ED151 2 ingelab ingelab Arief Wahyudin

KATA PENGANTAR

Syukur alhamdulillah Allah SWT masih memberikan nikmat kepada kita semua, sehingga saat ini masih dapat menikmati belajar dan berbagi ilmu.

Ngelab MikroTik Edisi Ke-2 adalah modul yang digunakan untuk kegiatan Ngebar Mikrotik Ke-2 pada tanggal 26 dan 27 Maret 2017. Ngelab MikroTik mengacu pada *Outline MTCNA* dan *MTCRE* yang ada di web resmi MikroTik (*www.mikrotik.com*).

Tujuan dari dibuatnya modul ini adalah untuk memudahkan peserta Ngebar MikroTik Ke-2 dalam memahami teori dan konsep dari materi *MTCNA* dan *MTCRE*, seperti materi *Model OSI Layer*, *Model TCP/IP*, *Subnetting*, IP *Address*, *Subnetting*, *Firewall*, *Wireless*, *Bridging*, *Routing*, *Tunnel*, dan *Network Management*.

Modul ini masih sangat jauh dari kata sempurna karena penyusunanya adalah hasil praktik secara mandiri, oleh karena itu saya selaku penulis modul ini sangat mengharapkan masukan untuk meningkatkan bobot dari modul ini agar kedepannya dapat diperbaiki menjadi lebih baik dan dapat membantu bagi sapa saja yang ingin belajar MikroTik.



DAFTAR ISI

I.	NETW	ORKING FUNDAMENTALS	1
	L1.1.	7 Layer OSI	2
	L1.2.	5 Layer TCP/IP	3
	L1.3.	IPv4	4
	L1.4.	Subnetting IPv4	7
II.	MIKRO	DTIK FUNDAMENTALS	10
	L2.1.	Mengakses Mikrotik	11
	L2.2.	System Identity Mikrotik	17
	L2.3.	Versi Mikrotik	19
	L2.4.	Fitur Mikrotik	20
	L2.5.	Enable dan Disable Fitur Mikrotik	20
	L2.6.	User Management	21
	L2.7.	Backup dan Restore	23
	L2.8.	Export dan Import Konfigurasi Mikrotik	24
	L2.9.	Reset Mikrotik	26
	L2.10.	IP Address Mikrotik	26
III.	FIREW	ALL	30
	L3.1.	NAT	31
	L3.2.	Firewall Logging Mikrotik	34
	L3.3.	Filter Rule	35
	L3.4.	Content	39
	L3.5.	Address List	43
	L3.6.	Layer 7 Protocols	48
	L3.7.	Transparent DNS	52
	L3.8.	Transparent Web Proxy	54
	L3.9.	Redirect	60
IV.	WIREL	ESS	61
	L4.1.	Access Point Bridge (Pemancar)	63
	L4.2.	Station (Penerima)	68
	L4.3.	Station Bridge (Penerima)	72
	L4.4.	Virtual Access Point Bridge	73
V.	BRIDG	Е	76
	L5.1.	Wired Bridge	77
	L5.2.	Wireless Bridge	80
VI.	ROUTI	NG	82
	L6.1.	Static Routing	83
	L6.2.	Dinamic Routing (RIPv2)	86
VII.	TUNNE	EL	89
	L7.1.	PPPoE Tunnel	90
VIII.	NETW	ORK MANAGEMENT	96
	L8.1.	Wireless Mac Address Filtering	97
	L8.2.	Wireless Nstreme	99
	L8.3.	Hotspot	100
IX.	NETW	ORK SIMULATION	104
	L9.1.	Instalasi Loopback Adapter GNS3 di Windows	105

LABORATORIUM 1





NETWORKING FUNDAMENTALS

L1.1. 7 LAYER OSI

Open System Interconection atau disingkat OSI adalah sebuah model yang digunakan untuk membantu desainer jaringan dalam memahami fungsi dari tiap-tiap layer yang berhubungan dengan aliran komunikasi data. *Layer OSI* adalah model arsitektural jaringan yang dikembangkan oleh Badan *International Organization of Standardization* (ISO) di wilayah Eropa pada tahun 1977.

NO	NAMA	DATA	DEVICE
7	APPLICATION	DATA	SOFTWARE
6	PRESENTATION	DATA	SOFTWARE
5	SESSION	DATA	SOFTWARE
4	TRANSPORT	SEGMEN	SOFTWARE
3	NETWORK	PAKET	ROUTER
2	DATA LINK	FRAME	SWITCH
1	PHYSICAL	BIT	HUB

Layer OSI

Model OSI secara konseptual terbagi ke dalam tujuh lapisan dimana masing-masing lapisan memiliki fungsi jaringan yang spesifik. Berikut adalah tujuh *layer* OSI :

Layer 7 Application

Layer ini menyediakan layanan untuk aplikasi pengguna, selain itu *layer* ini bertanggungjawab terhadap pertukaran informasi antara program komputer. Data pada *layer* ini berbentuk data.

Layer 6 Presentation

Layer ini menyediakan layanan pengkonversian dan pemformatan data sebelum di transfer. Layer ini membentuk kode konversi, kode translasi, dan enkripsi. Data pada layer ini berbentuk data.

• Layer 5 Session

Layer ini menentukan bagaimana dua terminal menjaga, memelihara, dan mengatur koneksi agar saling berhubungan satu sama lain. Data pada layer ini berbentuk data

• Layer 4 Transport

Layer ini membagi data menjadi segmen, menjaga koneksi logika *"end-to-end"* antar terminal, dan menyediakan penanganan *error*. Layer ini juga bertanggung jawab mencari jalur (*routing*) yang kosong untuk transmisi data. Data pada *layer* ini berbentuk segmen.

Layer 3 Network

Layer ini menentukan alamat jaringan, menentukan rute yang harus diambil selama perjalanan, dan menjaga antrian trafik di jaringan. Data pada layer ini berbentuk paket dan perangkat yang ada pada layer network adalah router. Pada Layer ini pengalamatan yang digunakan dalam bentuk desimal seperti 192.168.1.0.

Layer 2 Data Link

Layer ini menyediakan link untuk data, memaketkan data menjadi *frame* yang berhubungan dengan hardware, komunikasinya dengan kartu jaringan, mengatur komunikasi *layer physical* antara sistem koneksi dan penanganan *error*. Data pada *layer* ini berbentuk *frame* dan perangkat yang ada pada *layer* ini adalah switch. Pada *layer* ini pengalamatan yang digunakan dalam bentuk heksadesimal seperti A1-B2-C3-D3-E4-88.

• Layer 1 Physical

Leyer ini bertanggung jawab terhadap proses data menjadi bit dan mentransfernya melalui media dan menjaga koneksi fisik antar sistem. Data pada layer ini berbentuk bit dan perangkat yang ada pada layer ini adalah hub kabel kabel jaringan. Pada layer ini pengalamatan yang digunakan dalam bentuk biner seperti 11110000.

L1.2. 4 LAYER TCP/IP

Transmission Control Protocol/Internet Protocol atau disingkat TCP/IP adalah standar komunikasi data atau protocol yang digunakan dalam internet dalam proses tukar-menukar data dari satu komputer ke komputer lainnya. Protokol TCP/IP dikembangkan pada tahun 1970 hingga 1980 oleh Defense Advance Research projects Agency (DARPA).

NO	NAMA
5	APPLICATION
4	TRANSPORT
3	NETWORK
2	DATA LINK
1	PHYSICAL

Layer TCP/IP

Menurut dokumen RFC 1122 model lapisan protocol TCP/IP terdiri dari empat lapisan. Tidak seperti model OSI model TCP/IP bukan standar internasional sehingga banyak sumber yang menambahkan lapisan fisik di dalam model TCP/IP. Model TCP/IP antara lain sebagai berikut :

• Layer 5 Application

Layer ini bertanggung jawab untuk menyediakan akses kepada aplikasi terhadap layanan jaringan.

Layer 4 Transport

Layer ini bertanggung jawab menjamin data akan sampai dan berurutan ke tujuan. Jika ada data yang hilang, maka layer ini menyediakan mekanisme untuk meminta dan mengirim data ulang.

• Layer 3 Network

Layer ini bertanggung jawab mengatur perjalanan paket dari melewati banyak jaringan dengan berbagai media fisik yang berbeda. Informasi yang diberikan hanya IP address sumber dan tujuan.

• Layer 2 Data Link

Layer ini bertanggung jawab mengatur komunikasi antara dua komputer yang menggunakan saluran fisik yang sama.

• Layer 1 Physical

Layer ini bertanggung jawab menyalurkan data dari satu titik ke titik lain secara fisik.

L1.3. IPv4

IP Address versi 4 (IPv4) adalah sebuah jenis pengalamatan jaringan yang digunakan di dalam protokol jaringan TCP/IP yang menggunakan protokol IPv4. IPv4 memiliki panjang 32 bit dan dibagi menjadi 4 blok. Masing-masing blok berukuran 8 bit dan ditulis dalam bilangan desimal dengan nilai berkisar antara 0 hingga 255. IPv4 ditulis dalam notasi desimal bertitik yang dibagi ke dalam empat buah oktet dengan masing-masing berukuran 8 bit. Format notasi tersebut dikenal dengan *dotted-decimal format*.

IP Address adalah deretan bilangan biner (32 bit atau 128 bit) yang unik dan digunakan sebagai identitas untuk host dalam jaringan komputer



IP Address versi 4

a. Jenis IP versi 4 berdasarkan identitasnya

IPv4 yang dimiliki oleh sebuah *host* dapat dibagi dengan menggunakan *subnet mask* jaringan ke dalam dua buah bagian, yakni:

- 1) *Network Identifier* (NetID) atau *Network Address*. NetID adalah alamat yang digunakan khusus untuk mengidentifikasikan alamat jaringan di mana *host* berada.
- **2)** *Host Identifier* (HostID) atau *Host address*. HostID adalah alamat yang digunakan khusus untuk mengidentifikasikan alamat *host*.

b. Jenis IP versi 4 berdasarkan ketentuan penggunaanya Berdasarkan ketentuan penggunaanya IPv4 terbagi menjadi beberapa jenis, yakni sebagai berikut:

1) Alamat Unicast

Alamat *unicast* merupakan alamat IPv4 yang ditentukan untuk sebuah antarmuka jaringan yang dihubungkan ke sebuah *internetwork* IP. Alamat *unicast* digunakan dalam komunikasi *point-to-point* atau *one-to-one*. Alamat *unicast* menggunakan kelas A, B, dan C dari kelas-kelas alamat IPv4. Sebuah alamat *unicast* dibedakan dengan alamat lainnya dengan menggunakan *subnet mask*.

Alamat *unicast* dibagi menjadi dua, yaitu alamat publik dan alamat privat

 Alamat Publik Alamat publik adalah alamat-alamat yang telah ditetapkan dan berisi beberapa buah *network identifier* yang telah dijamin unik jika *intranet* tersebut telah terhubung ke *Internet*.

Alamat Privat

Alamat Privat adalah alamat IP yang berada di dalam ruangan alamat pribadi. Sebuah jaringan yang menggunakan alamat IP privat disebut juga dengan jaringan privat atau *private network*.

2) Alamat Multicast

Alamat *multicast* merupakan alamat IPv4 yang didesain agar diproses oleh satu atau beberapa *node* dalam segmen jaringan yang sama atau berbeda. Alamat multicast digunakan dalam komunikasi *one-to-many*. Alamat-alamat *multicast* IPv4 didefinisikan dalam ruang alamat kelas D dalam kelas IPv4.

3) Alamat Broadcast

Alamat *broadcast* merupakan alamat IPv4 yang didesain agar diproses oleh setiap *node* dalam segmen jaringan yang sama. Alamat *broadcast* digunakan dalam komunikasi *one-toeveryone*. Jenis-jenis alamat *broadcast* antara lain sebagai berikut :

Network Broadcast

Network broadcast IPv4 adalah alamat yang dibentuk dengan cara mengkonfigurasi semua *bit host* menjadi 1 dalam sebuah alamat yang menggunakan kelas (*classful*).

Subnet Broadcast

Subnet broadcast adalah alamat yang dibentuk dengan cara mengeset semua bit host menjadi 1 dalam sebuah alamat yang tidak menggunakan kelas (*classless*)

- All Subnets Directed Broadcast All subnets directed broadcast adalah alamat broadcast yang dibentuk dengan mengkonfigurasi semua bit-bit network identifier yang asli yang berbasis kelas menjadi 1 untuk sebuah jaringan dengan alamat tak berkelas (classless).
- Limited Broadcast
 Limited broadcast adalah alamat yang dibentuk dengan
 mengkonfigurasi 32 bit alamat IPv4 menjadi 1. Alamat ini
 digunakan ketika sebuah node IP harus melakukan
 penyampaian data secara one-to-everyone di dalam sebuah
 jaringan lokal tetapi ia belum mengetahui network identifier nya.

c. Jenis IP versi 4 berdasarkan kelasnya

Dalam RFC 791 alamat IPv4 dibagi ke dalam lima kelas.

Kelas	Oktet P	ertama	Untuk
Alamat IP	Desimal	Biner	Untuk
Kelas A	1 s.d 126	0xxxxxxx	Unicast skala besar
Kelas B	128 s.d 191	10xxxxxx	Unicast skala menengah
Kelas C	192 s.d 223	110xxxxx	Unicast skala kecil
Kelas D	224 s.d 239	1110xxxx	Multicast
Kelas E	240 s.d 255	1111xxxx	Eksperimen

d. Format Prefix IP versi 4

Dalam IPv4 sebuah alamat dapat direpresentasikan dengan menggunakan angka prefiks yang merujuk kepada *subnet mask* yang digunakan. *Prefix* adalah sebuah bagian dari IP yang memiliki nilai-nilai tetap dan menjadi bagian dari sebuah rute atau *subnet identifier*.



Format Prefix IPv4

Panjang *prefix* menentukan jumlah bit terbesar paling kiri yang membuat *prefix subnet*. Jika dalam sebuah IPv4 menggunakan *prefix* /24 maka jumlah bit 1 dari 32 bit deretan bilangan biner berjumlah 24.



Jumlah bit 1 berdasarkan prefix

L1.4. SUBNETTING (IPv4)

Subnetting adalah cara untuk menentukan jumlah penggunaan *IP* Address yang paling sesuai dengan kebutuhan atau jumlah host yang ada dalam jaringan. Ketika mendengar subnetting umumnya yang ditanyakan atau dicari adalah jumlah host per subnet, jumlah *ip* address per subnet, jumlah blok subnet, network, host, dan broadcast. Untuk menjawab pertanyaan tersebut umumnya yang digunakan adalah prefix atau netmask yang digunakan.

PREFIX	NETMASK	PREFIX	NETMASK
/8	255.0.0.0	/20	255.255.240.0
/9	255.128.0.0	/21	255.255.248.0
/10	255.192.0.0	/22	255.255.252.0
/11	255.224.0.0	/23	255.255.254.0
/12	255.240.0.0	/24	255.255.255.0
/13	255.248.0.0	/25	255.255.255.128
/14	255.252.0.0	/26	255.255.255.192
/15	255.254.0.0	/27	255.255.255.224
/16	255.255.0.0	/28	255.255.255.240
/17	255.255.128.0	/29	255.255.255.248
/18	255.255.192.0	/30	255.255.255.252
/19	255.255.224.0		

Perlu diketahui netmask diperoleh dari prefix, misal IP Address 192.168.1.0 dengan prefix 30 atau umumnya ditulis dengan 192.168.1.0/30 maka netmasknya adalah hasil dari penghitungan nilai biner dari prefix. Prefix /30 memiliki arti jumlah bit 1 dari total 32 bit IPv4 ada 30 dan jika ditulis sebagai berikut



Setelah total bit 1 tiap-tiap oktet diketahui maka dapat dilakukan konversi bilangan dari biner ke desimal

Bit ke	:	1	2	3	4	5	6	7	8
Biner	:	1	1	1	1	1	1	1	1
Desimal	:	128	64	32	16	8	4	2	1

		OKTET 1		OKTET 2		OKTET 3	OKTET 4
Biner	:	11111111		11111111	•	11111111	11111100
Desimal	:	255	•	255	•	255	252

Dari tahapan tersebut dapat diketahui bahwa netmask dari 192.168.1.0/30 adalah 255.255.255.252

Setelah mengetahui prefix dan Netmask maka dapat digunakan untuk mengetahui jumlah *ip address*, jumlah *host address, network*, dan *broadcast*. Berikut adalah cara untuk menentukan ip address, jumlah host, network, dan host pada IPv4 kelas C

IP Address 192.168.1.1/30 Netmask 255.255.255.0

Jumlah IP Address adalah 256 dikurangi nilai desimal oktet ke-4 256 – 252 = 4 IP Address

Jumlah Host Address adalah jumlah IP Address dikurangi 2, 2 adalah IP Address Network dan dan IP Address Broadcast. 4 – 2 = 2 Host Address

Blok subnet adalah urutan IP Address sesuai jumlah IP Address, Blok Subnet Ke-1nya adalah

IP Address Ke-1 192.168.1.0 IP Address Ke-2 192.168.1.1 IP Address Ke-3 192.168.1.2 IP Address Ke-4 192.168.1.3

Network Address adalah IP Address yang paling atas atau pertama, jadi Network Address adalah 192.168.1.0

Broadcast Address adalah IP Address yang paling bawah atau terakhir, jadi Broadcast Address adalah 192.168.1.3

LABORATORIUM 2





MIKROTIK FUNDAMENTALS

L2.1. MENGAKSES MIKROTIK

Perlu Anda ketahui ada banyak cara untuk mengakses Mikrotik, berikut adalah daftar cara mengakses MikroTik,

NO	VIA	KONEKSI	TEXT	GUI	IP
1	WinBox	Sistem Operasi	✓	\checkmark	\checkmark
2	WinBox (MAC)	Layer 2	✓	~	-
3	Web	Layer 3	~	~	~
4	Telnet (CMD/PuTTy)	Layer 3	✓	-	\checkmark
5	Telnet (MAC)	Layer 2	✓	-	-
6	SSH (PuTTy)	Layer 3	~	-	~

Yang perlu Anda lakukan sebelum menghubungkan *Routerboard* (RB) Mikrotik ke Komputer adalah memastikan *IP Address* pada Komputer Anda dalam keadaan kosong atau *obtain*.

Ethe	thernet	Properties				\rightarrow	<	
1	nternet P	rotocol Version 4 (TCP/IP	Pv4) Pr	opertie	es			×
	General	Alternate Configuration						
	You can this cap for the a	get IP settings assigned au ability. Otherwise, you nee appropriate IP settings.	utomat d to as	ically if k your i	your n netwo	ietwork s rk admini	upports strator	
) Ob	tain an IP address automat	tically					
	OUs	e the following IP address:					_	
	IP ad	dress:		1.1	1.	1.1		
	Subn	et mask:		1.1	1.			
	Defa	ult gateway:						
	() Ob	tain DNS server address au	utomat	ically				
	OUs	e the following DNS server	addres	ses:				
	Prefe	rred DNS server:						
	Alteri	nate DNS server:		1.1		1.1		
	Va	alidate settings upon exit				Adva	inced	
					ОК		Cance	1

Ethernet Properties dalam kondisi obtain

Setelah itu Anda hubungkan komputer ke RB (*Ether 2*) seperti topologi berikut ini dengan menggunakan kabel UTP tipe *straight*.



Topologi Konfigurasi Mikrotik

Secara otomatis atau *default configuration ether 2* pada RB sudah dikonfigurasi menjadi DHCP *Server*. IP *Pool* yang diberikan kepada *client* atau komputer yang terhubung dengan RB mulai 192.168.88.2 hingga 192.168.88.254.

Property	Value
Connection-specific DN	
Description	Realtek PCIe GBE Family Controller
Physical Address	
DHCP Enabled	Yes
IPv4 Address	192.168.88.254
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Friday, January 27, 2017 1:02:16 PM
Lease Expires	Friday, January 27, 2017 1:12:15 PM
IPv4 Default Gateway	192.168.88.1
IPv4 DHCP Server	192.168.88.1
IPv4 DNS Server	192.168.88.1
IPv4 WINS Server	
NetBIOS over Tcpip En	Yes
Link-local IPv6 Address	fe80::657b:3571:a1a7:5dea%8
IPv6 Default Gateway	
ID C DNC C	

IP Address Ethernet Komputer Yang diperoleh dari RB MikroTik

Selain itu *IP Address Ether* 2 pada RB juga memiliki IP *Address default* yang juga menjadi *Gateway* yaitu 192.168.88.1

Pertama Anda dapat mengakses Mikrotik dengan menggunakan Aplikasi WinBox. Aplikasi WinBox dapat diperoleh langsung dari situs mikrotik.com atau dapat juga diperoleh dari RB MikroTik.



Icon Aplikasi WinBox

Selanjutnya Anda jalankan Aplikasi WinBox dan masukkan *IP Address, login,* dan *password default* yang digunakan Mikrotik.

NGELAB MIKROTIK

WinBox v3.7	7 (Addresses)					-		×
File Tools								
Connect To:	192.168.88.1					🗸 Kee	p Passwo	rd
Login:	admin					🗌 Оре	en In New	Window
Pageword						=		
	Add/Set		Connect To F	RoMON	Connect			
A A Maria								
Managed Neigr	1Dors							
Refresh						Find	all	Ŧ
MAC Address	✓ IP Address	Identity	Version	Board				•
	192.168.88.1	MikroTik	6.38 (sta	RB951	G-2HnD			
1 item								

Winbox Mikrotik

Secara defaul *username* yang digunakan pada Mikrotik adalah "admin" dan password yang digunakan adalah kosong atau tanpa password.

