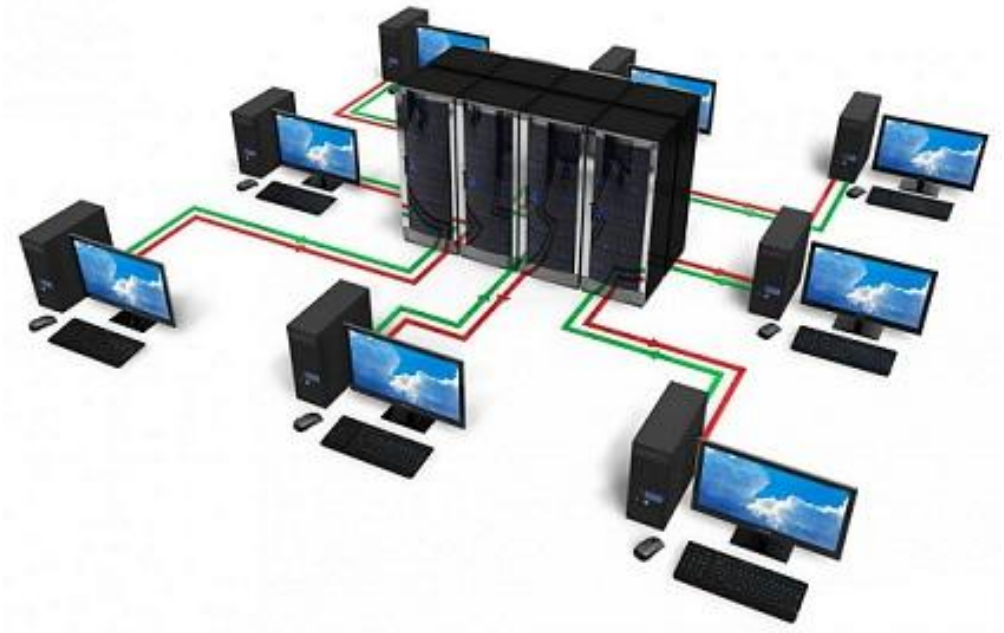
Materi Jaringan Komputer



※ Network Fundamentals ※

※ Membangun Jaringan LAN ※

※ MikroTik ※

DAFTAR ISI

BAB 1 - NETWORK FUNDAMENTALS

A. Apa itu Jaringan Komputer?

Jaringan Komputer atau Network adalah kumpulan perangkat komputer yang saling terhubung melalui perantara media transmisi untuk dapat berbagi data dan sumber daya.

Komponen jaringan komputer.

- End Device: PC, Laptop, Smartphone, dll.
- Network Device: Hub, Switch, Router, Access Point, Multi Layer Switch (Switch L3), Access Point, dll.
- Interconnection: Konektor (NIC, SFP); Media Transmisi (Copper, Fiber Optic, Wireless); dll.

Server adalah penyedia layanan dalam suatu jaringan, layanan ini bisa berupa file server, web, mail server, dsb.
Client adalah penerima atau pengguna dari layanan yang diberkan oleh server.

Catatan : Server dan Client adalah sebutan untuk mebedakan mana pemberi layanan dan mana penerima layanan. Baik server maupun client, dua-duanya bisa berupa end devices (PC, smartphone) ataupun server dalam bentuk network devices (router).

B. Komunikasi Digital

Komputer hakekatnya hanya bisa membaca bahasa mesin yaitu binary (angka binner). Bilangan binner merupakan bilangan berbasis 2, hanya terdiri dari angka 0 dan 1. Ya, data digital itu berupa angka 0 dan 1. Adapun tampilan teks, gambar, warna yang kita lihat di komputer itu sudah dikonversi sedemikian rupa, sehingga bisa dibaca oleh manusia (pengguna).

1. Satuan Data Digital

Satuan data digital adalah bit. 1 bit (*b*) terdiri dari satu angka (0 atau 1). 1 bit sama dengan 8 byte. Perlu diingat bit dan byte itu berbeda, bit disingkat dengan “b” sedangkan byte disingkat dengan huruf “B”. Selain itu, 1 bit sama dengan 8 byte.

Sedikit informasi, bahwa ada perdebatan tentang penulisan satuan data digital. Ada yang menyebut 1 Kilobit (Kb) = 1024 bit dengan argumen Kb adalah satuan data digital yang mana data digital menggunakan bilangan basis 2 atau kelipatan 2 (2, 4, 8, 16, 32, 64, 128, 256, ...). Jadi yang kelipatan dua adalah 1024 bukan 1000.

Ada juga yang menyebut 1Kb = 1000 bit dengan alasan K adalah satuan internasional untuk ribuan bilangan desimal selayaknya Kg, KM, dsb.

Ada pendapat lain bahwa penulisan satuan data digital (binary) yang benar adalah menambahkan kata binary. Seperti ini contohnya, Kilo binary bit (Kib) = 1024 bit. Dan ini pendapat yang saya ikuti. Untuk lebih detail tentang perbandingan satuan data digital, silakan simak list berikut.

1 Kibi bit (Kib) = 1024 bit
1 Mebi bit (Mib) = 1024 Kib
1 Gibi bit (Gib) = 1024 Mib
1 Byte (B) = 8 bit (b)
1 Kibi byte (KiB) = 1024 B
1 Mebi byte (MiB) = 1024 KiB = 1048576 B
1 Gibi byte (GiB) = 1024 MiB = 1073741824 B
1 Tebi byte (TiB) = 1024 GiB

2. Sistem Komunikasi Digital

- Simplex : transmisi satu arah, artinya penerima tidak dapat memberikan balasan terkait informasi yang dia terima. Contohnya radio, televisi.
- Half Duplex : transmisi dua arah tapi bergantian. Maksudnya penerima dapat mengirimkan balasan kepada pengirim tetapi setelah pengirim selesai mengirimkan data. Contohnya Handly Talkie (HT).
- Full Duplex : transmisi dua arah interaktif. Maksudnya baik pengirim maupun penerima dapat saling komuniakasi bersamaan. Contohnya telepon.

3. Konversi Binner ke Desimal

Di materi jaringan dasar kita harus bisa mengkonversi bilangan binner ke desimal, khususnya untuk mendukung materi *subnetting*. Karena yang kita gunakan adalah IPv4 yang berukuran 8 bit per oktet, bilangan desimal yang harus kita konversi adalah 0-256 atau jika dalam binner adalah 0-11111111. Kita bisa menggunkan tabel berikut untuk membantu mempercepat proses menghitung.

1	1	1	1	1	1	1	1
128	64	32	16	8	4	2	1

Bilangan binner berukuran 8 bit artinya ada 8 angka binner (0 atau 1). Bilangan binner di setiap posisi (urutanya) mempunyai value masing-masing yang mana dari kanan ke kiri valuenya adalah hasil $\mathbf{2^{n-1}}$ dengan $\boldsymbol{n}$ merupakan urutan posisinya (di hitung dari kanan). Value ini ada jika posisi tersebut diisi angka 1, jika angka 0 maka valuenya 0. Misal berdasarkan tabel di atas jika posisi 1 adalah angka 1 maka valuenya adalah $2^{1-1} = 1$, kemudian posisi 2 adalah angka 1 juga maka valuenya $2^{2-1} = 2$, demikian seterusnya sampai bit ke-8. Nah keseluruhan value tersebut dijumlahkan dan hasilnya adalah bilangan desimal. Contoh kasusnya seperti ini.

