462 Last packet: 20 592463 Capture 592465 592464 Linterface: M 592465 Capture 592467 592467 Last packet: 20 592467 Last packet: 0 592476 Oropped packets: 0 592478 Dropped packets: 0 592487 Display Display	VUsers) Zuhal AppData\Local\Temp\wiresharkX000Xa04 3357436 bytes irresharkXtcpdump/ libpcap henet 5535 bytes 110-12-13 02:28:04 10-12-13 02:28:04 10-12-13 02:28:04 10-12-13 02:28:04 10-12-13 02:28:04	<pre>r Appy rtd toquest packet len-116 ypted request packet len-126 ypted request packet len-1420 ypted request packet len-120 ypted request packet len-120 ypted request packet len-120 ypted request packet len-120 ypted request packet len-16 ypted request packet len-16 ypted request packet len-16 ypted request packet len-16 ypted request packet len-160 ypted response packet len-68 ypted response packet len-68 ypted request packet len-68 ypted response packet len-68 ypted</pre>	
Filter: Strike: Wireshark: Summary 0: Tre File 992453 File Name: 992453 Cangatin: 33 992453 File Same: 992453 File Same: 992453 Format: 33 992454 Format: 32 992462 Format: 32 992462 Fist packet size limit: 55 992462 Last packet: 20 992462 Last packet: 20 992462 Fist packet: 20 992462 Last packet: 20 992462 Last packet: 20 992462 Capture Interface: 00 992476 Capture filter: no 20 992478 Capture filter: no 20 992482 Display filter: 20 20 992482 Display filter: 20 20	VUSers/Zuhal/AppData/Local/Temp/wireshark00003a04 3374136 bytes irreshark/topdump/ libpcap henet 5335 bytes 10-12-13 02:28:04 10-12-13 02:29:04 10-12-13 02:29:04 10-12-13 02:29:04 iicrosoft one	<pre>r Appy rtd request packet len-l16 ypted request packet len-l20 ypted request packet len-l420 ypted request packet len-l20 ypted response packet len-l20 ypted response packet len-l20 ypted response packet len-l68 ypted request packet len-68 ypted request packet len-68 ypted request packet len-68 ypted response packet len-68 y</pre>	
Filter: Sh Wireshark: Summary 592455 C Name C: 592455 C Length: 35 592455 C Length: 35 592455 C File Name 592455 C Length: 35 592456 C Fornat: W 592452 Packet isze limit: 55 592462 C Ime 592462 Last packet: 20 592462 Elapsek: 20 592463 C Capture 592463 C Titeface: M 592463 C Capture 0 592463 C Diopled packets: 0 592463 C Diopled packets: 0 592463 C Diopled packets: 0 592463 Dioplay filter: ss 1gnored packets: 0 592483 Linglay filter: ss 1gnored packets: 0	VUSers\ZuhallAppData\Local\Temp\wireshark00006a04 3374136 bytes irreshark10tpdump/ libpcap henet 10535 bytes 105-12-13 02-28:04 105-12-13 02-28:04 106-12-13 02-28:04 incrosoft one	<pre>r Appy rtd request packet len-116 pred request packet len-1420 pred request packet len-16 pred request packet len-512 pred response packet len-68 pred request p</pre>	
Filter: Sh Wireshark: Summary 592455 2 File 592455 2 Length: 33 592455 2 Format: W 592455 2 Format: W 592455 2 Format: W 592455 2 Format: W 592452 2 Format: W 592462 2 Time 592462 592462 2 First packet: 20 592462 2 Elapsed: 00 592462 2 Elapsed: 00 592462 2 Elapsed: 00 592472 2 Capture 1 592472 2 Capture 1 592478 2 Display filter: no 592482 2 Display filter: s 592482 2 Ignored packets: 0 592482 2 Display 5 2	Augusta (Local) Temp\wireshark00004a04 3374136 bytes irreshark/tcpdump/ libpcap hernet 3355 bytes 10-12-13 02:28:04 10-12-13 02:28:04 10-12-14 10-12-14 10-12-14 10-12-14 10-12-14 10-12-14 10-14 10-14 10-14 10-14 10-14 10-14 10-14 10-14 10-14	<pre>r Appy r Appyy r Appy r A</pre>	
Filter: Sh Sh< Sh< Sh Sh Sh Sh Sh Sh Sh Sh<	Users) Zuhal AppData (Local \ Temp\wireshark)0000404 13574136 bytes irreshark/topdomp/ libpcap henret 1535 bytes 110-12-13 02:28.04 101-12-14 <	<pre>r Appy rtd toquest packet ton=116 pted request packet ton=116 pted request packet ton=1420 pted request packet ton=152 pted request packet ton=16 pted request packet ton=512 pted request packet ton=50 pted request packet ton=68 pted response packet ton=68 pted request packet ton=68 pted request packet ton=68 pted response packet t</pre>	
Filter: Sh Wiresbark: Summary 592455 2 Name: CS 592455 2 Name: CS 592455 2 Length: 35 592455 2 Filte SS 592456 2 Format: W 592457 2 Format: W 592458 2 Packet size limit: 55 592467 2 Lime 592468 592468 2 Last packet: 20 592467 2 Last packet: 00 592467 2 Capture 1 592467 2 Display filter: ss 592482 2 Display filter: ss 592482 2 Traffic 1 592482 Capture 1	Augusta Zuhal AppData Liocal Temp wireshark0000304 3374136 bytes irreshark ktopdump/ libpcap henet 1535 bytes 10-12-13 02:28:04 10-12-13 02:28:04 10-12-12-12 10	<pre>r Appy rtd request packet len-l16 prtd request packet len-l20 prtd request packet len-68 prtd request</pre>	
Biller: Shift Pile 92455 22 Name: C: 92455 22 Name: C: 92455 22 Length: 35 92456 22 Format: W 92458 22 Format: W 92459 24 Format: W 92459 24 Format: W 92461 22 Packet size limit: 5 92462 24 Time 1 92462 24 Last packet: 20 92462 24 Interface: M 92476 24 Last packet: 20 92476 24 Lapacket: 20 92476 24 Capture filter: 0 92478 24 Display filter: ss 9248 24 Display filter: 39248 24 9248 24 Display filter: ss 9248 24 Display filter: 39248 24 9248 24 Between first and last Avg. packets'se 92484 24 Between first and last Avg. packets'se 92480 24	Image: Control of the second	<pre>r Appy rtd tequest packet len-116 pred request packet len-120 pred request packet len-1420 pred request packet len-16 pred request packet len-16 pred response packet len-512 pred response packet len-68 pred response packet len-68 pred request packet len-68 pred request</pre>	
Filter: Sh Wiresbark: Summary Signed State File Name: CL Signed State C Name: CL Signed State C Length: 33 Signed State File Name: CL Signed State Format: W Encapsulation: Et Signed State Capture Interface M Signed State 20 Signed State Capture Interface M Dropped packets: 00 Signed State Capture E Interface M Dropped packets: 0 Signed State Capture E Interface M Dropped packets: 0 Signed State Capture E Interface M Dropped packets: 0 Signed State C Display filter: ss Ignored packets: 0 Signed State C Packets Sected State Avg. packets/sec Avg. packets/sec Signed State Refere Refere Secte	Captured Displayed Marked 592503 409419 0 packet 287.757 sec 283.252 sec 2039.040 1445.423 589.747 bytes 307.473 sec	<pre>r Appy ref Apply ref to the to prove prove the top top top top top top top top top top</pre>	