Setelah *ip address, username,* dan *password* dimasukkan langkah selanjutnya menekan tombol *Connect*.

Sadmin@192.168.88.1	(MikroTik) - WinBox v6.38 on RB951G-2HnD (mipsbe)	_	\times
Session Settings Das	nboard		
Safe Mode	Session: 192.168.88.1		
CAPsMAN CAPsMAN Interfaces Wireless OpenFlow MPLS OpenFlow Gueues Files Log Queues Files Log Radius Yools New Terminal New Terminal New Terminal New Terminal	RouterOS Default Configuration The following default configuration has been installed on your router: FourterMode: WAN port is protected by firewall and enabled DHCP client Wireless interfaces are part of LAN bridge 'P address 192.168.88.1/24 is set on LAN port Wan I Configuration: mode: ap-bridge; band: 2ghz/b/g/n; ht-chains: 0,1; ht-extension: 2U/4/Ohnhz-Ce; LAN Configuration: switch group: ether2 (master), ether3, ether4, ether5 DHCP Server: enabled; DNS: enabled; WAN (gateway) Configuration: gateway: ether1 ; firewall: enabled; NAT: enabled; Remove Configuration Show Script OK		

Jendela Konfigurasi Mikrotik melalui WinBox

Anda juga dapat mengakses MikroTik menggunakan *web browser* atau dikenal dengan *webfig (web configuration)*. Caranya dengan memasukkan *IP Address* MikroTik pada *browser* dan memasukkan *username* dan *password* lalu menekan tombol *Login*.

RouterOS v6,38	Mikro Tik	
You have connected to a router. Administrative access only. If this device is not in your possession, pleas WebFig Login: Login: admin Login Password:	e contact your local network administrator.	
Works Telef Ergen Letter Me		
	© mikrotik	

Halaman Login MikroTik pada Browser

Image: Section of the Research	MikroTik - Quick Se	et at ad ×						A	σ	×
WebFig v6.38 (stable) CAMMAN Network Stame March 10	← → C □ 19	2.168.88.1/webfig/							\$	≡
I. CARRAIN. Homma AP Quick Set Workings Homma AP Quick Set Workings Micro Ta-ZdoFT Address Aquination Static & Automatic PPoE Binder Association Static & Automatic PPoE Address Aquination Static & Automatic PPoE Binder Association Static & Automatic PPoE Beanse Research Binder Association Static & Automatic PPoE Beanse Research Binder Association Static & Automatic PPoE Beanse Research Binder Association Mick Address & Ext BOLIC / 4 of /F1 Hok Address & Ext BOLIC / 4 of /F1 Hok Address & Ext BOLIC / 4 of /F1 Binder Access List (ACL) Image Access List (ACL) Image Access List (ACL) Image Access List (ACL) Totals Uter Access List (ACL) Image Access List (ACL) Image Access List (ACL) Image Access List (ACL) Totals Uter Access List (ACL) Image Access List (ACL) Image Access List (ACL) Image Access List (ACL) Total Uter Access List (ACL) Image Access List (ACL) Image Access List (ACL) Image Access List (ACL) Mick External Guest Hetwork Uter Access List (ACL) Image Access List (ACL) Image Access List (ACL)	A Quick Set						WebFig	v6.38 (stable	1 -
I wries I wries <thi th="" wries<=""> <th< td=""><td>CAPSMAN</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>·</td></th<></thi>	CAPSMAN									·
Bitterings Bitteri	1 Wireless						Hom	e AP	Quick Se	st.
Bit Program Mikro Tk. 740FT Address Acquisition Static * Automatic PPPOE Whah Program (no. country, set ~ with Acdress Branden Branden Branden Openfion Country Mikro Tk. 740FF1 Branden Branden Branden Openfion Country Mikro Tk. 740FF1 Branden Branden Branden Openfion Country Mikro Tk. 740FF3 Heat make Branden Branden Openfion Country Mikro Tk. 740FF3 HAC Address E4 8D 8C 74 0F EC Ponde Freewalt Router Freewalt Router E4 8D 8C 74 0F EC Ponden Wiff Password ~ Log Log Tools Wiff Password ~ Wiff Password Log Ponden Guest Network Router Brewalt Router E0 8D 8C 74 0F EC Ponden Guest Network Router Brewalt Router E0 8D 8C 74 0F EC Ponden Guest Network Router Brewalt Router E0 8D 8C 74 0F EC Ponden Guest Network Router Brewalt Router E0 8D 8C 74 0F EC Ponden Guest Network Router Brewalt Router Brewalt Router Whee Router Wireless Clients Brewalt Router Brewalt Router Wireless Tin ACL Last IP Wireless Ro	🛲 Interfaces									
Bit Bridge Solution Milko Tik - 24FF1 Milko Tik - 24FF1 Solution Frequency ado In Milko Tik - 24FF1 With a Frequency ado In Milko Tik - 24FF1 With a Band 20H2 - 80:0N * In Milko Tik - 24FF1 With a Band 20H2 - 80:0N * In Milko Tik - 24FF1 With a Band 20H2 - 80:0N * In Milko Tik - 24FF1 Operfore Country In Country on Country of * In Milko Tik - 24FF1 Operfore Country In Country of * In Milko Tik - 24FF1 Operfore Country In Country of * In Milko Tik - 24FF1 Operfore Country In Country of * In Milko Tik - 24FF1 Operfore Country In Country of * In Milko Tik - 24FF1 Operfore Country In Country of * In Milko Tik - 24FF1 Operfore With Password Frequency In Milko Tik - 24FF1 In Mac Address Labor Critic Milko Tik - 24FF1 In Milko Tik - 24FF1 In Mac Taddeesing With Passe In Milko Tik - 24FF1 <td>C PPP</td> <td></td> <td></td> <td></td> <td>Wireless</td> <td></td> <td></td> <td></td> <td>Interne</td> <td>t l</td>	C PPP				Wireless				Interne	t l
Witch Network Rame Ninco (k-/4)PF1 Address Acquisition Static * Automatic PPPOE Witch Frequency adio * Main Static * Automatic PPPOE Witch Frequency adio * Main Static * Automatic PPPOE Witch Band 20045400.0* Ninco (k-/4)PF1 Ninco (k-/4)PF2 Witch Band 20045400.0* Ninco (k-/4)PF2 Rubring * MAC Address E4.80.80(7) Static * Automatic PPPOE Rubring * MAC Address E4.80.80(7) Static * Automatic PPPOE Rubring * Witch Password * Inco (k-/4)PF2 Mac Address Local Network Note Access List (ACL) - Witchess Class Network Prevail Router Class Network Tool * Witch Password * Inco (k-/4)PF2 Mac Address Local Network Mere Termank Guest Network * Outch Password * Inco (k-/4)PF2 Mere Termank Guest Network * Witchess Class Network DHCP Secret # Mere Termank Guest Network * Witchess Class Network DHCP Secret # Mere Termank Static * Automatic VPN * Med Rauwor In ACL Last IP Signal Strength Nat	🔀 Bridge				The clear				incente	÷
Image Prequency ado Image Renew	🛫 Switch	Network Name	MikroTik-740FF1			Address Acquisition	Static Automatic PPPe	θE		
Band 2014:B4:01 Bell 2014:B4:01 Bell VINUS Band 2014:B4:01 Bell Gareway Status Gareway Gareway Gareway Status Band Country Inc.country_stet Gareway Status MAC Address E480.06:74:0F.P1 MAC Address E480.06:74:0F.P2 Baddin Use Access Lut (ACL) Image: Status Freewall Router Image: Status Passe Use Access Lut (ACL) Image: Status Image: Status Image: Status Tool Image: Status Image: Status Image: Status Image: Status Passe VIFI Password Image: Status Image: Status Image: Status Image: Status Garest Network Image: Status Image: Status Image: Status Image: Status Image: Status Image: Status Image: Status Image: Status Image: Status Image: Status Image: Status Image: Status Image: Status Image: Status Image: Status Image: Status Image: Stat	°C Mesh	Frequency	auto	▼ MHz		IR Address		Denew	Delegen	
Units Band 2015-8/0 N Itelmask Openflow Country nc_country_set Gateway © yother MAC Address 6480.407.40F.FZ © yother WHE Access 114.404.404.740F.FZ © gradue WHE Access 112.108.81.1 © field Country 0HCP Server © hertdon Guest Network DHCP Server Range © Herd Room Wireless Clients DHCP Server Range Wireless Tin ACL Last IP Uptime Wireless Clients UPAC UPAC Wireless Tin ACL Last IP Uptime Wireless Clients UPAC UPAC Wireless Tin ACL Last IP Uptime Wireless Tin ACL Last IP Uptime Wireless UPAC UPAC	👜 IP 🔹 🕨					IF Address		Kellew	Kelease	4
Operation Gastrow Gastrow © Strate NAC Address E4805(724:0F/2) © Strate NAC Address E4805(724:0F/2) © Strate Use Access List (ACL) Image: Strate Access List (ACL) © Tools WIF1 Password Friewall Router © Reading WIF1 Password Image: Strate Access List (ACL) © Tools WIF1 Password Image: Strate Access List (ACL) © Reading WIF1 Password Image: Strate Access List (ACL) © Reading WIF1 Password Image: Strate Access List (ACL) © Reading WIF2 Access List (ACL) Image: Strate Access List (ACL) © Reading WIF2 Access List (ACL) Image: Strate Access List (ACL) © Reading WIF2 Access List (ACL) Image: Strate Access List (ACL) © Reading WIF2 Access List (ACL) Image: Strate Access List (ACL) © Reading Image: Strate Access List (ACL) Image: Strate Access List (ACL) © Reading Image: Strate Access List (ACL) Image: Strate Access List (ACL) © Reading Image: Strate Access List (ACL) Image: Strate Access List (ACL) <	Ø MPLS 🕨	Band	2GHz-B/G/N 🔻			Netmask				
R Rodig Lateral y Lateral y © Stratem MAC Address E480.8C.74.9F.EC © Varies B180.0C.74.9F.EC © Varies Use Access List (ACL) Firewall Router © Varies WirF Password Image: Comparison of the strategy © Parties WirF Password Image: Comparison of the strategy © Parties Coust Network Coust Network © Parties Guest Network OHCP Server @ Nake Support.nf OHCP Server Ramege 192.168.88.1 Wireless Clients DHCP Server @ OHCP Server @ MAC Address In ACL Last IP Uptime Stignal Strength Nat Wireles The Nat @ OHCP Server Ramege 192.168.88.10.1192.1108.88.25 © Parties In ACL Last IP Uptime Stignal Strength Nat @ Wireles The Nat @ OHCP Server Ramege 192.168.88.10.1192.1108.88.25 © Parties In ACL Last IP Uptime Stignal Strength Nat @ Wirelew Constructure VPN Constructure VPN © Partie Strende UPren UPren	OpenFlow	Country	no country set	•		6-t				
Bit AC Address Bit AC Address Bit AC Address E 4 I/D - 0.7 4/9 E C. Bit AC Address Bit AC Address E 4 I/D - 0.7 4/9 E C. E 4 I/D - 0.7 4/9 E C. Bit AC Address Bit AC Address E 4 I/D - 0.7 4/9 E C. Friewall Router I/D - 0.7 4/9 E C. Bit AC Address Use Access List (ACL) I/D - 0.7 4/9 E C. I/D - 0.7 4/9 E C. I/D - 0.7 4/9 E C. Tools WIF1 Password WIF1 Password WIF2 Access I/D - 0.7 4/9 E C. I/D - 0.7 4/9 E C. Tools WIF1 Password WIF2 Access I/D - 0.7 4/9 E C. I/D - 0.7 4/9 E C. Mark Fallework WIF2 Access I/D - 0.7 4/9 E C. I/D - 0.7 4/9 E C. I/D - 0.7 4/9 E C. WIF2 Access I/D - 0.7 4/9 E C. WIF2 Access I/D - 0.7 4/9 E C. WIF2 Access I/D - 0.7 4/9 E C. WIF2 Access I/D - 0.7 4/9 E C.	😹 Routing 🛛 🕨	Country	no_country_set			Gateway				
Butch Firewall Router Image: Constraint of the constraint of t	System	MAC Address	E4:8D:8C:74:0F:F1			MAC Address	E4:8D:8C:74:0F:EC			
ØR Addus Uter Access Lut (ACL) Friewall Router Friewall Router I Vitri Password Vitri Password LOcal Network Local Network Local Network Ibig WIFF Access 192 168 86 1 Local Network Local Network Ibig WIFF Access 192 168 86 1 Local Network Local Network Ibig Guest Network WIFF Server Ø Local Network DICP Server Range 192 168 86 10-192 168 86 25 WIRef Statustion WIRef Statustion DICP Server Range 192 168 86 10-192 168 86 25 UPUN WIRef Statustion In ACL Last 1P Uptime Stagad Strength NAT C WIRef Statustion In ACL Last 1P Uptime Stagad Strength UPN C VPN WIRef Statustion In ACL Last 1P Uptime Stagad Strength NAT C VPN WIRef Statustion In ACL Last 1P Uptime Stagad Strength NAT VPN WIRef Statustion WIRef Statustion VPN C VPN VPN	🙅 Queues									
Note With Password Local Network Inter Impact Local Network New Fernion Guest Network IP Address New Support Guest Network DICP Server Range Node DICP Server Range 102:168.81.01:02:168.82.23 Dice Server Range 102:168.81.01:02:168.82.23 VPN Operation Sint Upma Signal Strength Upma Strength Internet VPN Operation Sint Upma Signal Strength Winder Upma Control Upma	🥵 Radius	Use Access List (ACL)				Firewall Router	2			
Inters Log LOCal NetWork Log WPS Accept IP Address 192.158.81.1 If the Forminal Guest Network Beta Control DHCP Server 0HCP Server Make Support Wireless Clients DHCP Server Range 192.158.88.1 Make Support Wireless Clients DHCP Server Range 192.158.88.08.25 Make Support Wireless Clients DHCP Server Range 192.168.88.02.55 Wireless Clients Uptime Signal Strength Wireless Clients Uptime Signal Strength Wireless Clients Uptime Uptime Wireless Clients Uptime Signal Strength Wireless Clients Uptime Uptime Wire	🔀 Tools 🔹 🕨	WiFi Password	-							. I I I
Lisp WES Accept IP Address 192 168.81 New Terminal Guest Network CSS 255 0 (24) • Med Support CSS 255 0 (24) • Med Support MICP Server Range 192 168.86 10-192 168.88 25 Med Renu Wireless Clients DHCP Server Range 192 168.88 10-192 168.88 25 Med Renu Wireless Clients DHCP Server Range 192 168.88 10-192 168.88 25 Med Renu Wireless Clients DHCP Server Range 192 168.88 10-192 168.88 25 Med Renu Wireless Clients DHCP Server Range 192 168.88 10-192 168.88 25 Wireless Renu Wireless Clients DHCP Server Range 192 168.88 10-192 168.88 25 Wireless Renu Wireless Clients DHCP Server Range 192 168.88 10-192 168.88 25 Wireless Renu Wireless Clients DHCP Server Range 192 168.88 10-192 168.88 25 Wireless Renu Wireless Clients DHCP Server Range 192 168.88 10-192 168.88 25 Wireless Renu Wireless Clients DHCP Server Range 192 168.88 10-192 168.88 25 Wireless Renu Wireless Renu Wireless Renu 192 168.88 10-192 168.88 25 Wireless Renu Wireless Renu Wireless Renu 192 168.88 10-192 168.88 25 Wireless Renu Wireless Renu Wireless Renu 192 168.88 1	📄 Files							Local	Network	×
Item reminal SP HeadsOUTS Course Network Course Network Network Course Network DHCP Server 255,255,01(24) • P Hate Support If with de Support If with de Support If with de Stand With de Stand MAC Address In ACL Last IP Uptime Signal Strength NAT Image: Signal Strength NAT Image: Signal Strength Uptime Signal Strength Uptime VPRO Image: Signal Strength Image: Signal Strength Uptime VPRO Image: Signal Strength Uptime VPRO Image: Signal Strength	E Log				WPS Accept	IP Address	192.168.88.1			
MatchalorTER Guest Network DitCP Server Metmask Cos 25, 25, 81 (24) Cos Partision Guest Network DitCP Server Bit DitCP Server Bit Make Support Wireless Clients DitCP Server Range 192:168.88.10-192:168.88.25 MAC Address In ACL Last IP Uptime Signal Strength Nat C Make Renu Wireless Clients Uptime Signal Strength Uptime VIP Virel Assession VPM Access VPM Access VPN Virel Assession VPM Access VPM Access VPN	Mew Terminal									
Image: Particing in the system of the sy	MetaROUTER			Gue	st Wireless Network	Netmask	255.255.255.0 (/24)			
Make Support DHCP Server Range 102 168.08.01-192 168.08.25 Wireless Clients DHCP Server Range 102 168.08.01-192 168.08.25 Wireless Ranu Wireless Clients NAT Wireless Ranu Signal Strength NAT Make Ranu Uptume Signal Strength VPNA Uptume VPNA Oragin Strength UPNP Winder Ranuel VPNA Winder Ranuel VPNA Winder Ranuel VPNA	🌔 Partition	Guest Network	•			DHCP Server				
Windo Wireless Clients DHCP Server Range 192:163.88:10-192:168.80.25 # Rddo MAC Address In ACL Last IP Uptime Signal Strength Wireless Science UPwP Image: Clience UPwP Wireless Science VPN UPwP Wireless Science VPN Access VPN Access	📮 Make Supout.rif						[
Mile Red MAC Address In ACL Last IP Uptime Signal Strength NAT Ø Winder Reserveds	< Undo				Wireless Clients	DHCP Server Range	▲ 192.168.88.10-192.168.88.25			
WHide Resources UPwp WHide Resources VPN Z Design Skin VPN Access Windox Windox	A Redo	MAC Address	In ACL Last IP	Uptime	Signal Strength	NAT				
IMI de Bassavido UPinP VER Statistico VPN P Statistico VPN Access @ Window Window	🜪 Hide Menu									
P Safe Node VPN Z Design Skin VPN Access @ Hanual WH0 Access	···· Hide Passwords					UPnP				
<u>C</u> Design Skin VPN <u>P</u> Hanul <u>VPN Access <u>Windox <u>Windox </u> </u></u>	🕈 Safe Mode								VDA	
Image: WinBox VPN Access	🔀 Design Skin								VPr	N
WinBox	😭 Manual					VPN Access				
	(WinBox					unar a damas				

Jendela konfigurasi MikroTik via Browser

Anda juga dapat mengakses Mikrotik menggunakan Telnet. Telnet sendiri dapat diakses menggunakan *Command Prompt* pada Sistem Operasi Windows dan juga aplikasi *PuTTy*.

Sebelum mengakses Mikrotik menggunakan Telnet melalui *Command Prompt* pastikan terlebih dahulu aplikasi telnet sudah aktif dengan cara masuk ke *Windows Features* dan memastikan *Folder Telnet* (*Client/Server*) dalam kondisi centang.



Jendela Windows Features

Selanjutnya buka *Command Prompt* dan menuliskan "telnet 192.168.88.1" dan menekan *enter*.



Telnet pada Coommand Prompt

Telnet 192.	168.88.1									-		×
												^
MMMM M	MMM	KKK						TTTTTTTTTTT		KKK		
MMM MMMM	MMM III	KKK	KKK	RRRR	RR	000	000	TTT	III	KKK	KKK	
MMM MM	MMM III	KKKR	(K	RRR	RRR	000	000	TTT	III	KKK	KK	
MMM	MMM III	KKK	KKK	RRRR	RR	000	000	TTT	III	KKK	KKK	
MMM	MMM III	KKK	KKK	RRR	RRR	000	000	TTT	III	KKK	KKK	
MikroTik [?]	MikroTik RouterOS 6.38 (c) 1999-2016 http://www.mikrotik.com/											
command [?]	Giv	ves hel	lp on	the c	omman	d and	list	of argumen	ts			
[Tab]	ab] Completes the command/word. If the input is ambiguous, a second [Tab] gives possible options											
	Mot	ve up t	o bas	e lev	e 1							
	Mot	re up c	one le	vel								
/command	Use	comma	and at	the 1	base	level						
[admin@Mikr	oTik] >											

Jendela konfigurasi Mikrotik dengan Telnet

Sedangkan aplikasi selain *Command Prompt* yang dapat digunakan untuk mengkonfigurasi Mikrotik via Telnet dapat menggunakan aplikasi PuTTy



Icon Aplikasi PuTTy

Anda cukup menjalankan Aplikasi **PuTTy** lalu memasukkan *IP* Address yang digunakan Mikrotik pada **Hostname** dan memilih **Telnet** pada *radio button Connection type* dan menekan tombol **Open**.