$00101011_{(2)} =$ ..... $_{(10)}$

Kita masukan angka binner tersebut ke tabel di atas. Jika suatu posisi bit diisi angka 1 maka value dalam bingan desimalnya diisi sesuai rumus di atas. Jika diisi angka 0 maka valuenya adalah 0.

0	0	1	0	1	0	1	1
0	0	32	0	8	0	2	1

Kemudian kita jumlahkan semua value desimalnya
32 + 8 + 2 + 1 = 43.
Jadi $\mathbf{00101011_{(2)} = 43_{(10)}}$

LATIHAN SOAL
Konversi bilangan binner berikut menjadi bilangan desimal!
1. $11001100_{(2)}$
2. $00100111_{(2)}$
3. $10101010_{(2)}$
4. $11101101_{(2)}$
5. $01100011_{(2)}$

4. Konversi Desimal ke Binner

Sama halnya dengan binner ke desimal, untuk mengkonversi bilangan desimal ke binner kita bisa menggunakan tabel seperti sebelumnya. Karena sudah dibahas, kita bisa langsung masuk ke contoh cara menghitungnya.

$92_{(10)}$ = ... (2)

Cara menghitungnya yaitu dengan mengurangi angka yang kita hitung dengan angka desimal pada tabel berikut (yang atas), mulai dari yang paling kiri. Jika hasilnya >= 0 maka kita tulis di pada kolom binner dibawahnya dengan angka 1, kemudian hasil pengurangan tersebut dikurangi lagi dengan angka desimal sesudahnya. Tetapi jika < 0 kita isi kolom binnernya dengan angka 0 dan kita tetap gunakan angka tersebut (bukan hasil pengurangan) untuk dikurangi dengan angka yang lebih kecil.

128	64	32	16	8	4	2	1
0	1	0	1	1	1	0	0

92 - 128 = -36
92 - 64 = 28
28 - 32 = -2
28 - 16 = 12
12 - 8 = 4
4 - 4 = 0
Karena sudah 0, maka kolom berikutnya kita isi 0.

Kemudian angka pada kolom binner kita gabungkan jadi 01011100, dalam penulisan angka binner angka 0 di sebelah kiri boleh dihilangkan (tidak ditulis) seperti 1011100.

Jadi, **$92_{(10)} = 01011100_{(2)} = 1011100_{(2)}$**

LATIHAN SOAL
Konversi bilangan desimal berikut menjadi bilangan binner!
1. $10_{(10)}$
2. $226_{(10)}$
3. $99_{(10)}$
4. $161_{(10)}$
5. $244_{(10)}$

C. IP Address dan MAC Address

1. IP Address

Salah satu unsur terpenting yang memungkinkan perangkat dalam suatu jaringan bisa saling terhubung adalah IP Adddress (IP kependekan dari Internet Protocol). Penjelasan sederhananya, IP Address adalah deretan angka binner digunakan sebagai alamat suatu perangkat (device). Jika dalam kehidupan nyata IP bisa diibaratkan sebagai alamat rumah yang dibutuhkan saat mengirim surat atau barang.

Saat ini ada dua jenis IP Address, yakni IP Address versi 4 (IPv4) dan IP Address versi 6 (IPv6). Jika teman-teman pernah lihat angka-angka ini:

- 8.8.8.8
- 192.168.1.1
- 127.0.0.1

Itu adalah Internet Protocol version 4. Panjang IPv4 yaitu 32-bit yang dibagi menjadi 4 oktet (setiap oktet berukuran 8-bit) dan jumlah total IPv4 yang tersedia adalah 256 x 256 x 256 x 256 = 4.294.967.296. Agar mudah dimengerti manusia, penulisan IPv4 biasanya dikonversi ke dalam bentuk bilangan desimal (0-9) seperti contoh di atas.

Yang kedua yaitu IPv6 (Internet Protocol version 6). IPv6 diciptakan karena penggunaan IPv4 sudah mendekati jumlah maksimum. Meskipun jumlah IP yang tersedia pada IPv4 mencapai 4 milyar, tetapi pada implementasinya tidak semua IP bisa dipakai. Nah IPv6 ini hadir untuk menggantikan IPv4. Saat ini, IPv6 belum menjadi kewajiban artinya baru digunakan oleh beberapa provider atau perusahaan saja. Contoh IPv6 adalah sebagai berikut:

- ff02::2
- 21da:d3:0:2f3b:2aa:ff:fe28:9c5a
- fe80::2aa:ff:fe9a:4ca2

Panjang IPv6 yaitu 128-bit yang dibagi menjadi 8 oktet (setiap oktet berukuran 16-bit). Penulisan IPv6 menggunakan bilangan heksadesimal (0-F). Sementara itu, total IP yang tersedia adalah 2^{128} atau $3{,}4 \times 10^{38,}$

2. MAC Address

MAC Address adalah sebuah alamat berukuran 48-bit yang dimiliki suatu network interface, baik itu LAN Adapter (NIC), SFP, Wireless Adapter, dsb. MAC Address bersifat unik maksudnya mac address suatu network interface berbeda dengan network interface lain. Meskipun pada dasarnya mac address sama seperti IP yaitu angka binner. Akan tetapi untuk mempermudah pengguna maka penulisannya menggunakan hexadesimal.
Contoh: 70:5E:FD:6B:1E:23

- 24 bit pertama (70:5E:FD) menunjukan identitas vendor perangkat tersebut.
- 24-bit terakhir (6B:1E:23) menunjukan nomor perangkat itu sendiri.

Lalu, komputer berkomunikasi menggunakan MAC Address atau IP Address sih?

Pada dasarnya saat host to host, komputer berkomunikasi menggunakan mac address. Namun komputer tidak menetap di satu tempat saja, jika menggunakan mac address kita akan kesulitan dalam mobilitas. Maka digunakan IP address untuk menghubungkan komputer-komputer.

Bisa juga dianalogikan mac address itu seperti biometrik seseorang (misal: sidik jari, iris mata, dsb). Sedangkan IP adalah nama atau panggilan seseorang. Untuk memudahkan komunikasi kita akan memanggil nama, dan nama itu merujuk ke seseorang dengan biometrik yang sifatnya unik (tidak sama dengan yang lain).

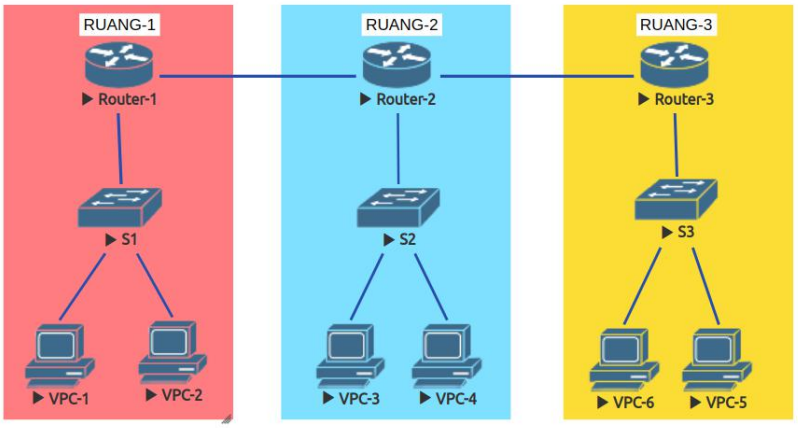
D. Jaringan Berdasarkan Area

- Local Area Network (LAN) adalah jaringan sederhana dalam sebuah gedung, kantor, rumah, atau sekolah.
- Metropolitan Area Network (MAN) adalah gabungan dari beberapa LAN dalam satu wilayah/kota.
- Wide Area Network (WAN) adalah gabungan dari beberapa MAN atau gabungan semua jaringan antar pulau, negara atau benua.