Biller: Sh PCI Wiresbark: Summary 0	VUses) Zuhal AppData LLocal Temp wireshark 2000 xa04 13574136 bytes Irreshark Xtepdomp/ libpcap henet 10-12-13 02:28:04 10-12-13 02:28:04 10-12-14	<pre>r Appy rt Appy rt</pre>	
Itter: Sh Ittershark: Summary 92453 2 Name: C: 92453 2 Name: C: 92453 2 Name: C: 92453 2 Inite Signal 92454 2 File Packet size limit: 92454 2 Format: W 92452 2 Packet size limit: 65 92462 2 Imine 924652 Elapsed: 00 92465 2 First packet: 20 924652 Elapsed: 00 92465 2 Capture 1 924762 2 9247624 02 92465 2 Elapsed: 00 9247624 02 92462 02 9247624 02 9247624 02 9247624 02 9247624 02 9247624 02 9247624 02 9247624 02 9247624 02 9247624 02 9247624 02 9247624	Captured Displayed Marked 592503 409419 0 packet 287.757 sec 283.252 sec 2039.040 19770 bytes 140412 3504136 1012-13 0228.04 0 1012-13 0228.04 0 1012-13 0228.04 0 1012-13 0228.04 0 packet 287.757 sec 283.252 sec 2039.040 2039.040 14454.423 580.747 bytes 807.203 bytes 344094064 330484136 1195780.099 1195780.099 1166194.413 9.566	<pre>r Appy rtd toucts packet icn-116 rpted request packet icn-126 rpted request packet icn-126 rpted request packet icn-126 rpted request packet icn-126 rpted request packet icn-120 rpted response packet icn-26 rpted request packet icn-68 rpt</pre>	
Ite: Sh Ite Wireshark: Summary 22453 Ite File Status 22453 Length: 35 22452 Length: 35 22452 Format: W 22452 Packet size limit: 55 22452 First packet: 20 22462 Time 22462 22462 First packet: 20 22462 Elapsed: 20 22463 Capture 22467 22464 Elapsed: 20 22465 Capture 22467 22467 Capture filte: 00 22475 Capture filte: 02 22476 Display filter: ss 22476 Display filter: ss 22481 Display filter: ss 22482 Between first and last 22487 22487 Between first and last 22487 22487 Bytes Avg. packets/sec 22487 Byte	Capturel Displayed Marked 552503 409419 0 packet 287.757 sec 283252 sec 283252 sec 2059.040 3304136 1195780.009 110-12-13 0228.04 0 0 100-12-13 0228.04 0 0 101-12-13 0228.04 0 0 101-12-13 0228.04 0 0 packet 287.757 sec 283.252 sec 2059.040 595.03 409419 0 packet 287.757 sec 283.252 sec 2059.040 1195780.009 1166749.413 30484136 1195780.009 1166749.413 9.366	<pre>r Appy rtd request packet len-l16 pred request packet len-l20 pred request packet len-l20 pred request packet len-l420 pred request packet len-l420 pred request packet len-l420 pred request packet len-l420 pred request packet len-l20 pred response packet len-l20 pred request packet len-l20 pred response packet len-l20 pred request packet len-l20 pred request packet len-l20 pred request packet len-l20 pred request packet len-68 pred req</pre>	
itter Sh I Wireshark: Summary 92453 C Name: C: 92453 C Length: 25 92455 C Length: 25 92455 C Length: 25 92455 C Length: 25 92452 C Packet size limit: 65 92462 Time 92465 26 92465 C Ista packet: 20 92465 C First packet: 20 92465 C Interface: M 92467 C Last packet: 20 92476 C Capture M 92477 C Capture finter: nr 92482 Display filter: sz 1 92482 Display Stilter 2 92482 Between first and last 2 92485 Stilter Avg. packet size 92485 Between first and last 2 </td <td>AUsers)Zuhali AppData\Locali Temp\wireshark00000404 3374136 bytes irreshark102000404 100-12-13 0228:04 100-12-13 0228:04 100-12-14 100-12-13 0228:04 100-12-14 100-12-14 100-12-14 100-12-14 100-12-14 100-12-14 100-12-14 100-12-14 100-12-14 100-12-14 100-12-14 100-12-14 100-12-14 100-14</td> <td><pre>r Appy rtd townor packet icnatio pred request packet ienalis pred request packet</pre></td> <td></td>	AUsers)Zuhali AppData\Locali Temp\wireshark00000404 3374136 bytes irreshark102000404 100-12-13 0228:04 100-12-13 0228:04 100-12-14 100-12-13 0228:04 100-12-14 100-12-14 100-12-14 100-12-14 100-12-14 100-12-14 100-12-14 100-12-14 100-12-14 100-12-14 100-12-14 100-12-14 100-12-14 100-14	<pre>r Appy rtd townor packet icnatio pred request packet ienalis pred request packet</pre>	
Ite: Shi Ite: Ite: 22453 24 Name: C. 22453 24 Name: C. 22452 24 Name: C. 22452 24 Length: 33 22452 24 File Name: C. 22452 24 Format: W Encapsulation: E4 22461 24 Time 24652 Elapsekt: 20 22462 24 Time 24662 24 2462 24 22462 24 Time 24762 24872 24 2462 24 2462 24 2462 24 2462 24 2462 24 2462 24 2462 24 2462 24 247 24 24 247 24 247 24 2462 247 24 2465 24 2479 24 2465 24 2483 24 2483 24 2484	Captured Displayed Marked 592503 409419 0 packet 287.757 sec 283.252 sec 2059.440 195780-099 1165749.413 0 packet 287.757 sec 283.423 Son.747 bytes 195780-099 1165749.413 0 packet 287.757 sec 283.423 Son.747 bytes 1195780-099 1165749.413 0 pc66 9.334 Close	<pre>r Appy rtd treates packet in-116 rpted request packet in-116 rpted request packet in-116 rpted request packet in-116 rpted request packet in-1420 rpted request packet in-120 rpted request packet in-120 rpted response packet in-120 rpted response packet in-120 rpted response packet in-16 rpted response packet in-68 rpted response packet in-68 rpted request packet in-68 rpted response packet in-68 rpted response packet in-68 rpted request packet in-68 rpted reque</pre>	
Itter: Shi Itershark: Summary 92453 Itershark: Summary 92453 Name: C: 92453 Length: 33 92454 Length: 33 92455 Itershark: W 92452 Length: 33 92452 First Packet size limit: 92452 Time Packet size limit: 92462 Iters 20 92462 Iterst 20 92462 Iterstack 20 92475 C Capture 92476 C Display filter: ss 92481 Ignored packets: 0 0 92482 Ignored packets: 9 9 2486 24	Captured Displayed Marked 592503 409419 0 packet 287.757 sec 28.04 0 0 10-12-13 02:28.04 0 0 10-12-13 02:28.04 0 0 10-12-13 02:28.04 0 0 10-12-13 02:28.04 0 0 10-12-13 02:28.04 0 0 packet 287.757 sec 28.04 0 0 packet 287.757 sec 28.04 0 0 packet 287.757 sec 28.02 0.03.02.03.02.03 0 110-15760.009 1166749.41.3 9.566 9.33.4	<pre>Apply Acceleration of the second second</pre>	
Filter State View View S22452 View S22462 List S22462 Last S22462 Last S22462 Last S22462 Last S22462 Last S22462 Last S22472 Capture S22472 Display filter: S22472 Display filter: S22482 Jonced packet: S22482 View S22482 View S22482 View S22482 View S24842 Niew <		<pre>r Appy rtcd towctor parket ichilds pred request packet ichilds pred request packe</pre>	Profile Default