Mengakses Mikrotik via Telnet dengan PuTTy



Telnet pada PuTTy

P 192.168.88	.1 - Pu1	ГТҮ									-		×
													^
1000/													
MMMM I			KKK								KKK		
MMM MMMM	MMM	III	KKK	KKK	RRRR	IRR	000	000	TTT	III	KKK	KKK	
MMM MM	MMM	III	KKKI	ΚK	RRR	RRR	000	000	TTT	III	KKKF	CK .	
MMM	MMM	III	KKK	KKK	RRRR	RR	000	000	TTT	III	KKK	KKK	
MMM	MMM	III	KKK	KKK	RRR	RRR	000	000	TTT	III	KKK	KKK	
MikroTik	Rout	erOS	6.38	(c) 1	.999-2	016		http	://www.miki	otik.c	:om/		
[2]		Give	a the	liat	ofa	vaila	ble c	ommar	nda				
command [?]	1	Give	s hel	n on	the c	ommar	nd and	list	t of aroume	ents			
									3				
[Tab]		Comp	letes	the sthe	comma	nd/wo	ord. I	f the	e input is	ambigu	lous,		
		a se	cond	[Tab]	give	s pos	ssible	opt	ions				
/		Move	up t	to bas	e lev	el							
		Move	upo	one le	vel								
/command		Use	comma	and at	: the	base	level						
[admin@Miku	roTik] >											\sim

Jendela konfigurasi Mikrotik dengan Telnet

Anda juga dapat mengakses Mikrotik melalui SSH menggunakan *PuTTy*. Caranya hampir sama dengan *Telnet* hanya mengganti *Connection Type* dari *Telnet* menjadi *SSH*.

Not the American Configuration		×
Category:		
Session	Basic options for your PuTTY se	ession
Logging	Specify the destination you want to conne	ect to
	Host Name (or IP address)	Port
Bell	192.168.88.1	22
Features	Connection type:	
- Window	◯ Raw ◯ Telnet ◯ Rlogin	H O Serial
Window Appearance Behaviour Translation Selection Colours Ornection Data Proxy Telnet Rlogin SSH SSH Serial	Load, save or delete a stored session Saved Sessions Default Settings	Load Save Delete
About	Open	Cancel

Mengakses MikroTik via Telnet dengan PuTTy

L2.2. SYSTEM IDENTITY MIKROTIK

System Identity atau lebih umum dikenal dengan *hostname* adalah nama dari perangkat MikroTik. *System Identity* pada MikroTik dapat digunakan sebagai pembeda perangkat satu dengan perangkat lainnya. Perlunya untuk mengubah *default system identity* agar ketika melakukan konfigurasi RB dengan jumlah banyak tidak terjadi kesalahan konfigurasi RB satu dengan RB lainnya. Jika Anda ingin mengubah *hostname* Mikrotik melalui WinBox caranya klik **System** lalu klik **Identity**.

Identity	
Identity: MikroTik	ОК
	Cancel
	Apply

Hostname default dari Mikrotik

Setelah mengubah *hostname default* dengan *hostname* yang baru klik **OK**.

Identity	
Identity: ATSWA	ОК
	Cancel
	Apply

Hostname diubah menjadi ATSWA

L2.3. VERSI MIKROTIK

Anda dapat mengetahui versi MikroTik dengan cara klik **System** lalu klik **Resource**.

Resources		
Uptime:	00:01:45	ОК
Free Memory:	105.7 MiB	PCI
Total Memory:	128.0 MiB	USB
CPU:	MIPS 74Kc V4.12	CPU
CPU Count:	1	IRQ
CPU Frequency:	600 MHz	
CPU Load:	0 %	
Free HDD Space:	97.4 MiB	
Total HDD Size:	128.0 MiB	
Sector Writes Since Reboot:	688	
Total Sector Writes:	79 588	
Bad Blocks:	0.0 %	
Architecture Name:	mipsbe	
Board Name:	RB951G-2HnD	
Version:	6.38 (stable)	
Build Time:	Dec/30/2016 11:33:56	
Factory Software:		

Jendela Resources pada WinBox Mikrotik

Selain dapat melihat versi dari sistem operasi Anda juga dapat melihat konsumsi system yang berjalan terhadap memory dan processor, kapasitas storage, arsitektur yang digunakan sistem operasi, serta seri motherboard.

L2.4. FITUR MIKROTIK

Anda dapat melihat fitur atau paket yang ada pada Mikrotik pada Jendela *Package List*. Caranya klik menu *System* lalu klik *Packages*.

Package List						
Check For Up	dates Enab	le Disable Unin	stall Unschedule I	Downgrade	Check Installation	Find
Name /	Version	Build Time	Scheduled			-
advanced-tools	6.38	Dec/30/2016 11:33:56				
🗃 calea	6.38	Dec/30/2016 11:33:56				
🖨 dhcp	6.38	Dec/30/2016 11:33:56				
🖨 gps	6.38	Dec/30/2016 11:33:56				
hotspot	6.38	Dec/30/2016 11:33:56				
₿ ipv6	6.38	Dec/30/2016 11:33:56				
🖨 lcd	6.38	Dec/30/2016 11:33:56				
🗃 te	6.38	Dec/30/2016 11:33:56				
🗃 mpls	6.38	Dec/30/2016 11:33:56				
multicast	6.38	Dec/30/2016 11:33:56				
🗃 ntp	6.38	Dec/30/2016 11:33:56				
openflow	6.38	Dec/30/2016 11:33:56				
🗃 ppp	6.38	Dec/30/2016 11:33:56				
routing	6.38	Dec/30/2016 11:33:56				
security	6.38	Dec/30/2016 11:33:56				
🗃 system	6.38	Dec/30/2016 11:33:56				
tr069-client	6.38	Dec/30/2016 11:33:56				
🖨 ups	6.38	Dec/30/2016 11:33:56				
🖨 user-manager	6.38	Dec/30/2016 11:33:56				
wireless	6.38	Dec/30/2016 11:33:56				
20 items						

Jendela Package List pada WinBox Mikrotik

Pada Jendela *Package List* Anda dapat melihat paket yang aktif dan terinstal pada sistem operasi Mikrotik, versi paket, serta tanggal paket tersebut di install.

L2.5. ENABLE DAN DISABLE FITUR MIKROTIK

Anda dapat mengaktifkan dan menonaktifkan Fitur dalam Mikrotik sesuai kebutuhan. Selain itu tujuannya agar mengurangi konsumsi dari sistem operasi terhadap *memory* dan *processor*. Cara menonaktifkan atau *disable* fitur dengan cara masuk ke *Package List* terlebih dahulu lalu memilih paket yang akan di disable dan klik menu *Disable*. Setelah di disable *reboot* Mikrotik dengan cara klik *System* lalu klik *Reboot*.

NGELAB MIKROTIK

ackage List							
Check For Up	odates Ena	able Disable	e Unins	stall Unschedule	Downgrade	Check Installation	Find
Name /	Version	Build Time		Scheduled			
advanced-tools	6.38	Dec/30/20	16 11:33:56				
🗃 calea	6.38	Dec/30/20	16 11:33:56				
🖨 dhcp	6.38	Dec/30/20	16 11:33:56				
🗃 gps	6.38	Dec/30/20	16 11:33:56				
hotspot	6.38	Dec/30/20	16 11:33:56				
€ipv6	6.38	Dec/30/20	16 11:33:56				
@lcd	6.38	Dec/30/20	16 11:33:56				
🗃 lte	6.38	Dec/30/20	16 11:33:56				
🗃 mpls	6.38	Dec/30/20	16 11:33:56				
@ multicast	6.38	Dec/30/20	16 11:33:56				
🖨 ntp	6.38	Dec/30/20	16 11:33:56				
@ openflow	6.38	Dec/30/20	16 11:33:56				
@ppp	6.38	Dec/30/20	16 11:33:56				
@ routing	6.38	Dec/30/20	16 11:33:56				
@ security	6.38	Dec/30/20	16 11:33:56				
@ system	6.38	Dec/30/20	16 11:33:56				
tr069-client	6.38	Dec/30/20	16 11:33:56				
🗃 ups	6.38	Dec/30/20	16 11:33:56				
user-manager	6.38	Dec/30/20	16 11:33:56				
@ wireless	6.38	Dec/30/20	16 11:33:56				

Disable paket ipv6

Untuk mengaktifkan atau *enable* paket caranya kurang lebih sama hanya saja menu yang dipilih adalah *Enable*. Setelah itu *reboot* kembali mikrotik sama seperti seperti proses sebelumnya.

Check For Up	dates En	able Disable Uni	nstall Unschedule	Downgrade	Check Installation	Find
Name /	Version	Build Time	Scheduled			
advanced-tools	6.38	Dec/30/2016 11:33:5	6			
🗃 calea	6.38	Dec/30/2016 11:33:5	6			
🗟 dhcp	6.38	Dec/30/2016 11:33:5	6			
🗃 gps	6.38	Dec/30/2016 11:33:5	6			
🖻 hotspot	6.38	Dec/30/2016 11:33:5	6			
€ipv6	6.38	Dec/30/2016 11:33:5	6 scheduled for enable			
🛢 lcd	6.38	Dec/30/2016 11:33:5	6			
🗃 te	6.38	Dec/30/2016 11:33:5	6			
🗃 mpls	6.38	Dec/30/2016 11:33:5	6			
🗃 multicast	6.38	Dec/30/2016 11:33:5	6			
🗃 ntp	6.38	Dec/30/2016 11:33:5	6			
openflow	6.38	Dec/30/2016 11:33:5	6			
🗃 ррр	6.38	Dec/30/2016 11:33:5	6			
routing	6.38	Dec/30/2016 11:33:5	6			
security	6.38	Dec/30/2016 11:33:5	6			
🗃 system	6.38	Dec/30/2016 11:33:5	6			
tr069-client	6.38	Dec/30/2016 11:33:5	6			
🖨 ups	6.38	Dec/30/2016 11:33:5	6			
🗃 user-manager	6.38	Dec/30/2016 11:33:5	6			
🗃 wireless	6.38	Dec/30/2016 11:33:5	6			

Enable paket ipv6

L2.6. USER MANAGEMENT

Mikrotik *User Manager* digunakan untuk mengatur hak akses bagi siapa saja yang ingin melihat dan memodifikasi konfigurasi MikroTik. MikroTik menyediakan pengaturan *user* serta *profile* hak akses. Secara *default* Mikrotik menyediakan tiga profil yaitu *read* (*hanya dapat melihat tanpa dapat mengubah*), *write* (*hanya dapat memodifikasi konfigurasi tanpa dapat melihat hasil*), dan *full* (*dapat* *melihat dan memodifikasi konfigurasi*). MikroTik juga menyediakan satu *user* dengan nama **Admin** dengan profil *full*.

Group <full></full>		Group <read></read>	Group <write></write>	
Name: full	ОК	Name: read OK	Name: write OK	(
Policies: I local I tehnet I sen V fip I rebot I read I write I policy I tet I writox I sasti V web I sasti V senative I and I remon I dude I tikapp Skin: default I F	Cancel Apply Comment Copy Remove	Policies: 🗘 local 🤍 telnet V ssh ftp Apply V tebot V read V test V winhox Comment V asstrond V web V anff V sensitive V api V romon dude V tikapp Skin: default	Policies: 🖉 local 🗭 tehnet Canc 🖉 sh ftp Appl V reboot V read V write policy V test V wrihox Com V password V web V api V romon dude V tikapp Skin: default ¥	xel ly ient y ive
System		System	System	

Daftar profil yang disediakan MikroTik

Anda dapat melihat atau memodifikasi pengaturan *user manager* dalam MikroTik dengan cara klik *System* lalu klik *User*.

User List	t						
Users	Groups	SSH Keys	SSH Private Keys	Active Users			
+ -	- 🖉	× =	AAA				Find
Name	Δ.	Group All	owed Address	Las	t Logged In		-
::: sys	stem defa	ult user					
💧 📥 ad	min	full				Jan/01/2002 01:09:29	
1 item							

Daftar User pada User List

Pada bagian menu **User** terdapat daftar pengguna yang tersedia dan pada menu **Groups** terdapat profil *user*.

User List			
Users Groups	SSH Keys SSH Private Keys Active Users		
+ - @	T		Find
Name 🛆	Policies	Skin	•
👗 full	local telnet ssh ftp reboot read write policy test winbox passw	default	
👃 read	local telnet ssh reboot read test winbox password web sniff s	default	
Å write	local telnet ssh reboot read write test winbox password web	default	
3 items			

Daftar Group pada User List

L2.7. BACKUP DAN RESTORE KONFIGURASI

Mikrotik menyediakan fitur untuk melakukan *backup* dan *restore* konfigurasi yang ada dalam sistem operasi MikroTik. Manfaat dari *Backup* dan *Restore* adalah ketika terjadi kondisi dimana RB harus dikembalikan ke pengaturan awal atau *reset* maka seluruh konfigurasi yang sudah dilakukan otomatis akan hilang dan perlu dilakukan konfigurasi lagi dari awal hingga akhir. Jika *user* sudah melakukan *backup* konfigurasi maka meringankan ketika terjadi kondisi tersebut dan tidak perlu melakukan konfigurasi dari awal cukup dengan *restore* seluruh konfigurasi kembali seperti semula. Untuk melakukan Backup konfigurasi yang harus dilakukan adalah masuk ke *File List* dengan cara klik *Files*.

File List					
😑 🍸 🖹 🖹 Backup	Restore Upload.		Find		
File Name	Туре	Size	Creation Time	-	
🖹 🖹 auto-before-reset.backup	backup	11.7 KiB	Jan/01/2002 01:43:40	•	
hotspot	directory		Jan/02/1970 00:23:43		
hotspot/alogin.html	.html file	1293 B	Jan/02/1970 00:23:43		
hotspot/error.html	.html file	898 B	Jan/02/1970 00:23:43		
hotspot/errors.txt	.bt file	3615 B	Jan/02/1970 00:23:43		
hotspot/img	directory		Jan/02/1970 00:23:43		
hotspot/img/logobottom.png	.png file	3925 B	Jan/02/1970 00:23:43		
hotspot/login.html	.html file	3454 B	Jan/02/1970 00:23:43		
hotspot/logout.html	.html file	1813 B	Jan/02/1970 00:23:43		
hotspot/v	directory		Jan/02/1970 00:23:43		
hotspot/lv/alogin.html	.html file	1303 B	Jan/02/1970 00:23:43		
hotspot/lv/errors.txt	.txt file	3810 B	Jan/02/1970 00:23:43		
⊨ hotspot/lv/login.html	.html file	3408 B	Jan/02/1970 00:23:43		
hotspot/lv/logout.html	.html file	1843 B	Jan/02/1970 00:23:43		
hotspot/lv/radvert.html	.html file	1475 B	Jan/02/1970 00:23:43	٠	
38 items 30.6 MiB	of 128.0 MiB used	765	% free		

Jendela File List MikroTik

Setelah masuk ke *File List* klik *Backup* dan isi nama file pada *name* dan *password* pada *password*.

Backup			
Name:	atswa	^	Backup
Password:	••••	^	Cancel
	Don't Enc	rypt	

Pemberian nama dan password file backup

Setelah langkah tersebut dilakukan secara otomatis file backup akan tersimpan pada *File List* dengan extensi file **backup**.

File List				×
🗕 🍸 🖹 🖺 Backup 🛛 F	lestore Upload		Find	_
File Name /	Туре	Size	Creation Time	•
📄 atswa.backup	backup	9.2 KiB	Jan/01/2002 01:03:52	+
🖹 auto-before-reset.backup	backup	11.7 KiB	Jan/01/2002 01:43:40	
hotspot	directory		Jan/02/1970 00:23:43	
hotspot/alogin.html	.html file	1293 B	Jan/02/1970 00:23:43	
hotspot/error.html	.html file	898 B	Jan/02/1970 00:23:43	
hotspot/errors.txt	.txt file	3615 B	Jan/02/1970 00:23:43	
hotspot/img	directory		Jan/02/1970 00:23:43	
hotspot/img/logobottom.png	.png file	3925 B	Jan/02/1970 00:23:43	
hotspot/login.html	.html file	3454 B	Jan/02/1970 00:23:43	
hotspot/logout.html	.html file	1813 B	Jan/02/1970 00:23:43	
hotspot/v	directory		Jan/02/1970 00:23:43	
hotspot/lv/alogin.html	.html file	1303 B	Jan/02/1970 00:23:43	
hotspot/lv/errors.bd	.txt file	3810 B	Jan/02/1970 00:23:43	
hotspot/lv/login.html	.html file	3408 B	Jan/02/1970 00:23:43	
hotspot/lv/logout.html	.html file	1843 B	Jan/02/1970 00:23:43	+
39 items (1 selected) 30.6 MiB of	f 128.0 MiB used	765	% free	

File backup pada File List

Untuk mengembalikan file cukup dengan klik *Restore* lalu pilih file backup dan masukkan password sesuai dengan yang dikonfigurasi sebelumnya lalu klik *Restore*. Jika nama file dan password sesuai akan muncul peringatan untuk *reboot* mikrotik lalu pilih **Yes**.

Restore			
Backup File:	atswa.backup	₹	Restore
Password:	****	^	Cancel

Nama file dan passsword dari file backup

Restore
Do you want to restore configuration and reboot?
Yes No

Permintaan reboot MikroTik

L2.8. EXPORT DAN IMPOR KONFIGURASI MIKROTIK

Export dan *import* adalah salah satu layanan untuk menyimpan file konfigurasi seperti *backup* dan *restore* namun *export* dan *import* dapat digunakan untuk konfigurasi tertentu atau tidak keseluruhan. Proses *export* dan *import* tanpa melalui proses enkripsi jadi *file* yang tersimpan dapat menunjukkan apa saja yang di konfigurasi. Selain itu proses *import* tidak memerlukan *reboot* seperti proses *restore*. Untuk melakukan *export file* masuk ke **New Terminal** MikroTik lalu ketikkan perintah *export* berikut

[admin@rb] > export file=semua_konfigurasi

Perintah tersebut digunakan untuk *export* seluruh konfigurasi yang ada pada MikroTik

File List				×
- 🝸 🗈 🛍 Backup Restore Upload Find				
File Name	∠ Туре	Size	Creation Time	T
hotspot/redirect.html	.html file	318 B	Jan/02/1970 00:23:43	
hotspot/rlogin.html	.html file	850 B	Jan/02/1970 00:23:43	
hotspot/status.html	.html file	3009 B	Jan/02/1970 00:23:43	
hotspot/xml	directory		Jan/02/1970 00:23:43	
hotspot/xml/WISPAccessGa	a xsd file	4251 B	Jan/02/1970 00:23:43	
hotspot/xml/alogin.html	.html file	821 B	Jan/02/1970 00:23:43	
hotspot/xml/error.html	.html file	416 B	Jan/02/1970 00:23:43	
hotspot/xml/flogout.html	.html file	361 B	Jan/02/1970 00:23:43	
hotspot/xml/login.html	.html file	787 B	Jan/02/1970 00:23:43	1
hotspot/xml/logout.html	.html file	359 B	Jan/02/1970 00:23:43	1
hotspot/xml/rlogin.html	.html file	530 B	Jan/02/1970 00:23:43	
Dpub	directory		Jan/02/1970 00:24:38	1
🖹 semua_konfigurasi.rsc	script	1135 B	Jan/01/2002 01:03:31	
Skins	directory		Jan/01/1970 00:00:01	
um-before-migration.tar	.tar file	17.0 KiB	Jan/02/1970 00:38:18	
39 items (1 selected) 31.0 MiE	of 128.0 MiB used	75	% free	

Hasil export pada file list

Sedangkan untuk *export* konfigurasi tertentu seperti hanya *export* konfigurasi *IP Address* pada MikroTik perintahnya sebagai berikut

[admin@rb] /ip address > export file=konfigurasi_ip_address

File List				×
🗕 🍸 🗈 🔒 🛛 Backup	Restore Upload		Find	
File Name	Туре	Size	Creation Time	-
hotspot/redirect.html	.html file	318 B	Jan/02/1970 00:23:43	+
hotspot/rlogin.html	.html file	850 B	Jan/02/1970 00:23:43	
hotspot/status.html	.html file	3009 B	Jan/02/1970 00:23:43	1
hotspot/xml	directory		Jan/02/1970 00:23:43	
hotspot/xml/WISPAccessGa.	xsd file	4251 B	Jan/02/1970 00:23:43	
hotspot/xml/alogin.html	.html file	821 B	Jan/02/1970 00:23:43	1
hotspot/xml/error.html	.html file	416 B	Jan/02/1970 00:23:43	
hotspot/xml/flogout.html	.html file	361 B	Jan/02/1970 00:23:43	
hotspot/xml/login.html	.html file	787 B	Jan/02/1970 00:23:43	
hotspot/xml/logout.html	.html file	359 B	Jan/02/1970 00:23:43	
hotspot/xml/rlogin.html	.html file	530 B	Jan/02/1970 00:23:43	
konfigurasi_ip_address.rsc	script	149 B	Jan/01/2002 01:05:28	
Dpub	directory		Jan/02/1970 00:24:38	
🖹 semua_konfigurasi.rsc	script	1135 B	Jan/01/2002 01:03:31	
🗀 skins	directory		Jan/01/1970 00:00:01	٠
40 items (1 selected) 31.0 MiB of	of 128.0 MiB used	75	% free	

Hasil export pada file list

Untuk melakukan import perintah yang digunakan adalah

[admin@rb] > import file-name=konfigurasi_ip_address

L2.9. RESET MIKROTIK

Untuk melakukan *reset* RB dapat dilakukan dengan 2 cara, yaitu dengan *soft reset* dan *hard reset*. *Soft reset* adalah cara melakukan *reset* MikroTik menggunakan *software* dan *hard reset* adalah cara melakukan *reset* mikrotik dengan cara menekan tombol *reset* pada RB.

Untuk melakukan *soft reset* caranya dengan klik *System* lalu klik *Reset Configuration* lalu klik *Reset Configuration*.

Reset Configuration	
Keep User Configuration	Reset Configuration
Do Not Backup	Cancel
Run After Reset:	

Jendela Reset Configuration

Untuk melakukan *hard reset* caranya dengan melepas kabel *power* dari RB, lalu menekan tombol *reset* pada RB dan menancapkan kembali kabel *power*, tunggu hingga led ACT berkedip setelah itu lepas kembali tombol *reset* yang ditekan.