E. Perangkat Jaringan (Network Devices)

1. Router

Router adalah perangkat untuk menghubungkan jaringan yang berbeda. Router bertugas untuk mengarahkan paket yang menuju jaringan lain, memilih rute mana yang akan ditempuh dalam mengirimkan data.



2. Switch

Switch adalah perangkat yang bekerja pada Layer 2 OSI yaitu Data-Link Layer. Tugasnya menyimpan mac address komputer yang terhubung di setiap portnya. “Menyebarkan” kabel dari

router agar bisa terhubung ke banyak end devices. Ada dua tipe switch, yaitu manageable dan unmanageable.

Manageable switch artinya switch yang bisa dikonfigurasi sedangkan unmanageable switch tidak bisa dikonfigurasi.

3. Switch Layer 3

Sama seperti switch biasa akan tetapi Switch Layer 3 atau Multilayer switch ini memiliki fitur-fitur selayaknya router.

4. Hub

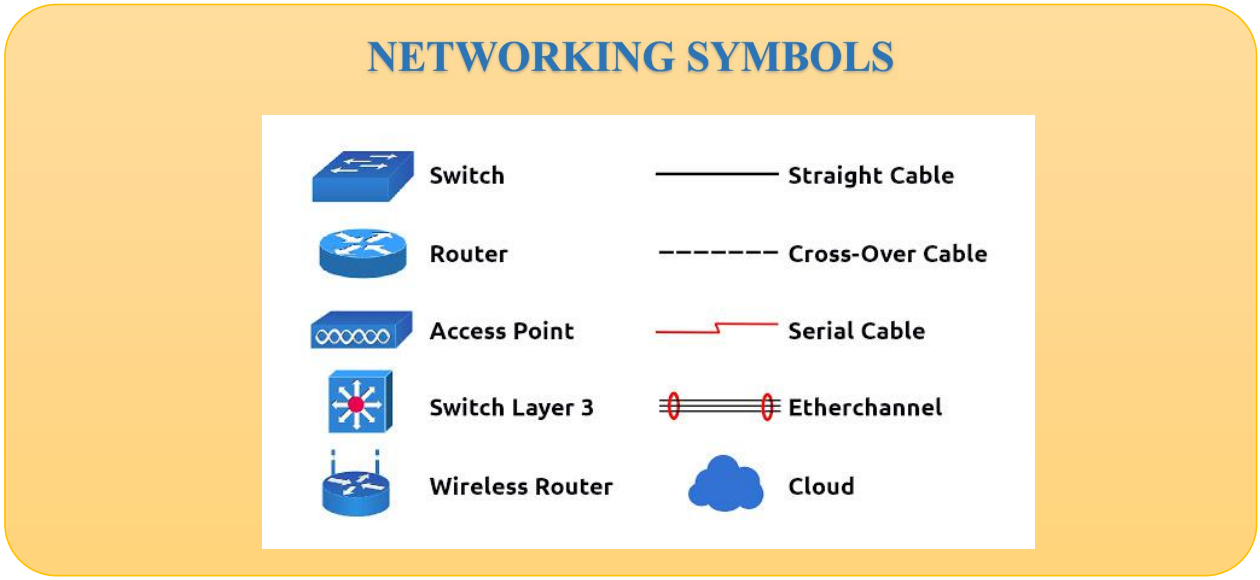
Hub berfungsi untuk meneruskan data ke semua port sehingga mungkin terjadi Collision (tabarakan jika ada lebih dari satu host yang mengirim data bersamaan).

Broadcast Domain, kondisi ketika penerima (tujuan) tidak ditemukan atau berada di luar jaringan pengirim. Paket tersebut akan terus dibroadcast ke semua host (komputer) yang ada di jaringan tersebut, hal tersebut bisa mengakibatkan jaringan menjadi lambat. Broadcast domain ini bisa diatasi dengan Router.

Collision Domain, yaitu tabrakan paket yang diakibatkan beberapa komputer saling mengirim data pada waktu yang bersamaan. Misalnya ada 3 komputer yang terhubung dengan 1 switch. PC 1 dan PC2 sama-sama ingin mengirim data ke PC-3 maka tidak akan terjadi tabrakan data karena switch meneruskan data ke port tujuan saja (tidak ke semua port). Lain halnya jika menggunakan Hub, maka akan terjadi Collision karena Hub tidak menyimpan mac address dan bekerja dengan cara mengirim data ke semua port.

5. Access Point

Access Point adalah perangkat untuk memancarkan gelombang elektromagnetik sehingga terbentuklah jaringan tanpa kabel (wireless). Dari alat inilah ada yang namanya wifi (wireless fidelity).



F. Media Transmisi

Media transmisi adalah perantara yang digunakan untuk membawa data digital dari satu perangkat ke perangkat lain. Media transmisi yang umum digunakan saat ini yaitu: Copper (tembaga), Fiber Optic, dan Wireless.

1. Copper

Copper adalah media transmisi yang menggunakan kawat tembaga sebagai media penghantarnya. Ada beberapa jenis kabel tembaga yang digunakan untuk mentransmisikan data digital saat ini.

a. Twisted Pair (Ethernet Cable)

Kabel twisted pair terdiri dari 8 inti kabel yang dipilin berpasangan (twisted), jadi total ada 4 pasang (pair). Tujuannya untuk meminimalisir gangguan elektromagnetik. Ada dua jenis kabel twisted pair yaitu Unshielded Twisted-Pair (UTP) dan Shielded Twisted-Pair (STP). UTP adalah yang paling banyak digunakan dalam membuat jaringan LAN, karena harganya yang lebih murah daripada STP.

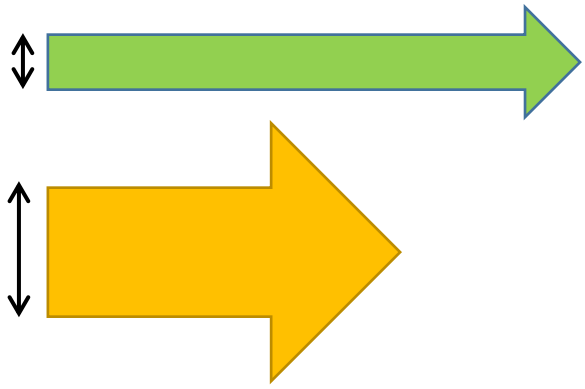
Perbedaan kedua jenis kabel ini, yang pertama adalah shielded (pelindung). Kabel STP memiliki alumunium foil sebagai pelindung tambahan dari gelombang elktromagnetik sedangkan UTP tidak mempunyai. Kabel UTP konektornya menggunakan RJ-45 yang biasa kita temukan dijadikan

sebagai medi transmisi jaringan LAN, untuk menghubungkan komputer ke komputer atau perangkat jaringan seperti router. Sedangkan STP menggunakan koenktor RJ-11 biasanya digunakan dalam jaringan telepon rumah. Panjang maksimum kabel twisted pair hanya mencapai 100m saja.