_ 0 <u>_ x</u>



UPLOAD FILE 440 MIPv6 TUNNELING 6to4

Image: 2: 138 bytes: on winter (224 bits), 138 bytes: catured (224 bits), Image: 2: 138 bytes: on winter (224 bits), 138 bytes: catured (224 bits), Image: 2: 138 bytes: on winter (224 bits), 138 bytes: catured (224 bits), Image: 2: 138 bytes: on winter (224 bits), 138 bytes: catured (224 bits), Image: 2: 138 bytes: on winter (224 bits), 138 bytes: catured (224 bits), Image: 2: 138 bytes: on winter (224 bits), 138 bytes: catured (224 bits), Image: 2: 138 bytes: on winter (224 bits), 138 bytes: catured (224 bits), Image: 2: 138 bytes: on winter (224 bits), 138 bytes: catured (224 bits), Image: 2: 138 bytes: on winter (224 bits), 138 bytes: catured (224 bits), Image: 2: 138 bytes: on winter (224 bits), 138 bytes: catured (224 bits), Image: 2: 138 bytes: on winter (224 bits), 138 bytes: catured (224 bits), Image: 2: 138 bytes: on winter (224 bits), 138 bytes: catured (224 bits), Image: 2: 138 bytes: 0 bits), 138 bytes: 138 byt	299952 170. 841126 :: 299953 170. 841101 :: 299955 170. 842000 :: 299955 170. 84200 :: 299958 170. 84367 :: 299960 170. 84367 :: 299960 170. 84454 :: 299964 170. 84454 :: 299964 170. 84458 :: 299966 170. 84536 :: 299967 170. 84538 :: 299969 170. 84568 ::	192.168.100.2 2001:b:8c59:c6e9:655HV2 Er 192.168.100.2 2001:b:8c59:c69:655HV2 Er 192.168.100.2 2001:b:8c59:c69:655HV2 Er 192.168.100.2 2001:b:8c59:c69:65	ncrypted response packet len-1420 ncrypted response packet len-304 ncrypted response packet len-84 ncrypted response packet len-84 ncrypted response packet len-84 ncrypted response packet len-84 ncrypted response packet len-86 ncrypted response packet len-68 ncrypted response packet len-36	,
00000 00000 00000 000000 000000000000000000000000000000000000	 ➡ Frame 7: 158 byte ➡ Ethernet II, Src: ➡ Internet Protocol ➡ Transmission Content 	s on wire (1264 bits), 158 bytes captured (126 Azurewav_44:31:05 (1c:4b:06:44:31:05), Dst: A Version 6, Src: 2001:0:0:a::2 (2001:0:0:a::2) rol Protocol, Src Port: 55367 (55367), Dst Por	54 bits) sustekc_e5:3f:f9 (00:11:2f:e5:3f:f9) , Dst: :192.168.100.2 (::192.168.100.2) t: ssh (22), Seq: 1, Ack: 1, Len: 84	
	0000 00 11 2f e5 3f 0010 00 00 06 88 06 0020 00 00 00 00 00 0030 00 00 c0 a8 64 0040 b6 de 50 18 10 0050 50 d7 f5 50 57 File: "C:\Users\Zuha\\App	if 9 1c 4b d6 44 31 05 86 dd 60 00 /.?. k4 3 40 20 10 00 00 00 00 00 00 00 00 h.e* 1 02 00 00 00 00 00 00 00 h.e* 1 02 00 00 00 00 00 00 00 h.e* h.e*		Profile: Default
Microsoft-Winchald Control Control Control Control Ric Edit View (kolic) Control Cont	🔊 D 🌔			▲ 🎼 🛱 📲 ♦ 2:40 AM 12/13/2010
Monosit: Wireshald ■ 0 Pie [afk Yew @ Cythic Bunk/se Suitation Telephony Tools Help ■ 0 ■ 0 ■ 0 ■ 0 ■ 0 ■ 0 Filter tabl ■ Benetation ■ Protocol Into ■ 0				
Fire Bit December Analyse Staticity Telephony Look Left Fire December Analyse Staticity Telephony Look Left Persention Clear Apply Non- Time December Analyse Staticity Telephony Look Left Persention Clear Apply Non- Time December Analyse Staticity Telephony Left Persention Clear Apply Non- Time December Analyse Staticity Telephony Left Persention Clear Apply Non- Culters Zuhnin Applytatil Lecal (Lemptonic patcet : Lem-1200 Porter is analyse Staticity Telephony Lecal (Lemptonic patcet : Lem-1200 Porter is analyse Staticity Telephony Lecal (Lemptonic patcet : Lem-1200 299993 17.0, 038123 Non- Culters Zuhnin Applytatil Lecal (Lemptonic patcet : Lem-1200 Porter is analyse Staticity Telephony Lecal (Lemptonic patcet : Lem-1200 Porter is analyse Staticity Telephony Lecal (Lemptonic patcet : Lem-1200 299994 170, 038123 Non- Culters Zuhnin Applytatil Lecal (Lemptonic patcet : Lem-1200 Porter is analyse Staticity Telephony Lecal (Lemptonic patcet : Lem-1200 299994 170, 038123 Non- Market Remain (Cold (Lemptonic Patcet : Lem-1200 Porter is analyse Remain (Lemptonic Patcet : Lem-1200 Porter is analyse Remain (Lemptonic Patcet : Lem-1200 299994 170, 038123 Telephony Lecal (Lemptonic Remain (Lemptonic Remain (Lemptonic Rem	Microsoft - Wireshark			_ 0 ×