Bagian belakang RB 951

L2.10. IP ADDRESS MIKROTIK

IP Address yang dapat dikonfigurasi pada MikroTik ada dua yaitu IP Statis dan IP Dinamis. IP Statis adalah *IP Address* yang dikonfigurasi secara manual sedangkan IP Dinamis adalah IP Address yang diperoleh secara otomatis (*DHCP Client*) atau dikonfigurasi untuk memberikan IP Address secara otomatis (*DHCP Server*) kepada host yang terhubung dengan RB Dynamic Configuration Protocol (DHCP) adalah layanan yang secara otomatis memberikan IP Address kepada komputer yang memintanya

Konfigurasi IP Statis dilakukan dengan cara klik IP lalu klik **Addresses** lalu klik + atau **Add** lalu masukkan IP Address (Host) beserta Prefix (Contoh : 192.168.1.1/24) pada kolom **Address**, IP Nettwork pada kolom **Network**, serta pilih Ethernet yang diinginkan pada menu **Interface** lalu klik **OK**.



Jendela Address pada menu Address List

perangkat yang memberikan IP Address disebut DHCP server, sedangkan perangkat yang meminta atau mendapatkan IP Address disebut sebagai DHCP Client.

Untuk konfigurasi *IP Address* Dinamis ada dua, DHCP *Client* dan DHCP *Server*. DHCP Client dikonfigurasi ketika *Ethernet* pada RB terhubung dengan perangkat lain yang menyediakan *IP Address* dari DHCP *Server*. Konfigurasi DHCP *Client* pada RB dengan cara klik **IP** lalu klik **DHCP** *Client* lalu klik **Add** lalu pilih *Ethernet* yang akan mendapatkan *IP Address* dari DHCP *Server* pada menu *Interface*, lalu klik OK.

DHCP Client <wlan1></wlan1>	
DHCP Status	ОК
Interface: wlan1	Cancel
✓ Use Peer DNS ✓ Use Peer NTP	Apply
	Disable
	Comment
	Сору
Add Default Route: yes 🔻	Remove
Default Route Distance: 0	Release
	Renew
enabled Status: bound	

Jendela DHCP Client

Setelah itu IP *Address* yang diperoleh dapat dilihat di *Address List* dan pada bagian depan IP Dinamis akan muncul huruf D sebagi informasi bahwa IP tersebut adalah IP Dinamis

Address List		
+ - 🖉 💥 [- 7	Find
Address / D ⊕ 12.12.12.1/24 ⊕ 192.168.1.1/24	Network 12.12.12.0 192.168.1.0	Interface value of the second
2 items		

IP Address yang diperoleh dari DHCP Server

Untuk membuat DHCP *Server* langkah yang dilakukan adalah melakukan konfigurasi *IP Address* yang digunakan *Ethernet* yang terhubung dengan perangkat penerima atau DHCP *Client*. Setelah siap langkah selanjutnya klik *IP* lalu klik *DHCP Server* lalu klik *DHCP* *Setup*, pilih *Interface*, dan masukkan *IP Address* sesuai yang di inginkan

DHCP Setup	DHCP Setup
Select interface to run DHCP server on	Select network for DHCP addresses
DHCP Server Interface: ether3	DHCP Address Space: 20.20.20.0/24
Back Next Cancel	Back Next Cancel
DHCP Setup	DHCP Setup
Select gateway for given network	Addresses to Give Out 20 20 20 1 20 20 20 19
Gateway for DHCP Network: 20.20.20.20	20.20.20.21-20.20.20.25 \$
Back Next Cancel	Back Next Cancel
DHCP Setup	DHCP Setup
Select DNS servers	Select lease time
DNS Servers: 8.8.8.8	Lease Time: 00:10:00
Back Next Cancel	Back Next Cancel
DHCP Setup	
Setup has completed successfully	

Langkah-Langkah konfigurasi DHCP Server

LABORATORIUM 3





MIKROTIK FIREWALL

L3.1. NAT

Network Address Translation (NAT) adalah suatu metode untuk menghubungkan banyak komputer ke jaringan internet dengan menggunakan satu atau lebih alamat IP

Pada *IP Firewall* NAT terdapat dua Chain, **srcnat** dan **dstnat**, srcnat mengijinkan action **masquerade** (*layanan jaringan LAN mendapatkan 1 alamat dinamis yang berasal dari IP Address WAN*) dan **srcnat** (*layanan jaringan LAN mendapatkan 1 alamat static yang berasal dari IP Address WAN*).

Untuk melakukan konfigurasi NAT pada RB dengan cara klik **IP** lalu klik **Firewall** lalu klik **NAT** lalu klik **"+**" atau **Add**.



Jendela NAT pada Firewall

Setelah masuk NAT *Rule* pada bagian **General** pilih "srcnat" pada **Chain** dan pilih ethernet yang terhubung dengan internet atau ip publik pada *Out Interface* lalu **Apply**.

VAT Rule	<u>ہ</u>					
General	Advanced	Extra	Action	Statistic	s	ОК
	Chain: sr	cnat		1	•	Cancel
Src.	Address:				•	Apply
Dst.	Address:			•	•	Disable
	Protocol:				-	Comment
:	Src. Port:				-	Сору
1	Dst. Port:				•	Remove
ļ	Any. Port:				•	Reset Counters
In. I	nterface:				•	Reset All Counters
Out. I	nterface:	wlan 1		Ŧ	•	
Pack	ket Mark:				•	
Connecti	on Mark:				•	
Routi	ng Mark:			•	•	
Routir	ng Table:				•	
Connecti	on Type:				-	

Jendela General pada NAT Rule



Penerapan Out dan In pada Router MikroTik

Setelah itu masuk ke **Action** dan pilih *masquerade* pada Action lalu klik **Apply** lalu klik **OK**.

NAT Rule <>						
General Advanced	Extra	Action	Statistics		ОК	
Action: mas	masquerade 🗧			Cancel		
	og				Apply	
Log Prefix:			•	[Disable	
				C	omment	
					Сору	
				F	lemove	
				Rese	t Counters	
				Reset	All Counters	

Jendela Action pada NAT Rule

Setelah itu masuk ke Terminal pada MikroTik lalu test ping ke *www.google.com* dan pastikan *reply*.

Terminal					
[admin@ATSWA] > ping www.google.com					+
SEQ HOST	SIZE	TTL	TIME	STATUS	
0 114.4.4.216	56	54	185ms		
1 114.4.4.216	56	54	139ms		
2 114.4.4.216	56	54	261ms		
3 114.4.4.216	56	54	189ms		
4 114.4.4.216	56	54	313ms		
5 114.4.4.216	56	54	385ms		
<pre>sent=6 received=6 packet-loss=0%</pre>	min-rtt=139ms a	avg-1	rtt=24	5ms max-rtt=385ms	
[admin@ATSWA] >					+

Hasil ping www.google.com melalui terminal

Selain itu lakukan tes ping pula menggunakan *Command Prompt* pada komputer untuk memastikan komputer sudah mendapatkan akses *internet*.



Hasil ping www.google.com melalui cmd
L3.2. FIREWALL LOGGING MIKROTIK

Firewall Logging adalah layanan pada *firewal* yang digunakan untuk mencatat aktifitas jaringan pada *Log MikroTik*. Untuk mengaktifkannya klik IP lalu klik *Firewall* lalu klik *Filter Rule* lalu klik *General* lalu tentukan *Chain* setelah itu pilih protokol ICMP pada menu *Protocol* dan pilih *interface* yang terhubung dengan komputer.

Firewall Rule <>		
General Advanced E	dra Action Statistics	ОК
Chain:	input 🗧	Cancel
Src. Address:	▼	Apply
Dst. Address:	▼	Disable
Protocol:	1 (icmp) ∓ 🔺	Comment
Src. Port:		Сору
Dst. Port:	•	Remove
Any. Port:		Reset Counters
P2P:	▼	Reset All Counters
In. Interface:	ether2 🔻 🔺	
Out. Interface:		
In. Interface List:		
Out. Interface List:		
Packet Mark:	▼	
Connection Mark:	▼	
Routing Mark:	▼	
Routing Table:		
Connection Type:		
Connection State:	•	
Connection NAT State:	•	

Jendela General pada Firewall Rule

Setelah itu masuk ke menu *Action* dan pilih *Log* pada menu *Action* lalu klik *OK*.

Firewall Rule <>	
General Advanced Extra Action Statistics	ОК
Action: log	Cancel
Log	Apply
Log Prefix:	Disable
	Comment
	Сору
	Remove
	Reset Counters
	Reset All Counters

Jendela Action pada Firwall Rule

Setelah itu lakukan ping dari komputer ke IP Address yang berada pada RB atau komputer lain dan masuk ke **Log** pada Mikrotik untuk melihat hasilnya.

Log			
Freeze			all 🔻
Jan/01/2002 03:02:45	memory	firewall, info	input: in:ether2 out:(none), src-mac 0 (.0111272). D:e3, proto ICMP (type 8, code 0), 192.168.1.2->192.168.1.1, len 60
Jan/01/2002 03:02:46	memory	firewall, info	input: in:ether2 out:(none), src-mac 24.37.46.75;-c:e3, proto ICMP (type 8, code 0), 192.168.1.2->192.168.1.1, len 60
Jan/01/2002 03:02:47	memory	firewall, info	input: in:ether2 out:(none), src-mac 0 1:97f0.75, 10.33, proto ICMP (type 8, code 0), 192.168.1.2->192.168.1.1, len 60
Jan/01/2002 03:02:48	memory	firewall, info	input: in:ether2 out:(none), src-mac \$1,5770.75,40.03, proto ICMP

Log pada Mikrotik

L3.3. FILTER RULE

Filter Rule atau aturan penyaringan adalah salah satu fitur pada firewall MikroTik yang digunakan untuk melakukan penyaringan trafik yang menuju ke router, keluar dari router, dan melewati router. Dalam *Filter Rule* terdapat tiga pilihan *Chain* yaitu *Input*, *Forward*, dan *Output*. Masing-masing *Chain* memiliki pengaturan trafik yang berbeda, antara lain sebagai berikut



Chain Filter Rules pada MikroTik



Penerapan Source (Src) dan Destination (Dst) pada MikroTik

Jika *Chain* dengan mode *Input* Anda dapat mengaturan trafik yang berasal dari komputer dan menuju *router* atau sebaliknya, jika *Chain* dengan mode *Forward* Anda dapat mengatur trafik yang melewati *router* dari komputer menuju Internet atau sebaliknya, dan jika *Chain* dengan mode *Output* Anda dapat mengaturan trafik yang berasal dari *router* menuju ke Internet atau sebaliknya. Anda dapat memanfaatkan *Filter Rule* untuk memmemblokir situs menggunakan Filter Rule pada firewall dengan cara klik *IP* lalu klik *Firewall* lalu klik *Filter Rule* lalu klik "+" atau **Add**. Pastikan terlebih dahulu situs yang akan Anda blokir dapat diakses dengan normal.



Situs www.nvidia.com sebelum diblokir

Setelah dipastikan situs yang akan diblokir dapat diakses langkah selanjurnya adalah mengetahui *IP Address* yang digunakan situs tersebut. Jika menggunakan *Command Prompt* dapat menggunakan perintah *nslookup*.

C61.	Command Prompt	-	×	
C:\>nslookup www.nvidia.com Server: google-public-dns-a.goo Address: 8.8.8.8	gle.com		~	•
Non-authoritative answer: Name: cs326284.adn.phicdn.net Address: 192.229.189.146 Aliases: www.nvidia.com www.nvidia.com.global.	ogslb.com			
C:<>				

IP Address dari www.nvidia.com

Setelah Anda mengetahui *IP Address* langkah selanjutnya kembali ke menu *Filter Rule* pada *Firewall*

Frewall		
Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols		
+ - 🖉 🖄 🖅 🛛 oo Reset Counters oo Reset Al Counters	Find all	∓
# Action Chain Src. Address Dst. Address Proto Src. Port Dst. Port In. Inter Out. Int Bytes	Packets	-
0 items		

Jendela *Filter Rule* pada *Firewall*

Pada menu *General* pastikan *Chain* dengan mode *Forward* karena yang akan dilakukan adalah melakukan pemblokiran trafik yang melewati *Router* yaitu dari Komputer ke Internet. Setelah itu masukkan *IP Address* dari situs yang akan diblokir pada bagian *Dst Address* lalu klik *Apply*.

Firewall Rule <192.229.18	39.146>				
General Advanced E	ixtra A	ction	Statistics		ОК
Chain:	forward	l		₹	Cancel
Src. Address:				•	Apply
Dst. Address:	192	.229.1	89.146]•	Disable
Protocol:				•	Comment
Src. Port:				•	Сору
Dst. Port:				-	Remove
Any. Port:				•	Reset Counters
P2P:				•	Reset All Counters
In. Interface:				•	
Out. Interface:				-	
Packet Mark:				•	
Connection Mark:				•	
Routing Mark:				•	
Routing Table:				•	
Connection Type:				•	
Connection State:				•	
Connection NAT State:				•	

Jendela *General* pada *Firewall Rule*

Setelah itu masuk ke menu *Action* pada *Firewal Rule* lalu pilih "*drop*" lalu klik *Apply* lalu klik *OK*.

Firewall Rule <192.229.189.146>	
General Advanced Extra Action Statistics	ОК
Action: drop 두	Cancel
	Apply
Log Prefix:	Disable
	Comment
	Сору
	Remove
	Reset Counters
	Reset All Counters

Jendela Action Firewall Rule

Anda dapat melihat *rule* yang telah dibuat pada menu *Firewal Rule*.

Firewall									
Filter Rules	NAT Mangle	Service Ports	Connections	Address List	s Layer7 Protocols				
+	/ 🛛 🖻	7 00 Re:	set Counters	00 Reset A	I Counters		Find	all	∓
#									•
0 🗶	Action:		drop	Cha	ain:	forward			
Dst	Address:		192.229.189.14	46 Log		no			
Byte	s:		DB	Pac	kets:	0			
Rat	e:		Obps	Pad	ket Rate:	0			
1 item									

Filter Rule yang sudah dibuat

Jika semua langkah tersebut sudah sesuai lakukan pengujian terhadap situs yang diblokir untuk melihat apakah sudah berhasil atau belum.

	⊥ = # × ☆ :
E.	
This site can't be reached	
www.nvidia.com took too long to respond.	
Try: Checking the connection Checking the proxy and the firewall Running Windows Network Diagnostics	
ERR_CONNECTION_TIMED_OUT	
Reload	DETAILS

halaman www.nvidia.com setelah berhasil diblokir

L3.4. CONTENT



Topologi Jaringan

Dalam firewal Anda juga dapat melakukan penyaringan berdasarkan konten atau informasi yang ada di halaman sebuah situs. Sebelum Anda melakukan pemblokiran uji terlebih dahulu terhadap web tersebut untuk memastikan bahwa web tersebut masih dapat diakses.



Halaman www.amd.com sebelum diblokir

Setelah itu klik *IP* lalu klik *Firewall* lalu klik *Filter Rule* lalu klik "+" atau *Add*.

Firewall			
Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols			
🔹 🖃 🖉 🖄 🖆 🍸 🛛 oo Reset Counters 🛛 oo Reset All Counters	Find	all	Ŧ
#			-
0 items			

Jendela *Filter Rule*

Masuk ke menu *General* pada *Firewall Rule* dan pilih mode *Forward* pada *Chain* lalu klik **Apply**.

Firewall Rule <>					
General Advanced	Extra	Action	Statistics		ОК
Chain:	forw	ard		Ŧ	Cancel
Src. Address:] •	Apply
Dst. Address:				•	Disable
Protocol				•	Comment
Src. Port:				-	Сору
Dst. Port:				•	Remove
Any. Port:				-	Reset Counters
P2P:				•	Reset All Counter
In. Interface:]•	
Out. Interface:				•	
Packet Mark:				•	
Connection Mark:]•	
Routing Mark:]•	
Routing Table:				•	
Connection Type:				•	
Connection State:]•	
Connection NAT State:				-	

Jendela *General* pada *Firewall Rule*

Klik *Advanced* dan pada bagian *content* masukkan kata yang akan diblokir lalu klik *Apply*.

Firewall Rule <>	
General Advanced Extra Action Statistics	ОК
Src. Address List:	Cancel
Dst. Address List:	Apply
Layer7 Protocol:	Disable
Contracts Claused	Comment
	Сору
Connection Bytes:	Remove
Connection Rate:	Reset Counters
Per Connection Classifier:	Reset All Counters
Out. Bridge Port:	
In. Bridge Port:	
IPsec Policy:	
Ingress Priority:	
Priority:	
DSCP (TOS):	
TCP MSS:	
Packet Size:	
Random: 🔽 🔻	
-▼- TCP Flags	
-▼- ICMP Options	
IPv4 Options:	
TTL: 🗸	

Jendela Advanced pada Firewall Rule

Klik *Action* lalu pilih *drop* pada daftar pilihan *Action* lalu klik *Apply* lalu klik *OK*.

Firewall Rule <>	
General Advanced Extra Action Statistics	ОК
Action: drop 두	Cancel
Log	Apply
Log Prefix:	Disable
	Comment
	Сору
	Remove
	Reset Counters
	Reset All Counters

Jendela Action pada Firewall Rule

Untuk melihat *rule* yang telah dibuat masuk ke menu *Filter Rule* pada *Firewall*.

Firewall					
Filter F	Rules NAT Mangle	Service Ports Connections	Address Lists Layer7 Protocols		
+	- ~ ~ 🖻	OO Reset Counters	00 Reset All Counters		Find all 🔻
#					•
0	X Action:	drop	Chain:	forward	
	Content:	amd	Log:	no	
	Bytes:	2452.6 KiB	Packets:	2 856	
	Rate:	0 bps	Packet Rate:	0	
1 item					

Filter Rule yang dibuat

Setelah semua selesai lakukan pengujian apakah konten tersebut sudah berhasil diblokir atau belum.

) www.amd.com		
← → × ③ www.amd.com		☆ :
	8	
	This site can't be reached	
	www.amd.com's server DNS address could not be found.	
	Search Google for amd	
	ERR,NAME_NOT_RESOLVED	
	Show saved copy	
lesolving host		

halaman www.amd.com setelah diblokir

L3.5. ADDRESS LIST



Topologi Jaringan

Jika Anda ingin melakukan pemblokiran terhadap situs yang memiliki *IP Address* lebih dari satu dapat menggunakan *Address List. Address List* adalah fitur yang digunakan untuk melakukan pemfilteran terhadap *Grup IP Address* menjadi *1 Rule Firewall*. Seperti sebelumnya lakukan pengujian terlebih dahulu terhadap situs atau *web* yang akan diblokir masih dapat diakses sebelum dilakukan pemblokiran.



Halaman www.intel.com sebelum diblokir

Selanjutnya adalah melihat *IP Address* dari domain yang akan diblokir menggunakan *nslookup*.

01	Command Prompt	-	×
C:\>nslookup www.intel.com Server: google-public-dns-a.goog Address: 8.8.8.8	yle.com		î
hon-authoritative answer: Name: a 961 g.akamai.net Addresses: 114.4.39.230 114.4.39.210 Aliases: www.intel.com www.intel.com.edgesuit www.intel.com.edgesuit	:.net .net.globalredir.akadns.net		
C:\>			
			· ·

IP Address dari www.intel.com

Setelah mengetahui *IP Address* langkah selanjutnya adalah masuk ke *Filter Rule Firewall* dengan cara klik *IP* lalu klik *Firewall* lalu klik *Filter Rule*

Frewall	
Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols	
🛉 🗖 🖉 🖾 🍸 00 Reset Counters 00 Reset All Counters Find	all 🔻
#	
() tems	
0 items	

Jendela Filter Rule Firewall

Firewall Rule <>			
General Advanced	Extra Action S	tatistics	ОК
Chain:	forward	₹	Cancel
Src. Address:			Apply
Dst. Address:		▼	Disable
Protocol		-	Comment
Src. Port:		-	Сору
Dst. Port:		-	Remove
Any. Port:			Reset Counters
P2P:			Reset All Counters
In. Interface:		•	
Out. Interface:		•	
Packet Mark:		•	
Connection Mark:			
Routing Mark:			
Routing Table:		•	
Connection Type:		•	
Connection State:			
Connection NAT State:		•	

Masuk ke menu *General* lalu pilih *Forward* pada pengaturan *Chain* lalu klik *Apply*.

Jendela *General* pada *Firewall Rule*

Masuk ke menu *Action*, pada *Action* pilih *drop* lalu klik *Apply*.

Firewall Rule 🔿				
General Advanced	Extra Actio	n Statistics	L	ОК
Action: drop			Ŧ	Cancel
				Apply
Log Prefix:			•	Disable
				Comment
				Сору
				Remove
				Reset Counters
				Reset All Counters

Jendela Action pada Firewall Rule

Masuk ke menu *Address List* lalu klik "+" atau *Add*.

Firewall				
Filter Rules NAT Mangle Service Ports	Connections Add	ress Lists Layer7 Protocols		
+ - 🖉 🗶 🕾 🍸			Find	all Ŧ
Name 🛆 Address	Timeout			-
0.3				
U items				

Jendela Address List pada Firewall

Pada *Firewall Address List* masukkan semua *IP Address* dari domain yang akan diblokir.