	10 Base-T (IEEE 802.3i)	100 Base-TX (IEEE 802.3u)	1000 Base-T (IEEE 802.3ab)
Media	EIA/TIA Cat. 3, 5 UTP 2 Pair	EIA/TIA Cat. 5 UTP 2 Pair	EIA/TIA Cat. 5e, 6 UTP 4 Pair
Max Segment Length	100 meter (328 ft)	100 meter (328 ft)	100 meter (328 ft)
Connector	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)
Max Speed	10Mbps	100Mbps	1Gbps

IEEE (Institute of Electrical and Electronics Engineers) adalah organisasi internasional yang mengembangkan standarisasi teknologi, mulai dari teknologi telekomunikasi, komputer, elektronika, kelistrikan, hinga antariksa.

Apa bedanya Cat 3, Cat 5, Cat 5e, Cat 6?
Yang membedakan setiap cat (category) dalam kabel Twisted pair yaitu lebar bandiwthnya.
Category 3 (cat 3) lebar bandwidthnya 16Mhz, banwidthnya mencapai 10Mbps.
Category 5 (cat 5) lebar bandwidthnya 100Mhz, bandidthnya mencapai 100Mbps.
Sedangkan category 6 (cat 6) memiliki lebar bandwidth 250Mhz dan badnwidth 1Gbps.



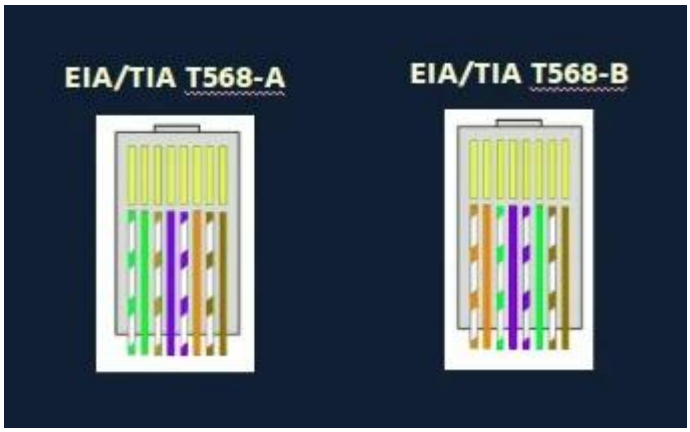
Lebar bandwidth adalah frekuensi data tersebut (bisa diibaratkan lebar diameter pipa air). Sedangkan **bandwidth** merupakan berapa besar data yang bisa dilewatkan dalam satuan detik (bisa diibaratkan sebagai berapa banyak air yang bisa melewati pipa tersebut).

Pengkabelan Kabel UTP

Ada dua jenis pengkabelan kabel UTP yaitu straight through dan crossover. Sebelum kita mempelajari perbedaannya, kita perlu tahu standar pengkabelan kabel UTP pada gambar berikut.

EIA/TIA T568A

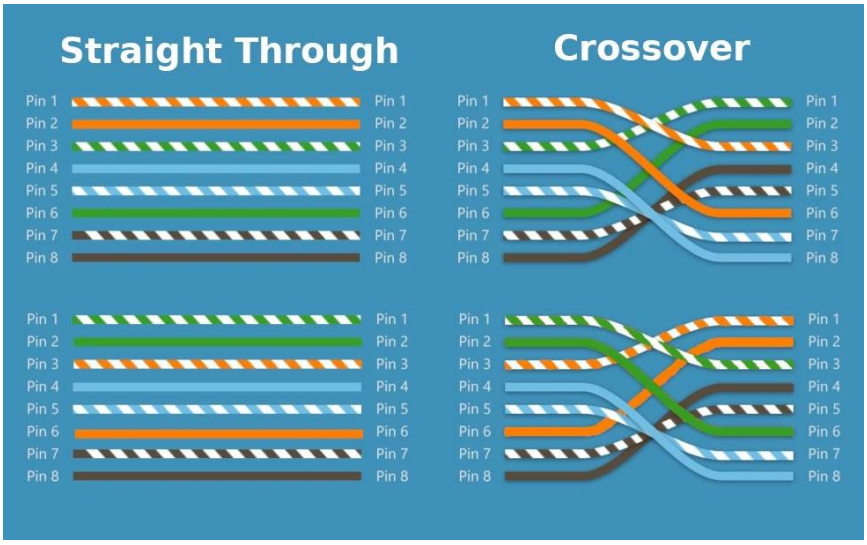
1. Putih Hijau
2. Hijau
3. Putih Orange
4. Biru
5. Putih Biru
6. Orange
7. Putih Coklat
8. Coklat



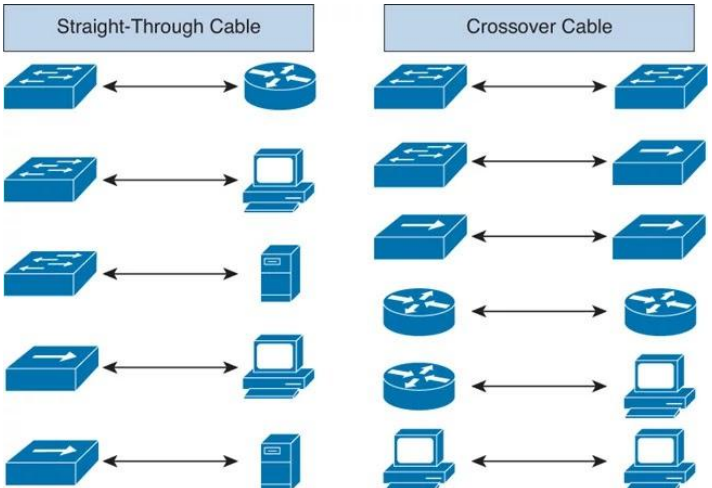
EIA/TIA T568A

1. Putih Orange
2. Orange
3. Putih Hijau
4. Biru
5. Putih Biru
6. Hijau
7. Putih Coklat
8. Coklat

Pengkabelan straight throught adalah pengkabelan yang kedua ujungnya menggunakan standar yang sama (T568A dengan T568A atau T568B dengan T568B). Sedangkan crossover, kedua ujungnya menggunakan standar yang berbeda (salah satu menggunakan T568A, ujung satunya lagi menggunakan T568B).



Kapan kita menggunakan Pengkabelan jenis Straight Through dan Crossover?



Saya pernah nyoba menghubungkan Router ke Router menggunakan Straight tetap terhubung?
Karena perangkat terbaru saat ini biasanya sudah mendukung Auto MDI/MDI-X. Perangkat yang sudah support Auto MDI/MDI-X bisa dihubungkan dengan kabel straight through maupun kabel crossover. Perangkat akan mendeteksi apakah koneksi membutuhkan crossover, dan secara otomatis akan menggunakan konfigurasi MDI atau MDIX untuk menyamakan koneksi perangkat lawan.

b. Kabel Serial

Kabel serial adalah salah satu jenis kabel tambaga yang digunakan khususnya dalam jaringan MAN dan WAN. Karena kabel serial lebih tahan gangguan (interference) dan jarak jangkauannya lebih jauh hingga puluhan kilometer. Akan tetapi bandwidthnya lebih rendah dibanding kabel UTP.