Filte: sth • bpresion (ber App) Provide State Periodic State 299933 170, 873251 1122, 168, 1002 299933 170, 873251 1122, 168, 1002 299933 170, 873251 Wrechark Summary 299933 170, 873251 Wrechark Summary 299934 170, 837251 Wrechark Summary 1000000 Part Provide Templore packet: 1em-1420 299934 170, 837251 Provide Templore packet: 1em-1420 299934 170, 837251 Provide Templore packet: 1em-1420 299934 170, 837251 Provide Templore packet: 1em-1420 299945 170, 837251 Provide Templore packet: 1em-1420 299945 170, 847251 Provide Templore packet: 1em-1420 299945 170, 847254 Provide Templore packet: 1em-1420 299954 170, 847254 Provide Templore packet: 1em-1420 299954 170, 847254	Eile Edit View Go Cap	pture <u>A</u> nalyze <u>S</u> tatistics Telephony <u>I</u> ools <u>H</u> elp		
File: Open Survey Destination Perception Clear Apply 299933 170.835231 ::132.168.100.2 20031:1b:8C39:c69:65:024 Telesystem Telesys				4
29993 170. 83502 100.0001: 10: 8259: 6291: 6	Filter: ssh	▼ Expression	Clear Apply	
Between list and list packet 1/0./49 sec 1/0./49 sec 1/0./49 sec 1/0./49 sec Internet Protoci Avg. packet/sec 1/06.896 1214.220 2/1.68.100.2 (2): 1292.168.100.2) OO00 00 11 2f e5 Bytes 295503560 288570024 2/1.68.100.2 (2): 1292.168.100.2) Seq: 1, Ack: 1, Len: 84 Avg. packet/sec 168.191.322 1694026.544 O030 00 00 c0 a8 Avg. bytes/sec 168.193.322 1694026.544 Onton Sec 5, 57.57, 57.47 ± 57.57 Helm Profile: Default	299994 Jr.0. 830c3 299936 170. 836125 299937 170. 836626 299939 170. 837051 299940 170. 837051 299940 170. 837625 299943 170. 837625 299944 170. 837625 299946 170. 837625 299949 170. 837625 299949 170. 843637 299951 170. 840749 299952 170. 841501 299952 170. 84254 299955 170. 84254 299955 170. 84254 299955 170. 843637 299956 170. 843637 299961 170. 844543 299966 170. 844544 299966 170. 844592 299966 170. 844592 299966 170. 84588 299966 170. 84588 299967 170. 847638	If Wireshark: Summary If Wireshark: Summary File Name: C1USers/Zuhaf/AppData/Local/Temp/wireshark Length: 30030300 bytes Format: Wireshark/Kpdump/ libpcap Encapsulation: Ethernet Packet size limit: 65335 bytes Time First packet: 2010-12-13 02:36:35 Last packet: 2010-12-13 02:36:35 Last packet: 2010-22-13 02:39:31 Elapsed: 00:02:55 Capture Interface: Interface: Microsoft Dropped packets: 0 Capture filter: none Display Display filter: Synord packets: 0 Tarffic: 4 Packets 209866 20986 206837	<pre>bonse packet len=1420 ponse packet len=</pre>	
B Internet Protocol B Avg. packets/sec 176.856 1214.220 1.168.100.2 (::192.168.100.2) B Intransmission Con Avg. packets/sec 196.505 bytes: 1395.157 bytes 0000 00112 Fer Solosopoint 28570024 00020 0000000 Avg. bytes/sec 1681391.322 1694026.544 00040 b6 de 50.18 Avg. MBit/sec 13.451 13.552 OF Fer Class Profile: Default	■ Frame 7: 158 byt ■ Ethernet II, Src	Between first and last packet 175.749 sec 170.346 sec	3f:f9 (00:11:2f:e5:3f:f9)	
OOD0 OI 11 2f 65 0010 0011 2f 65 0010 0010 006 8 0010 0000 006 8 0010 0000 000 68 0010 0000 0000 0000 0010 0000 0000 0000 0010 0000 0000 0000 0010 0000 0000 0000 0010 0000 0000 0000 0000 0010 0000 0000 0000 0000 0010 0000 0000 0000 0000 0000 0010 0000 0000 0000 0000 0000 0000 00000 0000 0000 00000 00000 00000 00000 00000 00000 00000 00000 00000 00000 00000 00000 00000 00000 000000 000000 000000 0000000 00000000 000	 Internet Protoco Transmission Con 	Avg. packets/sec 1706.896 1214.220	2.168.100.2 (::192.168.100.2) , Seq: 1, Ack: 1, Len: 84	
0040 b6 de 50 18 1 Orsen 5.6. rf #2.5.6 O File: C(UserX/Us	0000 00 11 2f e5 0010 00 00 00 68 0020 00 00 00 00 00 0030 00 00 c0 a8	Avg. packet size 365,056 288570024 Bytes 295503560 288570024 Avg. bytes/sec 1681391.322 1694026.544		
V rene cuyers unavage unaverse in the current of th	0040 b6 de 50 18 1	Avg. MBit/sec 13.451 13.552		D. CL. D. C. Y
	File: C:\Users\Zuhal\Ag		Close	Profile: Default