Firewall Address List <intel></intel>		Firewall Address List <intel></intel>	
Name: intel 🗧	ОК	Name: intel 🔻	OK
Address: 114.4.39.230	Cancel	Address: 114.4.39.210	Cance
Timeout:	Apply	Timeout:	Apply
	Disable		Disable
	Comment		Comme
	Сору		Сору
	Remove		Remov
enabled		enabled	

Jendela Firewall Address List

Untuk melihat *Address List* yang telah dibuat dapat dilihat di menu *Address List*.

Firewall							[□ ×
Filter Rules	NAT Mangle	Service Ports	Connections	Address Lists	Layer7 Protocols			
+ - [~ X 🖻	T				Find	all	∓
Name	∠ Address		Timeout					•
intel	114.4.39	230						
 intel 	114.4.39	210						
2 items								

Address List yang sudah jadi

Masuk kembali ke menu *Advanced* pada *Firewall Rule*, pada bagian *Dst. Address List* pilih daftar *IP Address* yang telah dibuat sebelumnya lalu klik *Apply* lalu klik *OK*.

К
ncel
ply
able
ment
ру
nove
Counters
Counters

Jendela Advanced pada Firewall Rule

Filter Rules NAT Mangle Service Ports Connections Address Lists Laver7 Protocols	
+ - 🖉 🖄 🖾 🍸 OO Reset Counters OO Reset All Counters Find all	Ŧ
#	▼
0 XAction: drop Chain: forward	
Dst. Address List: intel Log: no	
Bytes: 45.6 KiB Packets: 273	
Rate: 0 bps Packet Rate: 0	
1 item	

Lakukan pengujian terhadap domain dari *web* yang telah diblokir menggunakan *Address List* apakah sudah berhasil diblokir atau belum.



Halaman web www.intel.com setelah diblokir

L3.6. LAYER 7 PROTOCOLS





Anda juga dapat melakukan pemblokiran menggunakan *Regexp* melalui *Layer 7 Protocols* pada *Firewall*. Pastikan *web* yang akan diblokir sebelum dilakukan pemblokiran masih dapat diakses.



Halaman www.asus.com sebelum diblokir

Masuk ke *Firewall* dengan cara klik *IP* lalu klik *Firewall* lalu klik *Layer 7 Protocols*. Setelah masuk ke menu *Layer 7 Protocols* klik "+" atau *Add*.

Firewall	
Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols	
	Find
Name 🕢 Regexp	▼
0	
U rems	

Jendela Layer 7 Protocol pada Firewall

Masuk di jendela *Firewall L7 Protocol* lalu masukkan domain dari situs yang akan diblokir dengan menuliskan "^.+(nama_domain).*\\$" lalu klik *Apply* lalu klik **OK**.

Firewall L7 Protocol <asus></asus>		
Name: asus		ОК
	Regexp:	Cancel
^.+(www.asus.com).*\\$	^	Apply
		Comment
		Сору
		Remove
	\sim	

Jendela Firewall L7 Protocol

Daftar dari *domain* yang diblokir menggunakan *Layer 7 Protocol* dapat dilihat pada menu *Layer 7 Protocols* pada *Firewall*.

Firewall						
Filter Rules NA	T Mangle	Service Ports	Connections	Address Lists	Layer7 Protocols	
+ - 2	T					Find
Name 🗵	Regexp					▼
asus	^.+(www.asu	ıs.com). *∖\$				
1 item						

Daftar rule pada jendela Layer 7 Protocol

Setelah itu masuk ke menu *Filter Rule* lalu klik "+" atau *Add*. Setelah masuk ke jendela *Firewall Rule* klik menu *General* dan pada daftar *Chain* pilih *Forward* lalu klik *Apply*.

General	Advanced	Extra	Action	Statistics		ОК
	Chair	1: forw	ard		Ŧ	Cancel
	Src. Address	s: 📃			•	Apply
	Dst. Address	s:]•	Disable
	Protoco	l: 📃			•	Comment
	Src. Por	t: 📃			•	Сору
	Dst. Por	t: 📃			•	Remove
	Any. Por	t: 📃]•	Reset Counters
	P2F	:]•	Reset All Counte
	In. Interface]•	
(Out. Interface	e:]•	
	Packet Mark	u 🗌			•	
Con	nection Mark	c 🗌			-	
	Routing Mark				•	
F	Routing Table	:			•	
Con	nection Type	:			•	
Con	nection State				•	
Connectio	on NAT State	e:			-	

Jendela *General* pada *Firewall Rule*

Setelah itu masuk ke menu *Advanced* lalu pada daftar *Layer* 7 *Protocol* pilih daftar yang sudah dibuat lalu klik **Apply**.

Firewall Rule 🔿	
General Advanced Extra Action Statistics	ок
Src. Address List:	Cancel
Dst. Address List:	Apply
Layer7 Protocol: 🗌 asus 🗧 🔺	Disable
Content:	Comment
Connection Bites:	Сору
	Remove
	Reset Counters
Per Connection Classifier:	Reset All Counters
Src. MAC Address:	
Out. Bridge Port:	
In. Bridge Port:	
IPsec Policy:	
Ingress Priority:	
Priority:	
DSCP (TOS):	
TCP MSS:	
Packet Size:	
Random:	
-▼- TCP Flags	
-▼- ICMP Options	
IPv4 Options:	
TTL:	
And the second se	

Jendela Advanced pada Firewall Rule

Setelah itu masuk ke menu *Action* dan pada daftar *Action* pilih *drop* lalu klik *Apply* lalu klik **OK**.

Firewall Rule <>	
General Advanced Extra Action Statistics	ОК
Action: drop 🗧	Cancel
	Apply
Log Prefix:	Disable
	Comment
	Сору
	Remove
	Reset Counters
	Reset All Counters

Jendela Action pada Firewall Rule

Untuk melihat *rule* yang telah dibuat dapar dilihat pada *Filter Rule* pada menu *Firewall*.

Langkah terakhir adalah melakukan pengujian terhadap domain situs yeng telah diblokir untuk memastikan apakah sudah berhasil diblokir atau belum.



Halaman www.asus.com yang telah diblokir

L3.7. TRANSPARENT DNS



Topologi Jaringan

Untuk melakukan pemblokiran menggunakan *Transparent* DNS pastikan terlebih dahulu *IP Address* dari DNS yang akan digunakan. Di Indonesia ada DNS yang cukup terkenal adalah DNS dari *Nawala Project*. Alamat DNS dari *Nawala Project* adalah 180.131.144.144. Langkah pertama yang dilakukan adalah masuk NAT pada *Firewall* dengan cara klik *IP* lalu klik *Firewall* lalu klik *NAT* lalu klik "+" atau *Add*.

Firewall				×
Filter Rules NAT Mangle	Service Ports Connections	Address Lists Layer7 Protocols		
+ - 🗸 🖄 🖻	00 Reset Counters	00 Reset All Counters	Find all	∓
# Action Chain	Src. Address Dst. Addres	ss Proto Src. Port Dst. Port	In. Inter Out. Int Bytes Packets	-
0 ≓∥ mas srcnat			wlan1 971 B 17	
1 item				

Jendela NAT pada Firewall

Setelah masuk NAT masuk ke menu *General* dan pada *Chain* pilih dstnat, pada *Protocol* pilih *UDP*, pada *dst Port* masukkan 53 (*53 adalah port dari DNS*), lalu klik *Apply*.

NAT Rule <53>	
General Advanced Extra Action Statistics	ОК
Chain: dstnat	Cancel
Src. Address:	Apply
Dst. Address:	Disable
Protocol: 🗌 17 (udp) 🛛 🔻 🔺	Comment
Src. Port:	Сору
Dst. Port: 53	Remove
Any. Port:	Reset Counters
In. Interface:	Reset All Counters
Out. Interface:	
Packet Mark:	
Connection Mark:	
Routing Mark:	
Routing Table:	
Connection Type:	

Jendela *General* pada *NAT Rule*

Setelah itu masuk ke menu *Action* pada *Action* pilih *dst port*, pada *to address* masukkan *IP Address* dari *Nawala Project*, lalu pada *to port* masukkan *port* dari DNS yaitu 53, lalu klik *Apply* lalu klik OK.

NAT Rule <53>	
General Advanced Extra Action Statistics	ОК
Action: dst-nat	Cancel
	Apply
Log Prefix:	Disable
To Addresses: 180.131.144.144	Comment
To Ports: 53	Сору
	Remove
	Reset Counters
	Reset All Counters

Jendela Action pada NAT Rule

Setelah itu untuk melihat *NAT Rule* yang telah dibuat dapat melihat pada menu *NAT* pada *Firewall*.

Firewall												
Filter Rule	es NAT	Mangle	Service Ports	Connections	Address I	Lists Layer	7 Protocols					
+ -	+ - 🖉 🔅 🖆 🍸 00 Reset Counters 00 Reset Al Counters Find all								. ₹			
#	Action	Chain	Src. Address	Dst. Address	Proto	Src. Port	Dst. Port	In. Inter	Out. Int	Bytes	Packets	•
0	≓l mas	srcnat							wlan1	1482 B	22	
1	+ * dst	dstnat			17 (u		53			0 B	0	
2 items												

Daftar NAT Rule pada jendela NAT Firewall

L3.8. TRANSPARENT WEB PROXY



Topologi Jaringan

Untuk melakukan pemblokiran menggunakan *Transparent Web Proxy* pastikan terlebih dahulu domain dari web yang akan diblokir masih dapat diakses.



Halaman www.acer.com sebelum diblokir

Setelah itu masuk ke menu *Web Proxy Settings* dengan cara klik *IP* lalu klik *Web Proxy*. Setelah masuk di menu *Web Proxy Setting* aktifkan *web proxy* dengan cara memberikan ceklist pada *Enabled* lalu pada *port* masukkan 8080 (*8080 adalah port dari web proxy*), lalu pada *Cache Administrator* masukkan identitas yang ditampilkan dapat berupa *email* nomer telpon atau lain sebagainya, lalu beri ceklist pada *Cache On Disk* agar penyimpanan *cache web proxy* disimpan pada *harddisk* bukan *memory*.

Veb Proxy Settings						
General Status Lookup	s Inserts R	efreshes			OK	(
	Enabled				Cano	el
Src. Address:	::			\$	Арр	y
Port:	8080	-	_	÷	Clear C	ache
	Anonymou	5			Reset H	ITML
Parent Proxy:				•	Acce	SS
Parent Proxy Port:				•	Cact	ne
Cache Administrator:	atswamedia@	gmail.com		•	Dire	ct
Max. Cache Size:	unlimited		Ŧ	ĸв	Connec	tions
Max Cache Object Size:	2048			КiВ	Cache Co	onten
	Cache On	Disk				
Max. Client Connections:	600					
Max. Server Connections:	600					
Max Fresh Time:	3d 00:00:00					
	Serialize Co	onnections				
	Aiways Pro	m Cache				
Cache Hit DSCP (TOS):	4					
Cache Path:	web-proxy			₹		
unning			-		1	

Jendela Web Proxy Settings

Setelah itu masuk ke *NAT* pada *Firewall* lalu klik "+" atau Add.

Firew	all												×
Filte	r Rules	NAT	Mangle	Service Ports	Connections	Address Lis	sts Layer7	Protocols					
÷		/ 8	8	7 00 R	eset Counters	00 Reset	All Counters				Find	all	Ŧ
#	Acti	on	Chain	Src. Addre	ss Dst. Address	s Protocol	Src. Port	Dst. Port	In. Interface	Out. Interface	Bytes	Packets	-
0	≓∥ I	nas	srcnat							ether1	231.6 KiB	3 15	5
1 iter	m												

Jendela **NAT** pada **Firewall**

Setelah itu masuk ke menu *General* pada *NAT Rule* lalu pada *Chain* pilih *forward*, lalu pada *Protocol* pilih *TCP*, lalu pada *Dst Port* masukkan **80** (*80 adalah port dari www atau web*), lalu klik **Apply**.

VAT Rule	<80>					
General	Advanced	Extra	Action			ОК
	Chain: de	stnat			Ŧ	Cancel
Src.	Address:				•	Apply
Dst.	Address:				•	Disable
	Protocol:	6 (tcp)		Ŧ		Comment
9	Src. Port:				•	Сору
[Dst. Port:	80			 	Remove
A	ny. Port:				•	Reset Counters
In. I	nterface:				•	Reset All Counters
Out. I	nterface:				•	
Pack	et Mark:				-	
Connecti	on Mark:				•	
Routi	ng Mark:				•	
Routin	ng Table:				-	
Connecti	on Type:				•	

Jendela *General* pada *NAT Rule*

Setelah itu masuk ke menu *Action* pada *NAT Rule* lalu pada *Action* pilih *redirect* lalu pada *To Ports* masukkan 8080, lalu klik *Apply*, lalu klik *OK*.

NAT Rule <80>	
Advanced Extra Action Statistics	ОК
Action: redirect	Cancel
Log	Apply
Log Prefix:	Disable
To Ports: 8080	Comment
	Сору
	Remove
	Reset Counters
	Reset All Counters

Jendela Action pada NAT Rule

Untuk melihat *NAT Rule* yang sudah dibuat dapat dilihat pada menu *NAT Firewall*.

Setelah itu masuk kembali ke jendela *Web Proxy Setting* lalu masuk menu *Access* untuk masuk ke *Web Proxy Access*.

Veb Proxy Settings		
General Status	Lookups Inserts Refreshes	ОК
	 Enabled 	Cancel
Src. A	ddress: ::	Apply
	Port: 8080	Clear Cache
		Reset HTML
Parent	Proxy:	Access
Parent Prox	vy Port:	Cache
Cache Admini	istrator: atswamedia@gmail.com	Direct
Max. Cach	e Size: unlimited 🐺 KiB	Connections
Max Cache Obje	ct Size: 2048 KiB	Cache Conten
	Cache On Disk	
Max. Client Conne	ections: 600	
Max. Server Conne	ctions: 600	
Max Fresh	n Time: 3d 00:00:00	
	Serialize Connections	
	Always From Cache	
Cache Hit DSCP	(TOS): 4	
Cach	e Path: web-proxy 🔻	

Jendela *General* pada *Web Proxy Setting*

Pada *Web Menu Access* klik "+" atau Add.

Web	Web Proxy Access										
÷		🗂 🍸 00 Res	et Counters	00 Reset All C	ounters				Find		
#	Src. Address	Dst. Address	Dst. Port	Dst. Host	Path	Method	Action	Redirect To	Hits	-	
0 iter	ns										

Jendela Web Proxy Access

Setelah itu pada *Dst Port* masukkan 80, lalu pada *Dst Host* masukkan domain dari *web* yang akan diblokir, dan pada bagian *Action* pilih *deny*, lalu klik *Apply*, lalu klik *OK.*

Web Proxy Rule <>	
Src. Address:	ок
Dst. Address:	Cancel
Dst. Port: 🔲 80	Apply
Local Port:	Disable
Dst. Host: 🗌 www.acer.com 🔺	Comment
Path:	Сору
Method:	Remove
Action: deny	Reset Counters
Redirect To:	Reset All Counters
Hits: 0]
enabled	

Jendela Web Proxy Rule

We	b Proxy	Access									×
÷	_	*	00 Reset	Counters	00 Reset All Co	unters				Find	
#	Src	. Address	Dst. Address	Dst. Port	Dst. Host	Path	Method	Action	Redirect To	Hits	-
() 🧿			80	www.acer.com			deny		1	
1 ite	em										

Daftar Web Proxy Rule pada Web Proxy Access

a DRCA: forbidden x	1 - 8 ×
← → C ① www.acer.com	☆ :
ERROR: Forbidden	
While trying to retrieve the URL http://www.acer.com/:	
Access Denied	
Your cache administrator is atswamedia@gmail.com.	
Generated Sun, 26 Feb 2017 09:20:37 GMT by 192.168.2.1 (Mikrotik HttpProxy)	

Halaman www.acer.com yang telah diblokir

L3.9. REDIRECT



Topologi Jaringan

Sebelum Anda mengalihkan situs pastikan terlebih dahulu situs yang akan dialihkan tersebut masih dapat diakses.



Halaman www.logitech.com sebelum dialihkan

Setelah itu lakukan konfigurasi *Web Proxy* seperti sebelumnya, dan pada pengaturan *Web Proxy Rule* masukkan alamat situs yang akan dialihkan pada *Dst. Host* dan masukkan alamat situs tujuan pada *Redirect To*

Web Proxy Rule 🔿	
Src. Address:	ОК
Dst. Address:	Cancel
Dst. Port: 🗌 80	Apply
Local Port:	Disable
Dst. Host: 🗌 www.logitech.com 🔺	Comment
Path:	Сору
Method:	Remove
Action: deny T	Reset Counters
Redirect To: www.razerzone.com	Reset All Counters
Hits: 0	·
enabled	

Jendela Web Proxy Rule

Anda dapat melakukan pengujian dengan cara memasukkan situs yang di alihkan dan pastikan sudah berhasil mengakses ke situs tujuan.



Halaman www.razerzone.com

LABORATORIUM 4





MIKROTIK WIRELESS

L4.1. ACCESS POINT BRIDGE (PEMANCAR)



Topologi Wireless AP Bridge

Access Point adalah istilah yang digunakan untuk perangkat wireless yang dikonfigurasi sebagai pemancar atau pemberi koneksi. Untuk membuat *Access Point* pada perangkat MikroTik pertama masuk ke *Wireless Tables* dengan cara klik *Wireless* lalu double klik *Wireless* yang ada pada *Interface List*.

Wireless Tat	bles					
Interfaces	Nstreme Dual Access List	Registration Connect Li	ist Security Profiles	Channels		
+ •	V X 🗂 🍸	CAP Scanner F	Freq. Usage Alignn	nent Wireless Sniffer	Wireless Snooper	Find
Name	∠ Туре	Tx	Rx	Tx Packet (p	/s) Rx Packet (p/s) FP Ta 🔻
X ⟨\$>wla	an 1 Wireless (Athe	ros AR9	0 bps	0 bps	0	0
•						•
1 item out of	5					

Jendela Wireless Tables

Setelah Anda masuk di jendela *Wireless Interface* lakukan konfigurasi dengan memilih *AP Bridge* pada bagian *mode* lalu pilih *band* yang diinginkan lalu pilih *frequency* yang diinginkan lalu beri nama *AP Bridge* pada bagian *SSID* lalu aktifkan dengan cara klik *Enable* lalu klik *Apply* lalu klik *OK*.

Interface <wlan1></wlan1>		
General Wireless H	F WDS Nstreme NV2 Status Traffic	
Mode:	ap bridge 🗧 🗧	OK
Band:	2GHz-B/G ₹	Cancel
Channel Width:	20MHz Ŧ	Apply
Frequency:	2412 Ŧ MHz	Enable
SSID:	ATSWA AP BRIDGE	Comment
Scan List:	default 🔻 🕈	Advanced Mode
Wireless Protocol:	any 🔻	Torch
Security Profile:	default 🗧	WPS Accept
WPS Mode:	push button F	Scan
Bridge Mode:	enabled F	Freq. Usage
VLAN Mode:	no tag 두	Align
VLAN ID:	1	Sniff
Default AP Ty Bate:	▼ hns	Snooper
Default Client Tx Pate:	the	Reset Configuration
	· ups	
	Default Authenticate	
	Default Forward	

Jendela Wireless pada Interface Wireless Tables

Anda dapat memberikan password pada Access Point untuk memberikan fasilitas keamanan agar hanya pihak-pihak tertentu saja yang dapat terhubung. Caranya masuk ke menu *Security Profiles* pada *Wireless Tables* lalu klik "+" atau *Add*.

١	Vireless Tał	oles									
	Interfaces	Nstr	eme Dual	Access List	Registra	tion Connect Li	ist Security Pro	files Channels			
	+ -	T								Find	
	Name	- A	Mode	Auther	ticatio	Unicast Ciphers	Group Ciphers	WPA Pre-Shared	WPA2 Pre-Shared		•
	' default		none					*****	*****		
•	l item										
<u> </u>											

Jendela Security Profiles pada Wireless Tables

Metode keamanan pada perangkat wireless umumnya menggunakan metode authentication (WPA-PSK, WPA-AEP) dan Enkripsi (AES, TKIP, WEP)

Setelah masuk di jendela pengaturan *Security Profile* masukkan nama atau identitas *password* pada *name* lalu pilih enkripsi yang diinginkan pada *Autentication Types* lalu masukkan *Password* pada *Shared Key* lalu klik *Apply* lalu klik *OK*.

Security P	rofile <atsw< th=""><th>a></th><th></th><th></th></atsw<>	a>		
General	RADIUS	EAP	Static Keys	ОК
		Nam	e: atswa	Cancel
		Mod	e: dynamic keys 🔻	Apply
A	uthenticatio	n Type	s: VPA PSK VPA2 PSK WPA2 PSK WPA EAP	Сору
	Unicas	t Cipher	rs: 🗹 aes ccm 🗌 tkip	Remove
	Group	Cipher	rs: 🗹 aes ccm 🗌 tkip	
w	'PA Pre-Sha	ared Ke	y:	
WF	A2 Pre-Sha	ared Ke	y:	
	Supplican	t Identit	y:	
	Group Key	v Updat	e: 00:05:00	
Man	agement P	rotectio	n: allowed 🔻	
Manager	ment Protec	tion Ke	y:	

Jendela General pada Security Profile

Untuk melihat *Security Profile* atau *Password* yang telah dibuat dapat dilihat pada menu *Security Profiles Wireless Tables*.