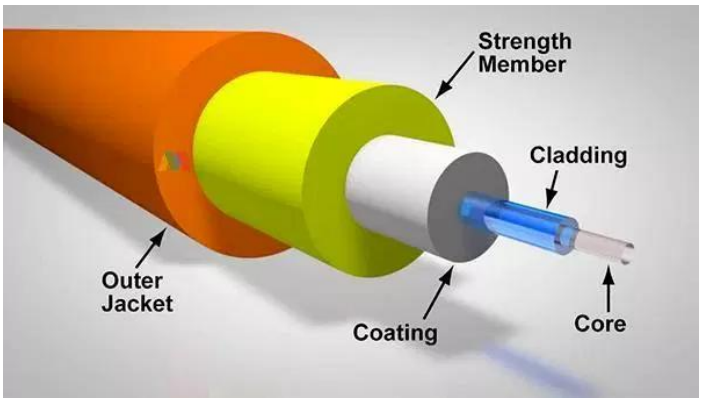
Konektor kabel serial sangat beragam, dari segi ukuran, bentuk, jumlah pin. Bentuknya hampir mirip seperti kabel VGA.

2. Fiber Optic

Fiber optic adalah kabel yang menggunakan serat optik sebagai media penghantarnya. Teknologi serat optik ini mampu menghantarkan sinyal digital hingga ratusan kilometer dengan kecepatan tinggi dan ketahanan terhadapa interference baik cuaca maupun gelombang elektromagnetik. Akan tetapi karena bahan intinya adalah serat optik atau serat kaca, maka fiber optic ini apabila tertekuk bisa berpotensi patah pada inti kabel. Jika patah maka untuk menyambungnya (splicing) memerlukan alat khusus yang harganya cukup mahal.

Fiber optic biasanya digunakan pada jaringan MAN dan WAN untuk menghubungkan jaringan antar kota, pulau, hingga benua. Selain itu fiber optic juga bisa kita temui di jaringan LAN dalam datacenter karena datacenter memerlukan koneksi yang cepat dan stabil.

a. Struktur Kabel Fiber Optic



Core : Bagian inti dari fiber optic yang berfungsi sebagai media transmisi, bagian ini terbuat dari serat kaca atau kaca silikon berdiameter 2 μm - 50 μm.
Cladding : Bagian ini juga terbuat dari kaca silikon akan tetapi indeks biasnya lebih rendah daripada bagian core. Fungsi bagian ini sebagai reflektor gelombang cahaya.

Coating/Buffer : Bagian ini terbuuat dari bahan polymer yang berfungsi sebagai pelindung dari gangguan fisik yang mungkin terjadi seperti lengkungan pada kabel, kelembaban udara, dll.

Strength Member dan Outer Jacket : Lapisan terluar fiber optic yang fungsinya juga sebagai pelindung. Biasanya terbuat dari braided ataupun plastik.

b. Single Mode dan Multimode

Fiber optic single mode memiliki diamater core yang sangat kecil (sekitar 5-10 mikron), sehingga membuat gelombang tidak memantul ke dinding-dinding cladding. Untuk mendapatkan performa terbaik pada kabel ini, biasanya ukuran selongsongnya adalah sekitar 15 kali dari ukuran core (sekitar 125 mikron). Kabel untuk jenis ini paling mahal, karena kabel single mode memiliki pelemahan kurang dari 0.35 dB per kilometer, sehingga memungkinkan kecepatan yang sangat tinggi dan jarak yang sangat jauh. Standar untuk kabel ini diantaranya yaitu ITU G.652C, G.653A, dan G.655C.

Fiber optic multi mode memiliki diameter core sekitar 50-62,5 mikron (lebih besar dibanding single mode) yang membuat cahaya di dalamnya akan terpantul-pantul di dinding cladding. Hal ini dapat menyebabkan berkurangnya bandwidth dari fiber optic jenis ini. Ukuran core yang besar memungkinkan fiber optic mendukung berbagai mode elektromagnetik untuk frekuensi dan polarisasi tertentu.

Fiber optic multi mode juga dibagi menjadi beberapa kelas berdasarkan bahan yang digunakan, umumnya ada 4:

- FDDI-grade : multimode fiber dengan bandwidth 160 MHz pada diameter cahaya 850 nm
- OM1 : fiber optic 62,5 mikron dengan bandwidth sedikit lebih banyak

• OM2 adalah fiber optic 50 mikron.
• OM3 adalah fiber optic yang dioptimalkan laser, cocok untuk pemancar berbasis VCSEL.

Daftar Fiber Optic Single Mode

Interface	Panjang Gelombang (nm)	Jangkauan	NDSF	DSF	NZDSF
1000 Base -LX 1000 Base -BX 10G Base -LR 10G Base -LW 10G Base -LX4	1310	10 KM	√	x	x
10G Base-ER	1550	30-40 KM	√	√	√
1000 Base-ZX 1000 Base-ZR	1550	80-100 KM	√	√	√
CWDM	1470-1610	80-120 KM	√	x	√
DWDM	1530-1565	80-100 KM	√	x	√

Interface	Panjang Gelombang (nm)	Dukungan	Jangkauan	MCP Requirement
1000 Base-SX	850	FDDI-Grade	220	x
		OM1	275	x
		OM2	550	x
		OM3	-	
1000 Base-LX	1300	FDDI-Grade	550	√
		OM1	550	√
		OM2	550	√
		OM3	-	
10G Base-SR	850	FDDI-Grade	26	x
		OM1	33	x
		OM2	82	x
		OM3	300	x
10G Base-LX4	1300	FDDI-Grade	300	√
		OM1	300	√
		OM2	300	√

		OM3	-	
10G Base-LRM	1300	FDDI-Grade	220	√
		OM1	220	√
		OM2	220	√
		OM3	220	x

Daftar Fiber Optic Multi Mode
Konektor Fiber Optic

Connector	Insertion Loss	Repeatability	Fiber Type	Applications
 FC	0.5--1.0 dB	0.2 dB	SM, MM	Datacom, telecom
 LC	0.15 db (SM) 0.10 dB (MM)	0.2 dB	SM, MM	High-density interconnection, datacom, telecom
 MT Array	0.3-1.0 dB	0.25 dB	SM, MM	High-density interconnection
 SC	0.2-0.45 dB	0.1 dB	SM, MM	Datacom, telecom
 ST	Type. 0.4 dB (SM) Type. 0.5 dB (MM)	Type. 0.4 dB (SM) Type. 0.2 dB (MM)	SM, MM	Inter-/intra-building, security, U.S. Navy

3. Wireless

Wireless (nirkabel) adalah teknologi yang memungkinkan pengiriman transmisi data digital melalui gelombang elektromagnetik. Jadi tidak menggunakan media fisik berupa kabel. Jarak yang dijangkai bisa pendek hanya beberapa meter seperti bluetooth, wifi (wireless fidelity). Atau jarak menengah hingga puluhan kilometer seperti sinyal operator (GSM). Dan bisa juga jaraknya ribuan kilometer, contohnya satelit.

Saat teknologi wireless cukup populer, karena menawarkan banyak keunggulan dibanding teknologi wired (kabel), mulai dari portabilitas hingga efisiensi biaya. Salah satu pemanfaatan teknologi wireless adalah wireless local area network (WLAN).

IEEE 802.11
IEEE 802.11 adalah serangkaian spesifikasi komunikasi wireless local area network di frekuensi 2.4, 3.6, 5, dan 60 Ghz.

1. Standarisasi IEEE 802.11a
Standard IEEE 802.11a bekerja pada frekuensi 5 GHz mengikuti standard dari UNII (Unlicensed National Information Infrastructure). Teknologi IEEE 802.11a tidak menggunakan teknologi

spread-spectrum melainkan menggunakan standar frequency division multiplexing (FDM). Mampu mentransfer data hingga 54 Mbps.