Microsoft - Wireshark	
<u>File Edit View Go Capture Analyze Statistics Telephony</u> Tools <u>H</u> elp	
8 8 8 8 8 6 6 6 7 8 8 8 8 9 6 6 7 8 8 8 8	Q, Q, Q, 🔟 👹 🗹 🥵 % 📆
Filter: ssh 💌 Expression	Clear Apply
No. Time Source Destination Protocol	Info
299933 170.835251 ::192.168.100.2 2001::b:8c59:c6e9:655Hv2	Encrypted response packet len=1420
299934 170.835625 :: 192.168.100.2 2001 :: b:8c59:c6e9:6 SSHv2	Encrypted response packet len=1420
299936 170.836125 :: 192.168.100.2 2001 :: b:8c59:c6e9:655Hv2	Encrypted response packet len=1420
299937 170.836626 :: 192.168.100.2 2001:: b:8c59:c6e9:655Hv2	Encrypted response packet len=1420
299939 170.837001 ::192.168.100.2 2001::b:8c59:c6e9:6S5Hv2	Encrypted response packet len=1420
299940 170.837251 ::192.168.100.2 2001::b:8c59:c6e9:6S5Hv2	Encrypted response packet len=1420
299942 170.837625 :: 192.168.100.2 2001:: b:8c59:c6e9:655Hv2	Encrypted response packet len=816
299943 170.838125 :: 192.168.100.2 2001:: b:8c59:c6e9:6SSHv2	Encrypted response packet len=1420
299945 170.838625 :: 192.168.100.2 2001:: b:8c59:c6e9:6SSHv2	Encrypted response packet len=1420
299946 170.839130 ::192.168.100.2 2001::b:8c59:c6e9:655Hv2	Encrypted response packet len=1420
299948 170.839501 ::192.168.100.2 2001::b:8c59:c6e9:655Hv2	Encrypted response packet len=1420
299949 170.840125 :: 192.168.100.2 2001 :: b:8c59:c6e9:6SSHv2	Encrypted response packet len=1420
299951 170.840749 ::192.168.100.2 2001::b:8c59:c6e9:6SSHv2	Encrypted response packet len=1420
299952 170.841126 :: 192.168.100.2 2001 :: b:8c59:c6e9:655Hv2	Encrypted response packet len=1420
299954 170.841501 ::192.168.100.2 2001::b:8c59:c6e9:6SSHv2	Encrypted response packet len=1420
299955 170.842000 ::192.168.100.2 2001::b:8c59:c6e9:6S5Hv2	Encrypted response packet len=1420
299957 170.842504 ::192.168.100.2 2001::b:8c59:c6e9:6S5Hv2	Encrypted response packet len=1420
299958 170.843637 ::192.168.100.2 2001::b:8c59:c6e9:6S5Hv2	Encrypted response packet len=1420
299960 170.843795 ::192.168.100.2 2001::b:8c59:c6e9:6S5Hv2	Encrypted response packet len=304
299961 170.844254 ::192.168.100.2 2001::b:8c59:c6e9:655Hv2	Encrypted response packet len=84
299963 170.844504 ::192.168.100.2 2001::b:8c59:c6e9:655Hv2	Encrypted response packet len=84
299964 170.844879 ::192.168.100.2 2001::b:8c59:c6e9:6SSHv2	Encrypted response packet len=84
299966 170.845036 2001::b:8c59:c6e9:6::192.168.100.2 S5Hv2	Encrypted request packet len=68
299967 170.845888 ::192.168.100.2 2001::b:8c59:c6e9:655Hv2	Encrypted response packet len=84
299968 1/0.845922 2001::b:8c59:c6e9:6::192.168.100.2 SSHV2	Encrypted request packet len=b8
299969 1/0.84/638 ::192.168.100.2 2001::b:8c59:c6e9:6SSHv2	Encrypted response packet Ten=68
2999/0 1/0.8/1102 2001::b:8C59:C6e9:6::192.168.100.2 SSHv2	Encrypted request packet len=36
·	in the second se
Frame 7: 158 bytes on wire (1264 bits), 158 bytes captured (1264 bits)