Wireless Tables				
Interfaces Nstreme Dual A	ccess List Registration	Connect List Security Profiles	Channels	
+ - 7				Find
Name:	atswa	Mode:	dynamic keys	
Authentication Types: WPA PSK WPA2 PSK		Unicast Ciphers:	aes ccm	
Group Ciphers: aes ccm		WPA Pre-Shared Key:		
WPA2 Pre-Shared Key:		Group Key Update:	00:05:00	
Management Protection:	gement Protection: allowed			
MAC Authentication:	MAC Authentication: no		no	
EAP Accounting:	EAP Accounting: no		00:00:00	
MAC Format:	XX:XX:XX:XX:XX:XX	MAC Mode:	as usemame	
MAC Caching Time:	disabled	Key 0:		
Key 1:		Key 2:		
Key 3:		St. Private Key:		
2 items				

Jendela Security Profiles pada Wireless Tables

Selanjutnya adalah memasukkan *Security Profile* ke *Wireless Interface* dengan cara masuk kembali ke jendela pengaturan *Wireless Interface* dan pada bagian *Security Profile* mengubah dari konfigurasi *default* ke *profile* yang telah dibuat.

Interface <wlan1></wlan1>										
General Wireless H	T WDS	Nstreme	NV2	Status	Traffic					
Mode:	ap bridge		ОК							
Band:	2GHz-B/G							Cancel		
Channel Width:	20MHz F							Apply		
Frequency:	2412 ¥ MHz							Disable		
SSID:	ATSWA AP BRIDGE							Comment		
Scan List:	default 두 🗢						Advanced Mode			
Wireless Protocol:	any						₹	Torch		
Security Profile: atswa							WPS Accept			
WPS Mode:	WPS Mode: push button							Scan		
Bridge Mode:	enabled T						Freq. Usage			
VLAN Mode:	no tag						₹	Align		
VLAN ID:	1							Sniff		
Default AP Tx Bate:						•	bos	Snooper		
Default Client Tx Rate:						•	hne	Reset Configuration		
	_						opa			
	Defaul	Authentic	ate							
	Uefaul	Forward								
		010								
enabled	running		slav	e		running ap				

Jendela Wireless pada Interface Wireless Tables

Hasil konfigurasi pada *Interface List* dapat dilihat pada *Wireless Tables*.

Wireless Tab	bles										
Interfaces	Nstreme Dual	Access List	Registration	n Connect	List Security P	Profiles C	hannels				
+ -	< X 4	• 7	CAP	Scanner	Freq. Usage	Alignme	nt Wire	less Sniffer	Wirele	ss Snooper	Find
Name	A	Туре	T	x	Rx			Tx Packet (p	/s)	Rx Packet (p/s)	FP To 🔻
∲ wla	an1 \	Nireless (Ather	os AR9		0 bps		0 bps		0		0
+											•
1 item out of	f 5										

Jendela Interface pada Wireless Tables

Setelah itu konfigurasi IP Address untuk Wireless Interface.

A	ddress 🗸	Network	Interface	- I -
Df	192.168.1.253	192.168.1.0	ether1	
ť	192.168.2.1/24	192.168.2.0	wlan 1	

Jendela Address List

Agar *host* mendapatkan *IP Address* secara otomatis dari *Wireless Interface* maka konfigurasi *Wireless Interface* menjadi DHCP *Server*.



Jendela DHCP Server

Lakukan pengujian pada komputer dengan cara melihat *Access Point* yang sudah dibuat.



Daftar Access Point pada Komputer

Masukkan *Password* sesuai dengan *Security Profile* yang sudah dibuat.

(a	ATSWA AP BRIDGE									
	Enter the network security key									
	••••••									
	pushing the button on my contacts									
	Next	Cancel								

Menu untuk memasukkan Password

Setelah itu periksa pada komputer apakah sudah mendapatkan *IP Address* dari *AP Bridge*.



Jendela Network Connection pada Komputer

L4.2. STATION (PENERIMA)



Topologi Wireless Station

Untuk membuat penerima atau *Station Bridge* pada Mikrotik caranya masuk ke jendela konfigurasi *Wireless Interface* dengan cara klik *Wireless* lalu double klik *Wireless* yang ada pada *Interface List Wireless Tables*. Setalah masuk di jendela konfigurasi *Wireless Interface* klik *Scan*.

Canada	<wian i=""> Wireless</wian>	117	MDC	Network	MIV/2	Advanced	Charles	Charles		
General	Willeless	н	WDS	INSTREME	INV2	Advanced	Status	Status		ОК
	Mod	le: s	tation						•	Cancel
	Ban	nd: 2	GHz-B/	G					₹	Apply
С	hannel Wid	th: 2	0MHz						₹	Афріу
	Frequence	cy: 2	412					Ŧ	MHz	Enable
	SSI	D:	/likroTik						_ ▲	Comment
	Scan Li	ist: d	lefault						∓ \$	Advanced Mode
Wire	eless Protoc	ol: a	ny						Ŧ	Torch
S	ecurity Profi	ile: d	lefault						₹	WPS Accept
	WPS Mod	le: p	ush butt	on					₹	Scan
	Bridge Mod	le: e	nabled						Ŧ	Freq. Usage
	VLAN Mod	le: n	io tag						Ŧ	Align
	VLAN I	D: 1								Sniff
Defau	It AP Tx Rat	te:						•	bos	Snooper
Default (Client Tx Ra	te:							bps	Reset Configuration
		v	Defau	t Authentic	ate					
		14	Defaul	t Forward						

Jendela Wireless pada Interface Wireless Tables

Setelah itu klik *Start* lalu pilih *Access Point* yang akan dihubungkan lalu klik *Connect*. Pilih *Access Point* yang bukan MikroTik karena *Station* adalah konfigurasi untuk terhubung dengan *Access Point* perangkat selain MikroTik.

Scanner	(Running)								
Interface	e: wlan 1						₹	Star	t
								Stop	2
								Clos	e
								Conne	ect
								New Wi	ndow
	Address	CCID	Channel	Cient	Naiaa	Ciana	Dadia	Name	Per -
A	F4·F2·6D·8D·F4·7A	pitech hotspot	2432/2	-87	-114	3igna 27	naulo	Name	nuų +
AP	48:88:CA:BA:87:05	ATSWA 1	2437/2	-39	-110	71			
ARW	68:72:51:46:E7:B0	SEVEN 1 (08563	2417/2	-91	-115	24	AP SE	VEN 1	2.9.31
									_
•									•
3 items (1	selected)								

Jendela Wireless Scanner

Setelah itu pada jendela konfigurasi *Wireless Interface* akan muncul konfigurasi sesuai dengan konfigurasi pada *Access Point* terutama pada bagian band, *ferquency*, dan SSID. Setelah itu klik *Apply* lalu klik *OK*.
NGELAB MIKROTIK

nterface <wlan1></wlan1>		
General Wireless H	T HT MCS WDS Nstreme NV2 Advanced Status	OK
Mode	station	•
Band	2GHz-B/G/N	₹ Cancel
Channel Width:	20MHz	Apply
Frequency	2437 Ŧ N	1Hz Disable
SSID	ATSWA 1	▲ Comment
Scan List	default 🛛 🗸	Advanced Mode
Wireless Protocol	any	▼ Torch
Security Profile:	default	WPS Accept
WPS Mode:	push button	▼ Scan
Bridge Mode:	enabled	Freq. Usage
VLAN Mode:	no tag	∓ Align
VLAN ID:	1	Sniff
Default AP Ty Bate	▼	Snooper
		Reset Configuration
Derault Client IX Rate:	✓ Default Authenticate	ops
	☑ Default Forward	

Jendela Wireless pada Interface Wireless Tables

Jika *Access Point* yang sudah terhubung menggunakan *password*, buat terlebih dahulu *password* pada *Security Profile* yang sama agar dapat terhubung dengan cara klik "+" atau *Add* pada menu *Security Profiles*.

Security Profile <atswa></atswa>	
General RADIUS EAP Static Keys	ОК
Name: atswa	Cancel
Mode: dynamic keys	Apply
Authentication Types: VPA PSK VPA2 PSK WPA2 PSK WPA2 EAP	Сору
Unicast Ciphers: 🗹 aes ccm 🗌 tkip	Remove
Group Ciphers: ☑ aes ccm	
WPA Pre-Shared Key:	
WPA2 Pre-Shared Key:	
Supplicant Identity:	
Group Key Update: 00:05:00	
Management Protection: allowed	
Management Protection Key:	

Jendela Security Frofile pada Wireless Tabless

Setelah itu masukkan *profile* yang telah dibuat pada jendelan pengaturan *Wireless Interface* lalu klik *Apply* lalu klik *OK*.

NGELAB MIKROTIK

nterface	<wlan1></wlan1>	1								
General	Wireless	HT	HT MCS	WDS	Nstreme	NV2	Advanced	l Status		OK
	Mod	de: st	ation						∓	UK .
	Bar	nd: 2	GHz-B/G/I	N					Ŧ	Cancel
С	hannel Wid	th: 2	OMHz						Ŧ	Apply
_	Frequen	cy: 2	437					Ŧ	MHz	Disable
	SS	ID: A	TSWA 1						•	Comment
	Scan L	ist: de	efault					Ŧ	\$	Advanced Mode
Wire	eless Protoc	ol: a	ny						Ŧ	Torch
S	ecurity Prof	ile: at	tswa						Ŧ	WPS Accept
	WPS Mod	de: pu	ush button						₹	Scan
	Bridge Moo	de: er	nabled						Ŧ	Freq. Usage
	VLAN Mod	de: no	o tag						Ŧ	Align
	VLAN	ID: 1								Sniff
Defau	H AP Ty Ra	te:						•	hne	Snooper
										Reset Configuratio
Default (lient Ix Ra	te:						•	bps	
		-	Default A	uthentic	ate					
		V	Default F	orward						

Jendela Wireless pada Interface Wireless Tables

Pastikan *Wireless Interface* pada *Interface List* sudah dalam kondisi *R* atau *Running* atau berjalan.

Wireless Tab	les							
Interfaces	Nstreme Dual	Access List R	legistration Conn	nect List Security Pr	ofiles Channels			
+ •	× × 1	C	AP Scanner	Freq. Usage	Alignment Wire	eless Sniffer Wirel	ess Snooper	Find
Name	A	Туре	Tx	Rx		Tx Packet (p/s)	Rx Packet (p/s)	FP To 🔻
R 🚸wla	n1	Wireless (Atheros	AR9	0 bps	0 bps	0		0
•								٠
1 item out of	5							

Jendela Interface pada Wireless Tables

Jika *Access Point* tersebut menggunakan konfigurasi *DHCP Server* lakukan konfigurasi *DHCP Client* pada *Wireless Interface*.

DHCP Client							×
DHCP Client	DHCP Client Optic	ons					
+ - 🖉	× 🖻 1	R	lelease	Renew	1	Find	
Interface	∧ Use P	Add D.	IP Addr	BSS	Expires After	Status	-
wlan1	yes	yes	192.168	3.43.2	00:59:46	bound	
1 item							

DHCP Client List pada DHCP Client

Lakukan pengujian terhadap *Access Point* dengan menggunakan perintah *ping* atau periksa pada *Address List* untuk memastikan *Wireless Interface* sudah mendapatkan *IP Address*.



L4.3. STATION BRIDGE (PENERIMA)

Station Bridge adalah mode penerima khusus untuk menerima dari perangkat *Access Point* MikroTik. Untuk tahap konfigurasi tidak berbeda dengan konfigurasi sebelumnya hanya saja pastikan perangkat yang akan dihubungkan benar-benar perangkat MikroTik, umumnya perangkat MikroTik muncul dengan ID *APRB* atau *Access Point Routerboard*.

Scanner (Running)								
Interface	wlan1						₹	Star	t
								Stop	þ
								Clos	e
								Conn	ect
								New Wi	ndow
	Address	SSID	Channel	Signa	Noise	Signa	Radio	Name	Roi 🔻
APRB	6C:3B:6B:48:77:62	ATSWA 2	2412/2	-10	-111	101	6C3B6	6B487762	6.34.2
AP	48:88:CA:BA:87:05	ATSWA 1	2437/2	-41	-110	69			
•									•
2 items (1	selected)								

Jendela Wireless Scanner

Setelah itu pastikan pada jendela pengaturan *Wireless Interface* mode yang aktif adalah *Station Bridge*.

Topologi Wireless Station Bridge

NGELAB MIKROTIK

nterface <wlan1></wlan1>			1					
General Wireless H	T WDS	Nstreme	NV2	Advanced S	Status	Status		OK
Mode:	station br	dge					Ŧ	
Band:	2GHz-B/	G					Ŧ	Cancel
Channel Width:	20MHz						Ŧ	Apply
Frequency:	2412					Ŧ	MHz	Disable
SSID:	ATSWA	2					-	Comment
Scan List:	default						∓ \$	Advanced Mode
Wireless Protocol:	any						₹	Torch
Security Profile:	penerima						Ŧ	WPS Accept
WPS Mode:	push butt	on					₹	Scan
Bridge Mode:	enabled						Ŧ	Freq. Usage
VLAN Mode:	no tag						Ŧ	Align
VLAN ID:	1							Sniff
Default AP Ty Bate:							hns.	Snooper
Default Client Tx Rate:						-	bps	Reset Configuration
	✓ Defaul	t Authentic	ate					
	🗸 Defaul	t Forward						

Jendela Wireless pada Interface Wireless Tables

L4.4. VIRTUAL ACCESS POINT BRIDGE



Topologi Virtual AP Bridge

virtual access point adalah fitur untuk membuat access point lebih dari satu menggunakan satu wireless interface

Anda dapat membuat lebih dari 1 *Access Point* menggunakan MikroTik, istilah umumnya *Virtual Access Point*. Langkah membuat *Virtual Access Point* adalah dengan cara masuk ke *Wireless Tables* lalu masuk ke menu *Interface* dan klik "+" atau *Add*.

Wireless Tal	bles												
Interfaces	Nstreme Dual Acc	ess List Re	egistration Con	nect List Sec	urity Profiles	Channels							
+ -		T C/	AP Scanne	r Freq. Usa	ge Align	nment Wir	eless Sniffer	Wirel	ess Snooper			Fino	1
Virtu	ual AP		Tx		Rx		Tx Packet (p	/s)	Rx Packet (p/s)	FP Tx		FP Rx	•
WDS	5	ss (Atheros /	AR9	0 bps		0 bps		0		0	0 bps		0
Nstr	eme Dual												
	cine o dai												
•													*
1 item out of	f 5												

Menu Create Virtual AP pada Interface Wireless Tables

Seperti pada jendela *Wireless Interface* yang perlu dikonfigurasi adalah SSID serta *Master Wireless Interface* yang digunakan.

Interface <wlan2></wlan2>										
General Wireless W	/DS Status Traffic		ОК							
SSID:	ATSWA 4 - virtual 1	▲	Cancel							
Master Interface:	wlan1	Ŧ	Apply							
Security Profile:	default	Ŧ	Disable							
WPS Mode:	WPS Mode: disabled									
VLAN Mode:	Сору									
VLAN ID:	1		Remove							
Default AP Tx Rate:		▼ bps	Advanced Mode							
Default Client Tx Rate:		▼ bps	Torch							
	Default Authenticate Default Forward Hide SSID									
enabled	running	slave								

Jendela Wireless Interface

Virtual Access Point yang telah dibuat dapat dilihat di menu *Interface* pada *Wireless Tables*.

Wirel	ess Tables							□ ×			
Inter	faces Nstreme Dua	Access List Registrat	tion Connect List Sec	urity Profiles Channels							
+ •	+ ⊘ ⊗ CAP Scanner Freq. Usage Alignment Wireless Sniffer Wireless Snooper Find										
	Name 🗸	Туре	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx	FP Rx 🔻			
R	<i>♦ wlan1</i>	Wireless (Atheros AR9	0 bps	0 bps	0	0	0 bps	0			
	«-»wlan2	Virtual AP	0 bps	0 bps	0	0	0 bps	0			
	«-»wlan3	Virtual AP	0 bps	0 bps	0	0	0 bps	C			
	«->wlan4	Virtual AP	0 bps	0 bps	0	0	0 bps	0			
	«-≫wlan5	Virtual AP	0 bps	0 bps	0	0	0 bps	0			
•	•										
5 iter	ns out of 9										

Daftar Virtual Access Point pada Wireless Interface

Selain itu dapat dilihat pada komputer



Tampilan Access Point pada Komputer

LABORATORIUM 5





MIKROTIK BRIDGE

L5.1. WIRED BRIDGE

Bridge adalah layanan yang menghubungkan dua atau lebih interface agar seolah-olah berada dalam satu segmen jaringan yang sama



Topologi Wired Bridge

Jika Anda ingin menggabungkan dua jaringan menggunakan fasilitas *Bridge* pada *MikroTik* seperti topologi tersebut yang perlu dilakukan adalah konfigurasi *IP Address interface* yang menghubungkan komputer dan juga *router*.

• — 🖉 🖾	T	Find	1
Address /	Network	Interface	•
20.20.20.1/24	20.20.20.0	ether2	
+ 40.40.40.1/24	40.40.40.0	ether1	

IP Address pada Router 1

Setelah itu masuk ke menu *Bridge* lalu klik "+" atau *Add*

Bridge						
Bridge	e Ports F	Filters NAT Hosts				
÷		🛛 🖾 🏹 🛛 S	ettings			Find
	Name	∠ Туре	L2 MTU	Tx	Rx	1
4						*
0 items	s out of 5					

Jendela Bridge List pada Bridge

Setelah itu buat *Interface Bridge* dengan cara memberikan nama *Bridge* lalu klik *Apply* lalu klik *OK*.

Interface <bridge1></bridge1>		
General STP Statu	s Traffic	ОК
Name:	bridge1	Cancel
Type:	Bridge	Apply
MTU:	▼	Disable
Actual MTU:	1500	Comment
L2 MTU:	65535	Сору
MAC Address:		Remove
ARP:	enabled T	Torch
Admin. MAC Address:	▼	
enabled	running slave	

Jendela General pada Bridge

Setelah itu masuk ke menu *Port* pada *Bridge* dan buat *Port* baru dengan cara klik "+" atau *Add*.

Bridge							
Bridge Ports	Filters NAT	Hosts					
+ - 🖉	× 🖻	T					Find
Interface	∠ Bridge	9	Priority (h F	Path Cost	Horizon	Role	Root Pat 🔻
0.3							
Ulterns							

Jendela Port pada Bridge

Port yang pertama dibuat adalah Port yang menghubungkan
Ethernet ke Router dengan Bridge. Pada Interface pilih Ethernet
yang terhubung dengan Router dan pada Bridge pilih Interface
Bridge yang dibuat sebelumnya lalu klik Apply lalu klik OK.

Bridge Port <ethe< th=""><th>:r1></th><th></th><th></th><th></th></ethe<>	:r1>			
General Statu	s			ОК
Interface:	ether1	:	•	Cancel
Bridge:	bridge1	:	•	Apply
Priority:	80	h	вх	Disable
Path Cost:	10			Comment
Horizon:			•	Сору
Edge:	auto	:	Ŧ	Remove
Point To Point:	auto	:	Ŧ	
External FDB:	auto	:	Ŧ	
	Auto Isolate			
enabled		inactive		

Jendela konfigurasi Bridge Port pada Bridge

Port yang pertama dibuat adalah Port yang menghubungkan
Ethernet ke Komputer dengan Bridge. Pada Interface pilih Ethernet
yang terhubung dengan komputer dan pada Bridge pilih Interface
Bridge yang dibuat sebelumnya lalu klik Apply lalu klik OK.

Bridge Port <ethe< th=""><th>er2></th><th></th><th></th><th></th></ethe<>	er2>			
General Statu	s			ок
Interface:	ether2		Ŧ	Cancel
Bridge:	bridge1		₹	Apply
Priority:	80		hex	Disable
Path Cost:	10			Comment
Horizon:			•	Сору
Edge:	auto		Ŧ	Remove
Point To Point:	auto		∓	
External FDB:	auto		₹	
	Auto Isolate			
enabled		inactive		

Jendela konfigurasi Bridge Port pada Bridge

Setelah itu *port* yang telah dibuat dapat dilihat di *Port List* pada *Bridge*.

Bridge	•								
Bridg	e Ports	Filters	NAT	Hosts					
÷	- 0	*	1	T					Find
	nterface	Δ.	Bridge	э	Priority (h	Path Cost	Horizon	Role	Root Pat 🔻
:	t_tether1		bridge	e1	80	10		designated port	
:	t_tether2		bridge	e1	80	10		designated port	
2 item	าร								

Daftar Port Bridge yang telah dibuat pada Ports Bridge

Untuk menghubungkan *router* sisi lainnya lakukan langkah yang sama dimulai dengan memberikan *IP Address* pada *Ethernet* yang terhubung dengan *Router* dan *Ethernet* yang terhubung dengan Komputer. Dan membuat *Interface Bridge* serta *Port Bridge*.

ddress List] ×
+ - / ×	T	Find	
Address /	Network	Interface	•
÷20.20.20.2/24	20.20.20.0	ether2	
÷ 40.40.40.2/24	40.40.40.0	ether1	
T 40.40.40.2/24	40.40.40.0	etheri	
iteme			
items			

IP Address pada Router 2

L2.11. WIRELESS BRIDGE



Topologi Wireless Bridge

Jika Anda ingin menerapkan menggunakan media *Wireless* langkah yang dilakukan tidak jauh berbeda, Anda hanya perlu mengganti *Interface* yang digunakan saja dari *ethernet* ke *wireless ethernet*. Langkah pertama memberikan *IP Address* pada *Ethernet* yang akan dihubungkan ke komputer dan ke *Router Bridge*.