2. Standarisasi IEEE 802.11b

Standar 802.11b saat ini yang paling banyak digunakan. Menawarkan throughput maksimum dari 11 Mbps dan jangkauan hingga 300 meter di lingkungan terbuka. Ia menggunakan rentang frekuensi 2,4 GHz, dengan 3 saluran radio yang tersedia.

3. Standarisasi IEEE 802.11g

Standar 802.11g menawarkan bandwidth yang tinggi (54 Mbps throughput maksimum) pada rentang frekuensi 2,4 GHz. Standar 802.11g kompatibel dengan standar 802.11b, yang berarti bahwa perangkat yang mendukung standar 802.11g juga dapat bekerja dengan 802.11b.

4. Standarisasi IEEE 802.11n

Standarisasi IEEE 802.11n adalah standar yang bisa bekerja pada frekuensi 2,4Ghz dan 5GHz, jadi perangkat yang menggunakan standar ini bisa terhubung ke WiFi 2,4Ghz ataupun 5GHz. Kecepatan yang ditawarkan mencapai 600Mbps.

5. Standarisasi IEEE 802.11ac

Standar 802.11ac adalah pengembangan dari IEEE 802,11a. Menggunakan frekuensi 5GHz dengan kecepatan bandwidth yang lebih tinggi yaitu mencapai 1,3Gbps.

6. Standarisasi IEEE 802.11ax

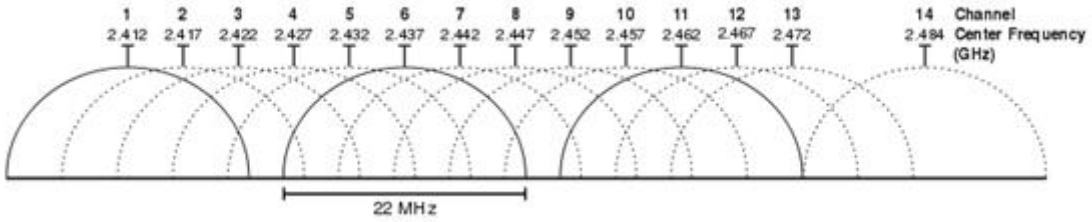
Standarisasi IEEE 802.11ax adalah teknologi yang baru-baru ini dikenalkan, menawarkan kecepatan hingga 11Gbps dan bekerja di 2,4GHz dan 5GHz.

7. Standarisasi IEEE 802.11ad

Standar IEEE 802.11ad adalah teknologi wireless (wifi) dengan frekuensi 60GHz dengan kecepatan 1Gbps.

Channel WiFi

Seperti yang sudah kita ketahuai perangkat wireless bekerja menggunakan frekuensi tertentu untuk mentransmisikan data. Ada yang 2,4 GHz dan ada juga yang5 GHz. Dari angka tersebut masih dibagi-bagi lagi dengan yang namanya channel. Misal 2,4 Ghz (2400MHz) yang digunakan bukan frekuensi 2400MHz pas, tetapi dibagi menjadi 14 channel. Frekuensi terendah WiFi 2,4GHz adalah 2402 MHz hingga yang tertinggi adalah 2502 MHz. Berikut ini adalah pembagian channel WiFi 2,4GHz dengan lebar channel 22MHz.



Ada juga istilah channel width atau istilahnya range frekuensi yang digunakan. Channel width yang umum digunakan saat ini yaitu 5MHz, 10MHz, 20MHz, 22MHz, 40MHz, 80MHz, 160MHz. Sebagai network engineer, saat mensetting perangkat wireless kita memperhatikan channel dan channel width ini. Pembagian channel dilakukan supaya meminimalisir interferensi antar wifi.

Interferensi elektromagnetik merupakan kondisi dimana ada 2 aliran frekuensi yang sama. Hal ini bisa menyebabkan penurunan performa bahkan loss connection. Bisa diibaratkan dengan 2 orang yang mempunyai suara mirip berbicara bersamaan, tentu akan sulit dibedakan.

Perangkat yang menggunakan frekuensi 2,4GHz bukan hanya WiFi saja, ada perangkat lain di sekittar kita yang memakai frekuensi tersebut, misalnya microwave (oven), alarm detector, bluetooth, dll.

Misal ada wifi menggunakan channel 1 berukuran 22MHz (2402-2424 MHz). Nah kita mau pasang wifi juga, maka untuk menghindari interferensi kita perlu memilih channel yang frekuensinya tidak masuk ke channel 1 (antara 2425-2502 MHz). Jadi kita bisa menggunakan channel 6 ke atas. Akan tetapi semakin tinggi frekuensi akan semakin pendek jangkauannya.

Jika kita memaksa ingin pakai channel 1 juga bagaimana? Tentu sah-sah saja tetapi ada kemungkinan mengalami interferensi. Apalagi jika banyak wifi menggunakan channel yang sama. Dan catatan: kebanyakan perangkat bekerja pada channel 1 secara default.

Meskipun ada 14 channel yang direkomendasikan untuk digunakan adalah channel 1, 6, 11. Kenapa? Karena jika ada dua WiFi yang channelnya berbeda tetapi range frekuensinya ada yang sama (nyrempet), contoh channel 1 dan 3, maka kemungkinan interferensinya lebih besar.

Jika ada channel yang sama maka mereka akan transmit data secara bergantian, tetapi bisa juga bersamaan dengan kriteria sesuai teknologi CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance).

CSMA/CA digunakan untuk mementukan apakah suatu channel tersedia atau tidak. Metode yang digunakan untuk mementukan suatu channel bisa digunakan adalah Clear Channel Assessment (CCA):

- Signal Detection (SD), untuk sinyal 802.11 jika ada threshold = 4dB SNR (Signal to Noise Ratio) maka channel dianggap bersih dan bisa digunakan.
- Energy Detection (ED), untuk sinyal selain 802.11, channel dianggap bersih dan bisa digunakan jika ada threshold 24dB.

Threshold adalah ambang batas.
Signal to Noise Ratio (SNR) adalah suatu ukuran untuk menentukan kualitas dari sebuah sinyal yang terganggu oleh derau (interferensi).

Jika channel dianggap tidak bersih, maka access point tidak akan melakukan transmit atau sekedar mengurangi airtime akibatnya mengurangi kapasitas.

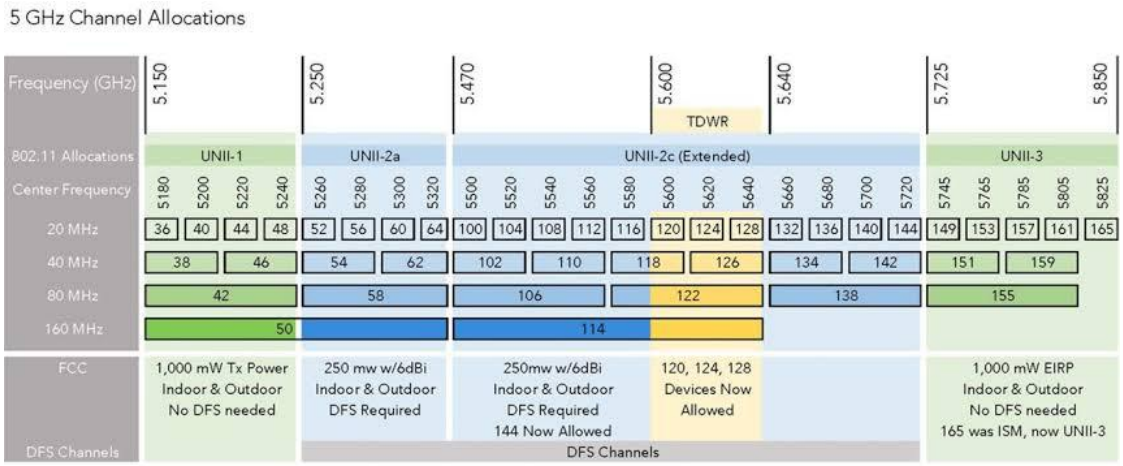
- Co-Channel Interference (CCI)

Terjadi apa AP (Access Point) yang berada dalam jarak dekat (bisa saling menjangkau) yang memancarakan sinyal dengan frekuensi yang sama. Interferensi ini akan diperlakukan seperti Signal Detection.