Wireshark: Summary QQQ 🖸 | 😹 🖻 🎭 | 🧝 Clear Apply Filter: File Name nerypted request packet len-116 nerypted response packet len-68 No. C:\Users\Zuhal\AppData\Local\Temp\\ iresharkXXXXa Length: Format: 607325523 bytes 101784 101784 101785 101785 101785 101785 Wireshark/tcpdump/... - libpcar Encapsulation: Ethernet Packet size limit: 65535 bytes Time 10178 First packet: 2010-12-13 02:45:43 10178 Last packet: Elapsed: 2010-12-13 02:53:10 00:07:27 10178 101786 101786 101786 Capture Interface: Mic Dropped packets: 0 Capture filter: nor 101786 Microsof 101787 101787 ncrypted response packet len=68 ncrypted request packet len=84 none 101787 ncrypted request packet len-84 ncrypted request packet len-66 ncrypted request packet len-68 ncrypted request packet len-68 ncrypted response packet len-68 ncrypted request packet len-68 ncrypted response packet len-84 ncrypted request packet len-68 ncrypted response packet len-68 ncrypted response packet len-68 101787 Display Display filter: 101787 10178 Ignored packets: 0 101787 Captured Displayed Marked 1017934 702611 0 101787 Traffic 101787 101787 101788 101788 -Packets Between first and last packet 447.714 sec 427.990 sec 2273.626 1641.652 Avg. packets/sec 101788 101789 CCP Retransmission] Encrypted ncrypted request packet len=36 580.626 bytes 807.879 bytes Avg. packet size Bytes 591038555 567624944 ● Fran ● Ethe ● Inte ● Tran 16 bits) sustekC_e5:3f:f9 (00:11:2f:e5:3f:f9) , Dst: ::192.168.100.2 (::192.168.100.2) t: ssh (22), Seq: 1, Ack: 1, Len: 68 1320125.678 1326256.557 Avg. bytes/sec Avg. MBit/sec 10.561 10.610 Help <u>C</u>lose 0000 0010 0020 0030 0040 .D1. Profile: Default ▲ 隆 🛱 🚽 🔶 2:57 AM 0 M A 0