IP Address Pada Router 1

Setelah itu membuat *Interface Bridge* dan membuat *Port* yang menghubungkan *Ethernet* ke *Interface Bridge*.

Bridge									
Bridge	Ports	Filters	NAT	Hosts					
+ -	- 🖉	88		T					Find
Inte	erface	1	Bridg	e	Priority (h	Path Cost	Horizon	Role	Root Pat 🔻
11	ether1		bridge	e1	80	10		designated port	
11	wlan1		bridge	e1	80	10		designated port	
2 items									

Daftar Bridge pada Ports Bridge Router 1

Pada sisi *Router* yang lainnya juga dilakukan konfigurasi yang sama yaitu memberikan *IP Address* pada *Ethernet* yang akan dihubungkan ke Komputer dan ke *Router Bridge*.



IP Address pada Router 2

Setelah itu membuat *Interface Bridge* dan membuat *Port* yang menghubungkan *Ethernet* ke *Interface Bridge*.

Bridge						
Bridge Ports Filters	NAT Hosts					
+- / *	- 7					Find
Interface /	Bridge	Priority (h	Path Cost	Horizon	Role	Root Pat
1⊐tether1	bridge1	80	10		designated port	
1 ⊐twlan1	bridge1	80	10		designated port	
	unagu i					
2 items						

Daftar Bridge pada Ports Bridge Router 2

LABORATORIUM 6





MIKROTIK ROUTING

L6.1. STATIC ROUTING

Routing adalah suatu proses pengiriman dan pengambilan paket dari jaringan yang berbeda

Static Routing adalah konfigurasi *router* untuk menghubungkan jaringan berbeda dengan menggunakan alamat *network* dari jaringan dengan *gateway* dari *router* tersebut.



Topologi Static Routing

Jika Anda ingin menerapkan *static routing* sesuai topologi tersebut konfigurasi *Ethernet* yang terhubung dengan jaringan lokal dengan *ethernet* yang terhubung dengan *router* lainnya.

* =	T		Find
∠ Netwo	ork	Interface	
9 40.40	.40.0	ether1	
24 192.1	68.1.0	ether2	
	 ✓ Netwo 9 40.40 24 192.1 	Network 40.40.40.0 24 192.168.1.0	Network Interface 9 40.40.0 ether1 24 192.168.1.0 ether2

IP Address pada Router 1

	6 7	Find
Address /	Network	Interface
÷40.40.40.2/29	40.40.40.0	ether1
the second seco	192.168.2.0	ether2

IP Address pada Router 2

Setelah *IP Address* pada masing-masing *Router* dikonfigurasi selanjutnya membuat *Static Routing* dengan cara klik *IP* lalu klik *Router* lalu klik "+" atau *Add*.

Route Lis	st					[
Routes	Nexthops	Rules	VRF				
+ -	• 🖉 💥	400	7		Fin	d all	Ŧ
	Dst. Address	A	Gateway	Distance	Routing Mark	Pref. Source	-
DAC	40.40.40.	0/29	ether1 reachable	0		40.40.40.1	
DAC	192.168.1	.0/24	ether2 reachable	0		192.168.1.1	
2 items							

Router List pada Router 1

Masukkan *Network Address* beserta *Prefix* dari Jaringan tujuan pada *Dst. Address* dan memasukkan *Gateway* pada *Gateway*.

Route <192.168.2.	.0/24>				
General Attribute	es				ОК
Dst. Address:	192.168.2.0/24				Cancel
Gateway:	40.40.40.2	₹ reachable ether1		\$	Apply
Check Gateway:				•	Disable
Type:	unicast			₹	Comment
Distance:	1			_	Сору
Scope:	30				Remove
Target Scope:	10				
Routing Mark:				-	
Pref. Source:				•	
enabled			active		

Jendela untuk membuat Routing Statis

Setelah itu periksa pada *router list* dan pastikan sudah dalam Status *AS* dan *reachable*.

Route Li	st					[□×		
Routes	Nexthops	Rules	VRF						
+ -									
	Dst. Address	A	Gateway	Distance	Routing Mark	Pref. Source	-		
DAC	40.40.40	0/29	ether1 reachable	0		40.40.40.1			
DAC	192.168.	1.0/24	ether2 reachable	0		192.168.1.1			
AS	192.168.	2.0/24	40.40.40.2 reachable ether1	1					
3 items									

Router List pada Router 1

Untuk *router* sisi lainnya lakukan hal yang sama dengan masuk ke *Router List* lalu membuat list baru dan memasukkan *Network Address* serta *Prefix* dari *Network* tujuan dan *Gateway* dari *Router* tujuan.

Route List					[×	
Routes Nexthop	s Rules	VRF					
Dst. Addre	ss 🛛	Gateway	Distance	Routing Mark	Pref. Source	•	
DAC 40.40.4	0.0/29	ether1 reachable	0		40.40.40.2		
DAC > 192.16	8.2.0/24	ether2 reachable	0		192.168.2.1		
2 items							

Router List pada Router 2

Route <192.168.1.	0/24>	
General Attribute	15	ОК
Dst. Address:	192.168.1.0/24	Cancel
Gateway:	40.40.1	Apply
Check Gateway:	v	Disable
Type:	unicast 🛛 🔻	Comment
Distance:	1	Сору
Scope:	30	Remove
Target Scope:	10	
Routing Mark:		
Pref. Source:	▼	
enabled	active	

Jendela untuk membuat Routing Statis

Setelah itu periksa hasil konfigurasi pada *Router List* bahwa kondisi sudah *AS* dan *reacable*.

Route Li	ist						
Routes	Nexthops	Rules	VRF				
	Dst. Address	Δ	Gateway	Distance	Routing Mark	Pref. Source	•
DAC	40.40.40.0	/29	ether1 reachable	0)	40.40.40.2	
AS	192.168.1.	0/24	40.40.40.1 reachable ether1	1			
DAC	192.168.2.	0/24	ether2 reachable	0		192.168.2.1	
3 items							

Router List pada Router 2

Untuk menguji apakah jaringan yang berbeda sudah saling terhubung lakukan pengujian dengan perintah *ping* dari komputer yang berada pada jaringan satu ke jaringan lainnya

L6.2. DINAMIC ROUTING (RIPv2)

Dinamic Routing adalah konfigurasi *router* untuk menghubungkan jaringan berbeda menggunakan alamat *network* dari jaringan yang terhubung dengan *router* tersebut



Topologi Dinamic Routing RIPv2

Pertama lakukan konfigurasi *IP Address* pada masing-masing *router* sesuai topologi tersebut.



IP Address pada Router 1 dan Router 2

Setelah itu klik menu *Router* lalu klik *RIPv2* lalu klik *Interface* lalu klik *Add* atau "+" lalu pilih interface yang terhubung dengan jaringan yang akan di *routing*. Sesuai dengan topologi yang digunakan maka *interface* yang digunakan adalah *interface* **ether1** da **ether2**.

terfaces N	letworks	Keys	Neighbours	Routes					
	/ 🐹	7	RIP Settings						Find
Interface	1	Receiv	re Send	Authentic.	Authenticati	Key Chain	Passive	In Prefix L	Out Prefix
A ether		v1-2	v1-2	none			no		
Nº ether?		v1-2	v1-2	none			no		

Daftar Interface yang digunakan pada R1

Setelah itu klik *Networks* klik *Add* atau "+" lalu masukkan *Network Address* tujuan yang akan di *routing*.

RIP					□ ×
Interfaces	Networks	Keys	Neighbours	Routes	
+		7			Find
Address	Δ.				-
▶ 10.1	0.10.0/24				
192.	168.1.0/24				
2 items					

Network Address pada R1

RIP					
Interfaces	Networks	Keys	Neighbours	Routes	
+ -		7			Find
Address	Δ.				-
▶ 10.1 ▶ 192.	0.10.0/24 168.2.0/24				
2 items					

Network Address pada R2

Untuk melihat konfigurasi *routing* yang telah dibuat Anda dapat melihat di *Router List.* Pastikan *ethernet* dalam kondisi *DAr* dan *reachable.*

Route L	jist					[
Routes	Routes Nexthops Rules VRF									
+										
	Dst. Address	A	Gateway	Distance	Routing Mark	Pref. Source	•			
DAC	10.10.10	.0/24	ether1 reachable	0		10.10.10.1				
DAC	192.168.	1.0/24	ether2 reachable	0		192.168.1.1				
DAr	192.168.3	2.0/24	10.10.10.2 reachable ether1	120						
3 items										

Route List pada R1

Route					[
Route	s Nexthops Rules	VRF							
+									
	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source	•			
DAC	10.10.10.0/24	ether1 reachable	0		10.10.10.2				
DAr	192.168.1.0/24	10.10.10.1 reachable ether1	120						
DAC	192.168.2.0/24	ether2 reachable	0		192.168.2.1				
3 items	3								

Route List pada R2

Jika diperlukan lakukan pengujian dari komputer yang terhubung dengan router R1 dengan R2 mengunakan ping.

L6.3. DINAMIC ROUTING (OSPF)



Topologi Dinamic Routing OSPF

Pertama konfigurasi *IP Address* masing-masing *router* sesuai topologi tersebut.

Address List			×	A	ddress List			[×
+- ** =	T	Find		4	• — 🖉 🗶 É		T	Find	
Address /	Network	Interface	-		Address	. I	Network	Interface	-
+ 40.40.40.1/24	40.40.40.0	ether1			÷40.40.40.2/24		40.40.40.0	ether1	
192.168.1.1/24	192.168.1.0	ether2			192.168.2.1/24		192.168.2.0	ether2	
2 items				2	items				

Konfigurasi IP Address R1 dan R2

Setelah itu klik *Routing* klik *OSPF* klik *Instances* double klik rules *default* pada *Instances list* lalu ubah Router ID. Router ID R1 1.1.1.1 dan R2 2.2.2.2

NGELAB MIKROTIK

OSPF Instance <default></default>			OSPF Instance <default></default>	
General Metrics MPLS Statu	s	ОК	General Metrics MPLS Status	ОК
Name:	default	Cancel	Name: default	Cancel
Router ID:	1.1.1.1	Apply	Router ID: 2.2.2.2	Apply
Redistribute Default Route:	never Ŧ	Disable	Redistribute Default Route: never	Disable
Redistribute Connected Routes:	no Ŧ	Comment	Redistribute Connected Routes: no	Comment
Redistribute Static Routes:	no Ŧ	Сору	Redistribute Static Routes: no	Сору
Redistribute RIP Routes:	no Ŧ	Remove	Redistribute RIP Routes: no	Remove
Redistribute BGP Routes:	no Ŧ		Redistribute BGP Routes: no	
Redistribute Other OSPF Routes:	no Ŧ		Redistribute Other OSPF Routes: no 🔻	
In Filter:	ospf-in 🔻		In Filter: ospf-in	
Out Filter:	ospf-out Ŧ		Out Filter: ospf-out	
enabled	default		enabled default	

Konfigurasi Router ID pada R1 dan R2

Setelah itu masuk klik menu *Network* lalu klik "+" atau *Add* lalu masukkan *Network Address* yang ada pada *network* dan pada *Area* pilih *backbone*.

OSPF Network <40.40.40.0/24>			OSPF Network <19	2.168.1.0/24	> IX
Network: 40.40.40.0/24	ОК		Network: 192.168	3.1.0/24	ОК
Area: backbone 🗧	Cancel		Area: backbo	ne Ŧ	Cancel
	Apply				Apply
	Disable				Disable
	Comment				Comment
	Сору				Сору
	Remove				Remove
enabled			enabled		

Konfigurasi pada R1

OSPF Network <40.40.40.0/24>		OSPF Netv	vork <192.1	68.2.0/24	> IX
Network: 40.40.40.0/24	ОК	Network:	192.168.2.	0/24	ОК
Area: backbone 🔻	Cancel	Area:	backbone	Ŧ	Cancel
	Apply				Apply
	Disable				Disable
	Comment				Comment
	Сору				Сору
	Remove				Remove
enabled		enabled			

Konfigurasi pada R2

Setelah itu periksa menu *Neighbors* pada **R1** dan pastikan **Router ID R2** sudah muncul dan juga sebaliknya pastikan pada *Neighbors* **R2 Router ID R1** sudah muncul.

OSPF									×
Virtual Links	Neighbors	NBMA Neighbors	Sham Links	LSA	Routes	AS Bo	rder Routers		
T								Find	
Instance /	Router ID	Address	Interface		State Ch	anges			Ŧ
🕏 default	2.2.2.2	40.40.40.2	ether1			5			
1 item									

Neighbors pada Router R1

OSPF							
Virtual Links	Neighbors	NBMA Neighbor	rs Sham Li	inks LS/	A Routes	AS Bo	rder Routers
T							Find
Instance 🛆	Router ID	Address	Inte	face	State Ch	anges	•
default	1.1.1.1	40.40.40	1 ethe	er1		5	
1 item							

Neighbors pada *Router* R2

Setelah itu masuk ke *Router List* untuk melihat konfigurasi routing sudah berhasil atau belum

Pouto		VDE			l	
noute	s Nexthops Rule	S VRF				
+	- 🖉 🗶 🖻	T		Fit	nd all	1
	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source	•
DAC	40.40.40.0/24	ether1 reachable	0		40.40.40.1	
DAC	192.168.1.0/24	ether2 reachable	0		192.168.1.1	
DAo	192.168.2.0/24	40.40.40.2 reachable ether1	110			
3 items						

Router List pada R1

Routes	Nexthops Rules	VRF			
+	- 🖉 💥 🖻	T		Fil	nd all
	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
DAC	40.40.40.0/24	ether1 reachable	0		40.40.40.2
DAo	192.168.1.0/24	40.40.40.1 reachable ether1	110		
DAC	192.168.2.0/24	ether2 reachable	0		192.168.2.1

Router List pada R2

Jika diperlukan lakukan pengujian dari komputer yang terhubung dengan router R1 dengan R2 mengunakan ping.

LABORATORIUM 7





MIKROTIK TUNNEL

L7.1. IPIP TUNNEL

IPIP bekerja dengan melakukan enkapsulasi paket data dari suatu ip ke ip lainnya dan membentuk sebuah tunnel



Topologi IPIP Tunnel

Pertama konfigurasi *IP Address* pada *Router* **R1** dan **R2** sesuai dengan topologi tersebut.

Address List			×	A	ldress List		[×
+- < =	T	Find		4		T	Find	
Address /	Network	Interface	-		Address /	Network	Interface	_
宁 40.40.40.1/24	40.40.40.0	ether1			÷40.40.40.2/24	40.40.40.0	ether1	
192.168.1.1/24	192.168.1.0	ether2			192.168.2.1/24	192.168.2.0	ether2	
2 items				2	tems			

IP Address pada Router **R1** dan **R1**

Setelah itu klik *Interface* lalu klik "+" atau *Add* dan masukkan *IP Address (Local/Asal dan Remote/Tujuan*) sesuai dengan Topologi lalu klik *Apply* klik *OK*.

NGELAB MIKROTIK

Interface <ipip-tunn< th=""><th>iel1></th><th></th><th></th><th></th><th></th></ipip-tunn<>	iel1>				
General Status	Traffic				ок
Name:	ipip-tun	nel1			Cancel
Туре:	IP Tunr	nel			Apply
MTU:			•		Disable
Actual MTU:	1480				Comment
L2 MTU:	65535				Сору
Local Address:	40.40.4	0.1	-		Remove
Remote Address:	40.40.4	0.2		 	Torch
IPsec Secret:			•		
Keepalive:			-		
DSCP:	inherit		₹		
Dont Fragment:	no		₹		
	Clam	p TCP MSS			
	✓ Allow	v Fast Path			
enabled		running	slave		

Konfigurasi IPIP Tunnel pada Router **R1**

Interface <ipip-tunn< th=""><th>el1></th><th></th><th></th><th></th></ipip-tunn<>	el1>			
General Status	Traffic			ОК
Name:	ipip-tuni	nel1		Cancel
Туре:	IP Tunr	nel		Apply
MTU:			▼ '	Disable
Actual MTU:	1480			Comment
L2 MTU:	65535			Сору
Local Address:	40.40.4	0.2		Remove
Remote Address:	40.40.4	0.1		Torch
IPsec Secret:			•	
Keepalive:			•	
DSCP:	inherit		₹	
Dont Fragment:	no		₹	
	Clam	p TCP MSS		
	Allow	/ Fast Path		
enabled		running	slave	

Konfigurasi IPIP Tunnel pada Router **R2**

Address <1.1.1.1>		Address <2.2.2>	
Address: 1.1.1.1	ОК	Address: 2.2.2.2	ОК
Network: 2.2.2.2	Cancel	Network: 1.1.1.1	Cancel
Interface: ipip-tunnel1 Ŧ	Apply	Interface: ipip-tunnel1 ₹	Apply
	Disable		Disable
	Comment		Comment
	Сору		Сору
	Remove		Remove
enabled		enabled	

IP Address (IPIP Tunnel) pada R1 dan R2

Setelah itu masuk ke *Route List* dan tambahkan *routing* pada **R1** dan R2. Pada Router R1 masukkan *IP Network Address* tujuan (**R2**) pada **Dst Address** dan *IP Tunnel* pada **Gateway** dan pada Router R2 juga sebaliknya. Setelah itu klik **Apply** dan klik **OK**.

Route <192.168.2.	0/24>			
General Attribute	es			ОК
Dst. Address:	192.168.2.0/24			Cancel
Gateway:	2.2.2.2	▼ reachable ipip-tunnel1	\$	Apply
Check Gateway:			▼	Disable
Type:	unicast		₹	Comment
Distance:	1			Сору
-				Remove
Scope:	30			
Target Scope:	10			
Routing Mark:			•	
Pref. Source:			•	
enabled			active	

Konfigurasi di Router **R1**

Route <192.168.1.	0/24>			
General Attribute	es			ОК
Dst. Address:	192.168.1.0/24			Cancel
Gateway:	1.1.1.1	▼ reachable ipip-tunnel1	\$	Apply
Check Gateway:			•	Disable
Type:	unicast		Ŧ	Comment
Distance	1			Сору
Scope:	30]	Remove
Target Scope:	10			
Routing Mark:				
Pref. Source:			•	
enabled			active	

Konfigurasi di Router R2

Pastikan hasil *routing* pada router *R1* dan *R2* dalam kondisi AS.

Route Li	ist						
Routes	Nexthops F	Rules	VRF				
+ -	- 🖉 🐹	2 12	T		Fil	nd all	₹
	Dst. Address	A	Gateway	Distance	Routing Mark	Pref. Source	•
DAC	2.2.2.2		ipip-tunnel1 reachable	0		1.1.1.1	
DAC	40.40.40.0/	24	ether1 reachable	0		40.40.40.1	
DAC	192.168.1.0)/24	ether2 reachable	0		192.168.1.1	
AS	192.168.2.0)/24	2.2.2.2 reachable ipip-tunnel1	1			
1 itame							

Route List Router **R1**

Route L	ist				[
Routes	Nexthops Rule	VRF				
+	- 🖉 🖾 🖻	T		Fi	nd all	₹
	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source	-
DAC	▶ 1.1.1.1	ipip-tunnel1 reachable	0		2.2.2.2	
DAC	40.40.40.0/24	ether1 reachable	0		40.40.40.2	
AS	192.168.1.0/24	1.1.1.1 reachable ipip-tunnel1	1			
DAC	192.168.2.0/24	ether2 reachable	0		192.168.2.1	
4 itoma						
4 items						

Route List Router **R2**

Jika diperlukan lakukan pengujian dari komputer yang terhubung dengan *router* **R1** dengan **R2** mengunakan ping

L7.2. PPPoE TUNNEL



Topologi PPPoE Server dan Client

Langkah pertama yang dilakukan dalam membuat jaringan PPPoE adalah membuat Server PPPoE lalu membuat PPPoE Client. PPPoE Client dapat berupa Router atau Komputer. Langkah membuat **PPPoE Server** dengan klik **PPP** lalu klik **PPPoE Servers** lalu klik **Add** atau "+".

PPP	
Interface PPPoE Servers Secrets Profiles Active Connections L2TP Secrets	
	Find
Service / Interface Max MTU Max MRU MRRU Default Profile Authentication	▼
0 items	

Jendela PPPoE Server pada PPP

Setelah itu buat nama *PPPoE Server* pada *Service Name* dan pilih *Interface* yang digunakan lalu klik *Apply* klik *OK*.

New PPPoE Service		
Service Name:	atswa_server_pppoe	ок
Interface:	ether2	Cancel
Max MTU:	1480	Apply
Max MRU:	1480	Disable
MRRU:	1600	Сору
Keepalive Timeout:	10	Remove
Default Profile:	default	:
	One Session Per Host	
Max Sessions:		•
Authentication:	✓ mschap2 ✓ mschap ✓ chap ✓ pap	1
enabled		

Jendela PPPoE Service

Setelah itu klik Secrets klik Add atau "+"

PPP								
Interface	PPPoE Servers	Secrets Pr	ofiles Active Co	nnections L	2TP Secrets			
+ -		PP PP	P Authentication8	Accounting]			Find
Name	A Password	Service	Caller ID	Profile	Local Address	Remote Address	Last Logged Out	-
0 items								

Jendela Secrets pada PPP

Pada jendela pengaturan *PPP Secret* buat **User** dengan memasukkan *name, password, service, local address,* dan *remote address* lalu klik **Apply** klik **OK**.