- Adjacent Channel Interference (ACI)

Disebabkan oleh perangkat 802.11 yang frekuensinya overlapping. ACI akan diperlakukan seperti Energy Detection.

Berikut ini adalah pembagian channel untuk WiFi 5 GHz.



Pembagian channel WiFi 5 mungkin terlihat lebih kompleks karena ditampilkan semua channel widthnya dan memang ada pembagian khusus untuk WiFi 5. Misalnya ada channel yang hanya digunakan diperangkat yang tersedia DFS (Dynamic Frequency Selection) untuk memilih frekuensi secara otomatis.

Di Indonesia, channel yang direkomendasikan untuk WiFi adalah channel 149 sampai dengan channel 165. Karena jika kita menggunakan frekuensi DFS, kita memerlukan perangakat yang support DFS selain itu WiFi bisa mati jika ada sinyal radar yang lewat.

G. Model OSI dan TCP/IP

1. Apa Itu Model OSI dan TCP/IP?

Model OSI dan TCP/IP adalah model atau arsitektur yang dijadikan acuan dasar dalam membuat dan mengembangkan jaringan (networking).

Definisi lain, Model OSI dan TCP/IP adalah suatu pola yang dijadikan standar dalam perangkat networking sehingga satu perangkat dapat compatible (cocok) dengan perangkat yang lain. Masih bingung? Coba perhatikan sejarahnya berikut ini.

Jadi, ceritanya dahulu ketika masa-masa awal perkembangan komputer, ada persaingan dua vendor komputer yaitu International Business Machines Corporation (IBM) dan Digital Equipment Corporation (DEC). Masalahnya saat itu perangkat dari kedua vendor tersebut tidak saling compatible (cocok). Maksudnya begini, jika kita punya PC merk IBM, maka tidak bisa dipasangkan dengan perangkat (misal: monitor, printer) dari vendor DEC, demikian pula sebaliknya. Hal itulah

yang membuat munculnya Model OSI yang dikembangkan oleh International Organization for Standardization (ISO) dan TCP/IP Model yang dikembangkan oleh Department of Defense (DoD).

Sudah ada gambaran? Jadi Model OSI dan Model TCP/IP hakekatnya berbeda tapi tujuannya sama yaitu sebagai sebuah standar yang memungkinkan semua perangkat saling compatible.

Dalam Model OSI terdapat 7 layer:
Physical, Data-link, Network, Transport, Session, Presentation, Application.
Pada Model TCP/IP (versi lama) memiliki 4 Layer:
Link, Internet, Transport, Application.
Sedangkan TCP/IP (versi baru) dibagi menjadi 5 layer:
Physical, Data-link, Network, Transport, Application.

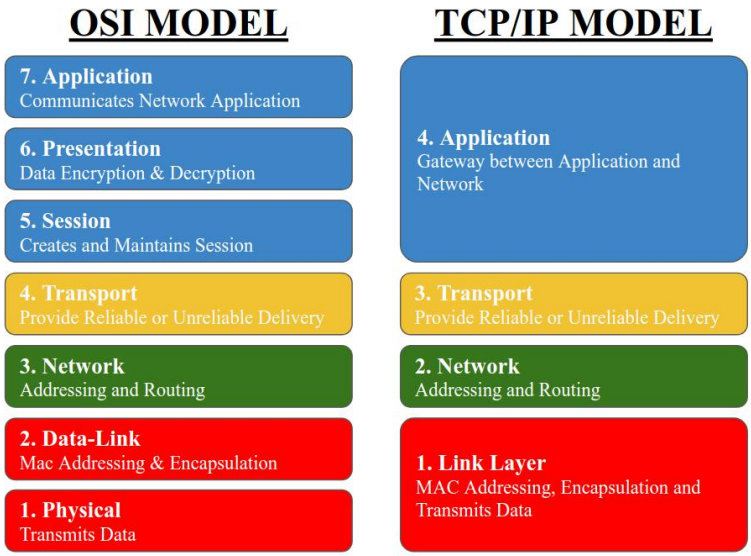
2. Perbedaannya Model OSI dan TCP/IP

Sebenarnya yang dipakai sebagai standar protokol dari dulu sampai saat ini adalah TCP/IP, sedangkan OSI hanya dijadikan sebagai teori untuk dipelajari. Oleh karena itu, kita akan lebih sering menggunakan Model OSI dalam praktiknya nanti. Termasuk dalam sertifikasi Cisco maupun mikrotik.

3. Mengenal dan Memahami Fungsi Setiap Layer

Sebelum melanjutkan ke pembhasan berikutnya, teman-teman perlu ketahui beberapa istilah berikut yang nantinya akan sering dipakai.

- Protokol : adalah suatu aturan yang mengatur proses terjadi suatu hubungan, komunikasi atau perpindahan data pada jaringan komputer. Intinya setiap protokol dibedakan agar datanya diproses sesuai dengan jenisnya, tidak bercampur-baur.
- PDU : Packet Data Unit, yaitu bentuk data yang sedang diproses, bisa berupa segment, packet, frame, ataupun bit,



Coba perhatikan Model OSI dan TCP/IP pada gambar di atas. Kami sengaja memberikan perbedaan warna agar temen-temen bisa memahami fungsi setiap layer dan perbedaan antara OSI dan TCP/IP (versi baru) dengan mudah. Yaps, layernya sama, kecuali pada Application Layer (warna biru). TCP/IP meringkasnya dalam 1 layer sedangkan OSI menjabarkanya menjadi 3 layer.

Prinsipnya, apa yang dilakukan pada layer 5-7 OSI yang warna biru, juga terjadi pada layer 4 TCP/IP. Demikian pula layer lainnya yang secara garis besar tugas dan cara kerjanya sama. Oleh karena itu Kami akan mennggunakan Model OSI untuk menjelaskan fungsi setiap layer OSI dan TCP/IP.