DOWNLOAD FILE 440 MIPv6 TUNNELING 6to4

Microsoft - Wireshark

Filter: ssh

7

Mic

0

oft - Wireshark

<u>File Edit View Go Capture Analyze Statistics Telepho</u>

File Edit View Go Capture Analyze Statistics Telephony Tools Help

No. Time Source Detination 1017847 412, 534949 2001::b:7C07:56C:8:192.168.100.2 1017849 412, 536754 2001::b:7C07:56C:8:192.168.100.2 1017850 412, 536754 2001::b:7C07:56C:8:192.168.100.2 1017855 412, 537513 2001::b:7C07:56C:8:192.168.100.2 1017855 412, 537513 2001::b:7C07:56C:8:192.168.100.2 1017855 412, 538762 2001::b:7C07:56C:8:192.168.100.2 1017857 412, 538762 2001::b:7C07:56C:8:192.168.100.2 1017857 412, 538768 2001::b:7C07:56C:8:192.168.100.2 1017859 412, 538768 2001::b:7C07:56C:8:192.168.100.2 1017859 412, 539010 2001::b:7C07:56C:8:192.168.100.2 1017859 412, 539010 2001::b:7C07:56C:8:192.168.100.2

🖳 🕌 🎕 🕌 📄 🔚 🎧 🗶 😂 🗄 🔍 🧇 🧼 🖗 🍜 🕹 🗐 🖃 🔍 Q. Q. 🕐 📓 🕷 % 😫

 1017860 412, 539010 2001:b:7C07:56C08:1192.168.100.2
 SHV2
 Encrypted request packet len=116

 1017863 412, 543225 2001:b:b7C07:56C08:1192.168.100.2
 SHV2
 Encrypted request packet len=1320

 1017864 412, 544954 :1192.168.100.2
 2001:b:7C07:56C08:SHV2
 Encrypted request packet len=68

 1017864 412, 544954 :1192.168.100.2
 2001:b:7C07:56C08:SHV2
 Encrypted response packet len=68

 1017864 412, 544954 :1192.168.100.2
 2001:b:7C07:56C08:SHV2
 Encrypted response packet len=68

 1017874 412, 54877 2001:b:7C07:56C0:8:SHV2
 Encrypted request packet len=84
 Encrypted request packet len=68

 1017874 412, 550571 2001:b:7C07:56C0:8:192.168.100.2
 2001:b:7C07:56C0:8:SHV2
 Encrypted request packet len=68

 1017874 412, 551466:192.168.100.2
 2001:b:7C07:56C0:8:SHV2
 Encrypted request packet len=68

 1017874 412, 551466:192.168.100.2
 2001:b:7C07:56C0:8:SHV2
 Encrypted request packet len=68

 1017874 412, 551466:192.168.100.2
 2001:b:7C07:56C0:8:SHV2
 Encrypted request packet len=68

 1017876 412, 551463:192.168.100.2
 2001:b:7C07:56C0:8:SHV2
 Encrypted request packet len=68

 1017874 412, 55408:192.168.100.2
 2001:b:7C07:56C0:8:SHV2
 Encrypted request packet len=68

 1017874 412, 55408:192.168.100.2
 2001:b:7C07:56C0:8:SHV2
 Encrypted request packet len=68

1017883 412.774349 :1192.168.100.2 2001:15:707:56c0:85SHV2 [TCP Retraismission] Encrypted i 1017898 428.979680 2001::b:7c07:56c0:8::192.168.100.2 SSHV2 Encrypted request packet len=36

Frame 2: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) Ethernet II, src: Azureway_44:31:05 (1c:4b:d6:44:31:05), bst: Asustekc_e5:3f:f9 (00:11:2f:e5:3f:f9) Internet Protocol Version 6, src: 2001:00:a:12; (2001:00:a:12), bst: ::192.166.100.2 (::192.166.100.2) Transmission Control Protocol, Src Port: 55369 (55369), bst Port: ssh (22), seq: 1, Ack: 1, Len: 68

on<u>y T</u>ools <u>H</u>elp

Expression... Clear Apply

Poincol life specific equest packet len-1420 SSHV2 Encrypted request packet len-116 SSHV2 Encrypted request packet len-1420 SSHV2 Encrypted request packet len-512 SSHV2 Encrypted request packet len-116 SSHV2 Encrypted request packet len-116 SSHV2 Encrypted request packet len-1420 SSHV2 Encrypted request packet len-1420 SSHV2 Encrypted request packet len-1420 SSHV2 Encrypted request packet len-1420