New PPP Secret			
Name:	peserta_a	ונ	ОК
Password:	123456	•	Cancel
Service:	pppoe Ŧ	:	Apply
Caller ID:			Disable
Profile:	default	;	Comment
Local Address:	40.40.40.1		Сору
Remote Address:	40.40.40.2	•	Remove
Routes:			
Limit Bytes In:		-	
Limit Bytes Out:	•		
Last Logged Out:			
enabled			

Jendela PPP Secret

Setelah selesai membuat *PPPoE Server* selanjutnya melakukan konfigurasi pada sisi *Client*. Jika sisi Client yang Anda inginkan adalah Komputer caranya ke *Network and Sharing Center* lalu klik *Set up a new connection or network*.

	Network and Sharing C	enter
) 🍥 👻 🕇 🔡 « All Cont	rol Panel Items > Network and Sharing Center	✓ ♂ Search Control Panel
Control Panel Home	View your basic network information	and set up connections
Change adapter settings	View your active networks	
Change advanced sharing settings	Unidentified network Public network	Access type: No Internet access Connections: U Ethernet
	Change your networking settings	· · · · · · · · · · · · · · · · · · ·
	Set up a new connection or network Set up a broadband, dial-up, or VPN c	onnection; or set up a router or access point.
	Troubleshoot problems Diagnose and repair network problem	s, or get troubleshooting information.
See also		
HomeGroup		
Internet Options		

Jendela Network and Sharing Center

Lalu klik *Connect to the Internet* lalu klik *Next*.

Connect to the Internet Set up a broadband or dial-up connection to the In	nternet.
Set up a new network Set up a new router or access point.	
Manually connect to a wireless network Connect to a hidden network or create a new wirel	less profile.
Connect to a workplace Set up a dial-up or VPN connection to your workpl	lace.

Jendela Connection or Network

Klik **Broadband (PPPoE)** dan masukkan **username** dan **password** sesuai dengan *user* yang telah dibuat pada **PPP Secrets** lalu klik **Connect** dan tunggu hingga terhubung.

Connect to the Internet	- • ×
How do you want to connect?	
Broadband (PPPoE) Connect using DSL or cable that requires a user name and password.	
\square Show connection options that this computer is not set up to use	
	Cancel

Jendela Connection or Network

📀 🤏 Connect to the Int	- 🗆 🗙
Type the information	n from your Internet service provider (ISP)
User name:	peserta_a
Password:	123456
	✓ Show characters ✓ Remember this password
Connection name:	Broadband Connection
Allow other people This option allows I don't have an ISP	t o use this connection anyone with access to this computer to use this connection.
	Connect Cancel

Jendela Connection or Network

S S Connect to the Internet	- • ×
Creating your Internet connection	
i 🔍 ———— (
	Cancel

Proses terhubung dengan PPPoE Server



Pemberitahuan koneksi PPPoE berhasil

Untuk memastikan koneksi berhasil dan sesuai dengan konfigurasi yang dilakukan pada *PPPoE Server* periksa *IP Address* yang diperoleh pada *Ethernet* Komputer.

8	Network and Sharing Center	er – 🗆 🗙				
🔄 🍥 🕤 🕈 ີ 🖳 « All Contr	ol Panel Items > Network and Sharing Center	✓ ♂ Search Control Panel				
Control Panel Home	View your basic network information and set up connections View your active networks					
Change adapter settings Change advanced sharing settings	Network 4 Public network	Access type: Internet Connections: Broadband Connection				
	Unidentified network Public network	Access type: No Internet access Connections: 🔋 Ethernet				
	Change your networking settings Set up a new connection or network Set up a broadband, dial-up, or VPN conne Troubleshoot problems Diagnose and repair network problems, or	ection; or set up a router or access point. get troubleshooting information.				
See also HomeGroup Internet Options Windows Firewall						

Jendela Network and Sharing Center

Broadband Connection Status	×	Network	Connection Details
General Details		Network Connection Details	
Connection		Property	Value
IPv4 Connectivity:	Internet	Connection-specific DN	
IPv6 Connectivity: No network	rk access	Description	Broadband Connection
Media State: Co	onnected	Physical Address	Ne
Duration: 0	00:00:50	IPv4 Address	40 40 40 2
Speed: 100	0.0 Mbps	IPv4 Subnet Mask	255.255.255.255
Details		IPv4 Default Gateway	
Dectails		IPv4 DNS Server	192.168.43.1
Activity		IPv4 WINS Server	
Sent — 🛒 — R	Received	NetBIOS over Tcpip En	No
Bytes: 170.713	190.677		
Compression: 0 %	0 %		
Errors: 0	0		
Properties Disconnect Diagnose			
Г			Clos
	Close		

Connection Status pada Network Connection

LABORATORIUM 8





NETWORK MANAGEMENT

_ _



L8.1. WIRELESS MAC ADDRESS FILTERING

Topologi Wireless MAC Address Filtering

Untuk mencegah perangkat lain terhubung dapat memanfaatkan fitur MAC Filtering dengan cara masuk ke menu **Registration** *Wireless Tables* pada *Router AP Bridge* dan *Router Station Bridge*. Setelah itu double klik Wireless interface yang akan digunakan.

Media Access Control (MAC) Address adalah alamat fisik suatu interface jaringan yang bersifat unik dan berfungsi sebagai identitas perangkat tersebut



Jendela Registration pada Wireless Tables Router AP Bridge

Pada AP Bridge pilih Copy to Access List.

NGELAB MIKROTIK

AP Client <6C:3B:6B:4	48:77:08>					
General 802.1x S	Signal Nstr	reme 1	VV2	Statistics	;	OK
Radio Name:	6C3B6B487	7708				Remove
MAC Address:	6C:3B:6B:4	48:77:08				Reset
Interface:	wlan1					Copy to Access List
Uptime:	00:00:13					Copy to Connect List
Distance:						Ping
RouterOS Version:	6.34.2					MAC Ping
AP Tx Limit:						Telnet
Client Tx Limit:						MAC Telnet
Last IP:	40.40.40.2					Torch
	AP					
[
[Compres	ssion				
[WMM Er	nabled				

Jendela General AP Client pada Router AP Bridge

Wireless Tab	bles									
Interfaces	Nstreme Dual Access Lis	Registration	Connect List	Security P	Profiles Char	nnels				
- 7	00 Reset									Find
Radio Nam	e 🔺 MAC Address	Interface	Uptime A	P W	Last Activit	. Tx/Rx Signal	Tx Rate	Rx Rate		-
6C3B6E	34 6C:3B:6B:48:77:62	wlan1	00:01:01 y	es no	0.460) -11/-11	5.5Mbps	1Mbps		
1 item										

Jendela Registration pada Wireless Tables Router Station Bridge

Pada Station Bridge pilih Copy to Connect List.

AP Client <6C:3B:6B	:48:77:62>	
General 802.1x	Signal Nstreme NV2 Statistics	ОК
Radio Name:	6C3B6B487762	Remove
MAC Address:	6C:3B:6B:48:77:62	Reset
Interface:	wlan1	Copy to Access List
Uptime:	00:01:29	Copy to Connect List
Distance:		Ping
RouterOS Version:	6.34.2	MAC Ping
AP Tx Limit:		Telnet
Client Tx Limit:		MAC Telnet
Last IP:	40.40.40.1	Torch
	AP WDS Compression	
	WMM Enabled	

Jendela General AP Client pada Router Station Bridge

L8.2. WIRELESS NSTREME



Untuk mengkonfigurasi *Nstreme* pada bagian *AP Bridge* masuk ke menu *Nstreme* pada *Wireless Interface*. Aktifkan *ceklist* pada *Enable Nstreme* pada *Framer Policy* pilih *dynamic size* dan pada frame limit masukkan nilai 500 lalu klik *Apply* lalu **OK**.

Interface <wlan1></wlan1>				
General Wireless H	T WDS Nstreme	NV2 Status Traffic		
✓ Enat	ole Nstreme			ок
💌 Enat	ole Polling			Cancel
Disa	ble CSMA			Apply
Framer Policy: dynamic	c size		₹	Disable
Framer Limit: 500				Connect
				Comment
				Advanced Mode
				Torch
				WPS Accept
				Scan
				Freq. Usage
				Align
				Sniff
				Snooper
				Reset Configuration
enabled	running	slave	running ap	

Jendela Nstreme pada Router AP Bridge

Pada bagian *Station Bridge* cukup mengaktifan degan cara ceklist Enable Enstreme lalu klik *Apply* lalu klik **OK**.
Interface <wlar< th=""><th>1></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></wlar<>	1>							
Wireless HT	WDS	Nstreme	NV2	Advanced Status	Status	Traffic		01/
	🖌 Enat	ole Nstreme						UK
	🗸 Enat	ole Polling						Cancel
	Disa	ble CSMA						Apply
Framer Policy:	none						Ŧ	Disable
	3200							Comment
								Advanced Mode
								Torch
								WPS Accept
								Scan
								Freq. Usage
								Align
								Sniff
								Snooper
								Reset Configuration

Jendela Nstreme pada Router Station Bridge

L8.3. HOTSPOT

Untuk membuat *hotspot* caranya klik IP klik *Hotspot* klik *Server* klik *Add* atau "+".

Hot	spot									
Se	rvers	Server Profiles	Users	User Profiles	Active	Hosts	IP Bindings	Service Ports	Walled Garden	Walled Garden IP List
÷	-	X	R	eset HTML	Hotspot	Setup				Find
	Name	e .	Interfa	ace	Address	Pool	Profile	Addresses		•
0 it	ems									

Menu Hotspot Server

Lalu klik *Hotspot Setup* tentukan *interface* yang akan digunakan pada *Hotspot Interface*, masukkan IP *Address* yang digunakan pada *Local Address of Network*, tentukan IP *Address* yang diberikan kepada *User* pada Address Pool of Network, tentukan DNS Server yang digunakan pada DNS *Servers*, tentukan domain yang digunakan pada DNS Name, dan buat satu *User* yang digunakan untuk masuk ke *Hostpot*.

Hotspot Setup	Hotspot Setup
Select interface to run HotSpot on	Set HotSpot address for interface
HotSpot Interface: ether2	Local Address of Network: 192.168.2.2/24
	Masquerade Network
Back Next Cancel	Back Next Cancel

Hotspot Setup		Hotspot Setup	Г
Set pool for HotSpot addresses		Select hotspot SSL certificate	
Address Pool of Network: 68.2.3-192.1	168.2.254 🗢	Select Certificate: none	
Back Next	Cancel	Back	ext Canc
Hotspot Setup		Hotspot Setup	[
Select SMTP server		Setup DNS configuration	
IP Address of SMTP Server: 0.0.0.0		DNS Servers: 8.8.8.8	
		8.8.4.4	
Back Next	Cancel	Back	ext Cance
Hotspot Setup		Hotspot Setup	[
DNS name of local hotspot server		Create local HotSpot user	
DNS Name: atswa.co.id		Name of Local HotSpot User: p	eserta
		Password for the User: p	eserta
Back Next	Cancel	Back	ext Cance
Hotspot Setup			
Setup has completed successful	ly		

Pengaturan Hotspot Setup

Hotspot Server yang dibuat dapat dilihat di *Server List* pada menu *Servers, Profile* yang dibuat dapat dilihat pada menu *Server Profiles,* dan *User* yang dibuat dapat dilihat di menu **Users**.

Hotspot										
Servers	Server Profiles	Users	User Profiles	Active	Hosts	IP Bindings	Service Ports	Walled Garden	Walled Garden IP List	
+ -	V 💥 🍸	R	eset HTML	Hotspot	Setup]				Find
Name	a J	Interf	ace	Address	Pool	Profile	Addresses			•
💮 he	otspot1	ether	2	hs-pool-	2	hsprof1	2	2		
1 item										

Menu *Servers* pada *Hotspot*

Hotspot									[×
Servers	Server Profiles	Users	User Profiles	Active	Hosts	IP Bindings	Service Ports	Walled Garden	Walled Garden IP List	
+ -	T								Find	
Name	A D	NS Name	HTML Di	rectory	Rate	Limit (rx/tx)				•
* 😗 defa	ult		hotspot							
A hspr	of1 a	tswa.co.id	hotspot							
2 items										

Menu Server Profile pada Hotspot

+ - <	× 🖻 🍸	00 Reset Count			1		
				leset All Counters			Find
Server	∧ Name	Address	N	IAC Address	Profile	Uptime	
;;; counters a	nd limits for trial users						
🚱 all	default-trial				unknown	00:00:00	
🚱 all	peserta				default	00:00:00	

Menu User pada Hotspot

Hubungkan Komputer dan lakukan pengujian dengan cara mengakses *internet* melalui *web browser*, jika konfigurasi *hotspot* sudah benar maka *browser* akan langsung masuk ke *hotspot gateway* yang sudah dibuat dan menampilkan menu untuk memasukkan user name dan password yang telah dibuat.



Halaman Hotspot Gateway

Setelah user melakukan login,

← → C D atswa co id/	login			~ =		
	nogin			<u> </u>		
	Welcome	e peserta!				
	IP address:	192.168.2.254				
	bytes up/down:	0 B / 0 B				
	connected: Os					
	status refresh:	1m				
	log	off				
	log	UII				
🕂 🚞 👩 🍕	🧭 🚫	0:N	() P 🕆 🗘 🖓	6:25		
				20/02/2017		

Halaman yang muncul setelag user berhasil login

LABORATORIUM 9





NETWORK SIMULATION

_ _

L9.1. INSTALASI LOOPBACK ADAPTER GNS3 DI WINDOWS

Jika Anda ingin menghubungkan GNS3 dengan Komputer maka perlu dibuat loopback adapter.

loopback adapter adalah sebuah perangkat virtual yang diimplementasikan dalam perangkat lunak dan tidak terhubung ke perangkat keras, namun terintegrasi dalam jaringan komputer

Dengan adanya loopback adapter Anda dapat melakukan konfigurasi atau pengujian menggunakan aplikasi seperti command prompt, winbox, dan lain sebagainya. Untuk membuat loopback adapter pada sistem operasi windows caranya dengan masuk ke *Hardware Wizard* dengan cara mengetikkan *hdwwiz* pada run.



Jendela run pada windows

Setelah muncul jendela Add Hardware Wizard lalu klik Next



Jendela pengaturan

Setelah itu pilih *Search for and install the hardware automatically* lalu klik *Next*.



Jendela pengaturan

Klik **Next**.

The	he wizard did not find any new hardware on your computer								
	If you know the list.	pecific hardwa	re model you	want to in	stall, click l	Next to sele	ct it fron	n a	
					< Back	Next :	,	Cancel	

Jendela pengaturan

Setelah itu pilih *Network Adapter* pada *Hardware Category* lalu klik *Next*.

Fre	m the list below, select the type of hardware you are installing	
	If you do not see the hardware category you want, click Show All Devices.	
	Common hardware types:	
	Memory technology devices	-
	Miracast display devices	
	Modems	
	Network adapters	_
	PCMCIA adapters	
	Portable Devices	
	Ports (COM & LPT)	
	POS HID Barcode scanners	

Pengaturan

Setelah itu pilih *Microsoft* pada *Manufacture* dan pilih *Microsoft KM-TEST Loopback Adapter* pada *Model* lalu klik *Next*.

 Soloct the manufacturer 	rand model of your bardware device and then a	lick Next If you have a
disk that contains the di	river you want to install, click Have Disk.	LICK INEXC. IF you have a
Manufacturer	^ Model	^
Marvell Semiconductor. Inc.	Microsoft IP-HTTPS Platform Adapter	r
Marvell Semiconductor. Inc. Mellanox Technologies Ltd.	Microsoft IP-HTTPS Platform Adapter	r
Marvell Semiconductor. Inc. Mellanox Technologies Ltd. Microsoft	Microsoft IP-HTTPS Platform Adapter Microsoft ISATAP Adapter Microsoft KM-TEST Loopback Adapte	r er
Marvell Semiconductor. Inc. Mellanox Technologies Ltd. Microsoft Oracle Corporation	Microsoft IP-HTTPS Platform Adapter Microsoft ISATAP Adapter Microsoft KM-TEST Loopback Adapte Microsoft Teredo Tunneling Adapter	r er
Marvell Semiconductor. Inc. Mellanox Technologies Ltd. Microsoft Oracle Corporation	Microsoft IP-HTTPS Platform Adapter Microsoft ISATAP Adapter Microsoft KM-TEST Loopback Adapter Microsoft Teredo Tunneling Adapter Microsoft Teredo Tunneling Adapter	

Jendela pengaturan

Setelah proses instalasi berhasil lalu klik Next.

Add Hardware						
The wizard is	ready to install y	our hardware				
Hardware	to install:					
	Microsoft KM-T	EST Loopback Ad	lapter			
To start in	nstalling your new H	hardware, click Ne	ext.			
				< Back	Next >	Cancel

Jendela instalasi KM-TEST Loopback Adapter



Proses instalasi software

Setelah seluruh proses selesai klik *Finish*.



Jendela pemberitahuan bahwa instalasi sudah berhasil

Adapter loopback dapat dilihat di Network Insterface, secara default adapter loopback yang dibuat umumnya muncul dengan nama Ethernet dan ada keterangan Microsoft KM-TEST Loopback Adapter.



Icon Adapter Loopback

L9.2. INSTALASI MIKROTIK DENGAN QEMU GNS3

Anda dapat menjalankan MikroTik OS di dalam GNS3 menggunakan fasilitas Qemu yang ada pada GNS3.

Qemu adalah aplikasi yang digunakan untuk menjalankan emulasi suatu sistem operasi

Untuk membuat emulasi MikroTik OS pada GNS3 pertama persiapan terlebih dahulu file Image MikroTik, file image dapat di download di situs mikrotik dengan ekstensi CHR.



File Image CHR Mikrotik OS

Setelah itu buka aplikasi GNS3 lalu klik *Edit* dan klik *Preferences*.



Menu Preference

Setelah itu klik **QEMU** lalu klik **New**.

Preferences				?	×
General	QEMU VM template	s			
Server					
Packet capture					
VPCS					
~ Dynamips					
IOS routers					
VIOS on UNIX					
IOU devices					
~ VirtualBox					
VirtualBox VMs					
~ QEMU					
QEMU VMs					
	<				>
		New	Edu	Delete	=
		INEW	cuit	Delete	
			OV Creat		
			UK Cancel	Арр	y

Jendela pengaturan Qemu

Klik Next.

🛞 New	QEMU VM template		?	×
QEMU Pl	I VM type ease choose a type of QEMU VM to help with pre-configur	ation.		
Type:	Default			•
	< Back	Next >	Cano	el

Jendela pengaturan Qemu

Beri nama **QEMU** yang akan dibuat pada bagian **Name** lalu klik **Next**.

🛞 New QEMU VM template			?	×
QEMU VM name Please choose a descriptive name for your r	new QEMU virtual	machine.		
Name: ROUTER_MIKROTIK				
	< Back	Next >	Cano	el

Jendela pengaturan Qemu

Tentukan kapasitas RAM yang digunakan pada bagian RAM lalu klik *Next*.

New OEMU	VM template	?	×
QEMU binary Please ch enough m	and memory kck the Qemu binary is correctly set and the virtual machine has emory to work.		
Qemu binary:	C:\Program Files\GNS3\qemu-2.4.0\qemu-system-x86_64w.exe (v2.4.0)	•
RAM:	256 MB		\$
	< Back Next >	Car	cel
	COUCK INC.		

Jendela pengaturan Qemu

Pilih file image yang sudah dipersiapkan sebelumnya lalu klik **Open**.

- → ✓ ↑ ↓ > This PC > Downloads	Search Downloads
Organize 🔻 New folder	E 🔻 🚺
CneDrive	
Desktop	
	A 10 KT (0.00)

Jendela pengaturan Qemu

Klik **Yes**.

💰 New QEMU VM template	? ×
Disk image Please choose a base disk image for your virtual machine.	
Disk image (hda):	Browse
😢 QEMU disk image	×
Would you like to copy chr-6.37.3.img to the default images di	rectory
Yes	0
< Back Finish	Cancel

Jendela pengaturan Qemu

Klik Finish.



Jendela pengaturan Qemu

Seneral	QEMU VM templa	ites	
ierver Zacket capture (PCS Dynamips IDS routers OS on UNIX IDU devices /irtualBox VMS EMU QEMU VMs	ROUTER_MIK	 General WM name: Server: Memory: GEMD binary: Mokimage (hda): Network: Adapters: Type: Optimizations CPU throtting: Process priority: V Additional options 	ROUTER_MKROTIK local 25 MB qemo-system:s8,54w.exe C:\Users\412WAF.GNS3\image1\QEM 1 e1000 diabled normal -nographic
		New	Edit Delete

Jendela pengaturan Qemu

Anda dapat merubah Icon default agar menjadi icon router yang telah dibuat dengan cara klik icon lalu klik *Change Symbol*

NGELAB MIKROTIK



Jendela pengaturan Qemu

Setelah itu klik icon yang di inginkan lalu klik OK.



Memilih Icon untuk Qemu





Jendela pengaturan Qemu

Jika seseorang meninggal dunia, maka terputuslah amalannya kecuali tiga perkara (yaitu): sedekah jariyah, ilmu yang dimanfaatkan, atau do'a anak yang sholeh"

-: HR. Muslim :-

DAFTAR PUSTAKA

Mikrotik. 2016. *MikroTik Certified Network Associate Training Outline*. https://www.mikrotik.com/download/pdf/MTCNA_Outline.pdf

Mikrotik. 2015. *Mikrotik Certified Routing Engineer Training Outline*. https://www.mikrotik.com/download/pdf/MTCRE_Outline.pdf

Purbo, Onno W. 2017. *Model Protocol TCP/IP di Internet*. bit.ly/2nxpPer