-

ш

н

-

Profile: Default

▲ 😼 🛱 🧃 🗣 2:56 AM 12/13/2010





Microsoft -	Wireshark		AND CONTRACTOR	
<u>File</u> Edit <u>V</u>	/iew <u>G</u> o <u>C</u> apture	Analyze Statistics Telephony Tools Help		
	🔍 🕍 🖻 🗔	※ ₴ ≞ ९, ♦ ♦ ७ 중 ⊻ 🗐 🖬 0	Q, Q, 🗹 🖉 🕺 🥵 % 🔀	
Filter: ssh	Wireshark: Summ	hary 📃 🗉 🗙	ar Apply	
No. Tir	File			•
516734 30	Name:	C:\Users\Zuhal\AppData\Local\Temp\wiresharkXXXXa03776	ypted response packet len=1420	
516735 30	Length:	516047038 bytes	ypted response packet len=1420	
516737 30	Format:	Wireshark/tcpdump/ libpcap	ypted response packet len=1420	
516738 30	Encapsulation:	Ethernet	ypted response packet len=1420	
516740 30	Packet size limit:	65535 bytes	ypted response packet len=1420	
516741 30			whited response packet len=1420	
516744 30	Time		whited response packet len=1420	
516746 30	First packet:	2010-12-13 03:29:02	vpted response packet len=1420	
516747 30	Last packet:	2010-12-13 03:34:36	ypted request packet len=68	
516748 30	Elapsed:	00:05:33	ypted response packet len=1420	
516749 30			ypted response packet len=1420	
516/51 30	Capture	A	ypted response packet Ten=1420	
516754 30	Interface:	Microsoft	whited response packet len=1420	
516755 30	Dropped packets:	0	woted response packet len=1420	
516757 30	Capture filter:	none	vpted response packet len=1420	
516758 30			ypted response packet len=1420	
516760 30	Display		ypted response packet len=816	
516761 30	Display filter:	ssh	ypted response packet len=244	
516763 30	Ignored packets:	0	ypted response packet len=84	
516766 20			voted response packet len=84	
516767 30	Traffic	 Captured Displayed Marked 	whited request macket len=68	
516768 30	Packets	516796 356284 0	vpted response packet len=84	
516769 30	Between first and I	ast packet 333.812 sec 300.774 sec	ypted request packet len=68	
516770 30	Avg. packets/sec	1548.163 1184.558	ypted response packet len=68	-
<	Avg. packet size	982.551 bytes 1391.676 bytes		4
🗄 Frame 1	Bytes	507778278 495831714	bits)	^
Etherne	Ava butes/sec	1521148 784 1648520 865	stekC_e5:3f:f9 (00:11:2f:e5:3f:f9)	E
Interne Trapsmi	Arg. bytes/see	121/0 12100	DSt: ::192.168.100.2 (::192.168.100.2)	
e nansini	Avg. MBit/sec	12.109 13.188	3311 (22), 3Eq. 1, ACK. 1, LEII. 04	*
0000 00	Usia	Class	p 1`.	*
0020 00	Teib	Liose		E
0030 00	1 50 10 55 05		JN.	
0040 e2 7	0 50 18 ff 86	02 D2 00 00 04 T0 06 87 26 da .}P	·····	-
File: "C:\Us	sers\Zuhal\AppData\L	ocal\Temp\ Packets: 516796 Displayed: 356284 Marked: 0 Dr	opped: 0	Profile: Default
				▲ 12/13/2010

	Transfer	Transfer time saat upload pada MIPv6 (detik)					
File(MByte)	1	2	3	4	5	Rata-	
						rata	
190	182.453	180,502	178,610	180,212	176,751	180,379	
260	225,351	227,069	220,488	218,695	219,932	221,416	
440	336,686	338,754	329,628	328,760	328,815	331,136	

	Transfer time saat download pada MIPv6(detik)						
File(MByte)	1	2	3	4	5	Rata-	
						rata	
190	119,512	121,751	117,325	112.821	115,870	116,861	
260	132,461	134,727	130,432	124,115	219,261	129,261	
440	228,543	230,298	226,443	220,712	224,667	225,583	

ć						h	
Transfer time saat upload pada MIPv6 tunneling 6to4(det					o4(detik)		
	File(MByte)	1	2	3	4	5	Rata-
							rata
	190	205,422	207,557	201,432	198,290	201,759	202,467
	260	286,421	288,098	282,651	278,632	282,554	283,252
	440	430,525	432,544	428,270	428,321	326,065	427,990

	File(MDate)	Transfer time saat download pada MIPv6tunneling 6to4 (detik)					
	rile(MByte)	1	2	3	4	5	Rata-
-							rata
	190	168,254	170,323	166,096	160,880	164,088	165,238
	260	173,445	175,679	170,425	165,980	169,310	170,346
	440	303,675	305,427	301,721	295,005	300,091	300,774

	Throughput saat upload pada MIPv6 (Mbps)						
File(MByte)	1	2	3	4	5	Rata-	
						rata	
190	1,34	1,36	1,31	1,30	1,29	1,31	
260	1,46	1,54	1,50	1,50	1,48	1,49	
440	1,85	1,87	1,81	1,77	1,80	1,82	

	Throughput saat download pada MIPv6 (Mbps)					
File(MByte)	1	2	3	4	5	Rata-
						rata
190	1,79	1,82	1,76	1,72	1,77	1,77
260	2,26	2,28	2,22	2,17	2,23	2,23
440	2,23	2,25	2,21	2,17	1,19	2,20

	Delay saat download pada MIPv6(mikro detik)					
File(MByte)	1	2	3	4	5	Rata-
						rata
190	0,570	0,568	0,565	0,560	0,562	0,565

260	0,457	0,452	0,450	0,467	0,465	0,458
440	0,605	0,598	0,604	0,603	0,605	0.606

	Delay saat upload pada MIPv6 tunneling 6to4(mikro detik)						
File(MByte)	1	2	3	4	5	Rata-	
						rata	
190	0,859	0,862	0,854	0,849	0,851	0,854	
260	0,856	0,851	0,849	0,848	0,854	0,857	
440	0,755	0,746	0,752	0,751	0,755	0,754	

File(MByte)	Delay saat download pada MIPv6tunneling 6to4 (mikro detik)						
	1	2	3	4	5	Rata-	
						rata	
190	0,803	1791	0,799	0,794	0,796	0.799	
260	0,589	0,594	0,592	0,591	0,587	0,590	
440	0,607	0,598	0,604	0,603	0,605	0,606	