Protocol adalah standar prosedur pengiriman data. Data dikelompokan agar mempermudah transmisi dan encoding/decodingnya.Protocol yang sering digunakan,

- Transmission Control Protocol (TCP).
- User Datagram Protocol (UDP)
- Internet Control Message Protocol (ICMP), ping
- Hypertext Transfer Protocol (HTTP), web
- Post Office Protocol (POP3), email
- File Transfer Protocol (FTP),
- Internet Message Access Protocol (IMAP), email
- dll

Port adalah sebuah aplikasi spesifik atau proses software pada komputer/host yang digunakan untuk komunikasi jaringan. Bisa diibaratkan port adalah ruangan-ruangan dalam sebuah gedung (gedung = komputer). Jumlah total port adalah 65535, dengan klasifikasi penomoran sebagai berikut:

- 0 s.d. 1023 (well-known ports)
- 1024 s.d. 49151 (registered port),
- 49152 s.d. 65535 (unregistered/dynamic, private ephemeral ports)

Service	Protocol/Port
FTP	TCP/21
SSH	TCP/22
Telnet	TCP/23
SMTP	TCP/25
HTTP	TCP/80
POP3	TCP/110

Service	Protocol/Port
HTTPS	TCP/443
Winbox	TCP/8291
DNS	UDP/53
SNMP	UDP/161
NTP	UDP/123

Ururan OSI Layer

7. Application Layer.
Layer ini berfungsi sebagai perantara antara aplikasi (user interface) dan jaringan. Jadi saat aplikasi melakukan request ke jaringan (misal web browser request sebuah halaman web), layer ini lah yang menjadi perantaranya ke protokol terkait (dalam contoh kasus adalah web protocol yaitu HTTP).
Protokol : HTTP, SSH, POP3, SMTP, Telnet. Protokol ini digunakan sampai Session Layer sesuai jenis layanan, misalnya kita requet halaman web protokolnya HTTP/HTTPS, misal mengirim email protokolnya SMTP/POP3/IMAP. Sedangkan *PDU (Protocol Data Unit)-nya berupa Data.*

6. Presentation Layer.
Layer ini bertugas menentukan format dan melakukan enkripsi data. Contohnya saat teman-teman melakukan request halaman web, datanya akan dibentuk dalam format http-request dan dienkripsi misal supaya menjadi https menggunakan SSL/TLS.

5. Session Layer.
Session Layer mendefinisikan bagaimana komunikasi dimulai, dikontrol dan dihentikan. Contohnya begini, temen-teman pasti pernah buka beberapa tab dalam browser (misal satu ngakses google.com, satunya lagi mengakses webiptek.com). Nah session layer ini lah yang bertugas menjaga masing-masing koneksi supaya tetap terhubung dan data yang masuk tidak tertukar meskipun protokolnya sama dan masuknya juga bersamaan.

4. Transport Layer.
Layer ini bertugas untuk menyediakan koneksi reliable (TCP / Transmission Control Protocol) dan unreliable (UDP / User Datagram Protocol). Maksud reliable dan unreliable bukanlah terpercaya dan tidak terpercaya seperti kata google translate. Reliable di sini maksudnya koneksinya membutuhkan acknowledgement sedangkan Unreliable tidak memerlukan acknowledgement.

Apa itu acknowledgement? Sederhananya, acknowledgement adalah indikasi yang melaporkan data diterima dengan utuh, untuk lebih detailnya silakan baca Perbedaan TCP dan UDP. Di layer 4 ini juga terjadi yang namanya error-recovery, jadi semisal teman-teman request web dan datanya ada yang tertinggal, layer ini yang melakukan request lagi sampai datanya utuh kemudian diteruskan ke session layer. Di situlah gunanya acknowledgement, dia akan melakukan request lagi sampai datanya diterima dengan sempurna.

Perbedaan mendasar lainnya yaitu koneksi unreliable lebih cepat dibanding reliable karena si acknowledgement tadi. Contoh koneksi reliable: upload dan download file, contoh koneksi unreliable : DNS dan streaming.
Protokol : TCP dan UDP. Data Unit : Segment.

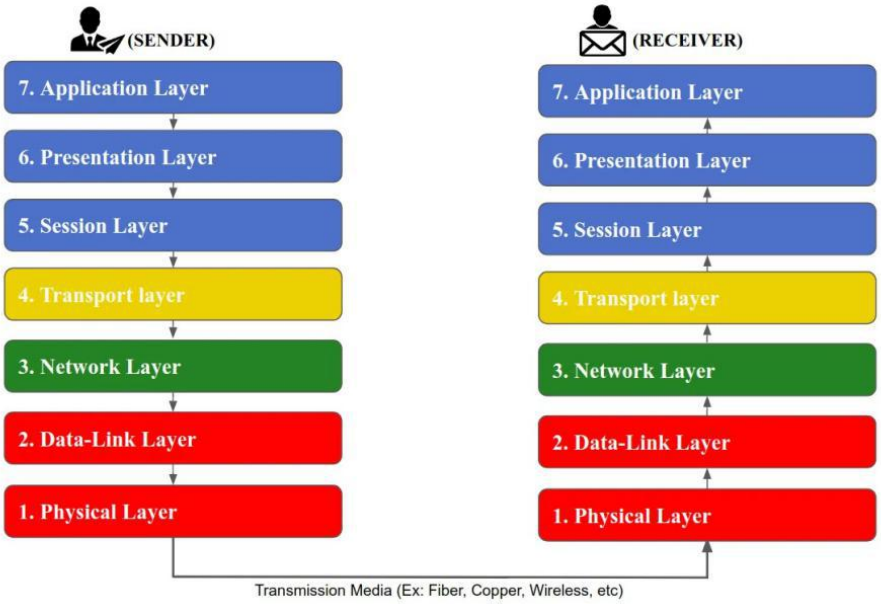
3. Network Layer.
Tugas layer ini yaitu melakukan pengalamatan dan melakukan routing. Bisa dianalogikan bahwa layer ini menentukan kemana data yang dibawa akan dikirim dengan proses yang namanya routing. Ada banyak routing protocol seperti RIP, OSPF, EIGRP, dll, yang masing-masing punya cara tersendiri dalam menentukan jalur mana yang akan dilewati. Contoh perangkat di layer 3 adalah router.
Protokol : IP. Data Unit : Packet.

2. Data-link Layer.
Data-link bertugas menentukan aturan ketika perangkat mengirim data melalui media, aturan tersebut biasanya berupa enkapsulasi. Kita akan belajar lebih jauh tentang enkapsulasi pada materi WAN. Perangkat Layer 2 adalah perangkat yang menghubungkan perangkat dengan media transmisi, conotohnya: switch, bridge, NIC.

Protokol : HDLC, PPP, Frame Relay. Data Unit : Frame.

1. Physical Layer.
Tugasnya mengconversi frame menjadi bits menentukan karakteristik fisik media transmisi. Di sini data ditransmisikan dalam bentuk bit.
Protokol : Ethernet, RJ-45, Fiber. Data Unit : Bit.

4. Cara Kerja Model OSI



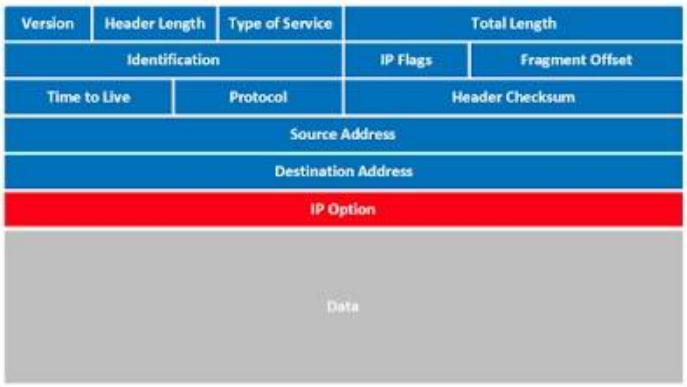
Untuk lebih tahu tentang bagaimana networking model ini bekerja silakan perhatikan gambar di atas. Dalam kasus ini kita akan mencontohkan proses pengiriman data berupa file melalui FTP.

1. Proses pengiriman file dimulai dari aplikasi FTP, bisa berupa filezilla, dsb. Kemudian seperti yang sudah dijelaskan sebelumnya, layer pertama yang dilalui adalah Application Layer yang tugasnya menghubungkan aplikasi filezilla ke protocol jaringan yaitu FTP.
2. Kemudian masuk ke layer berikutnya, Presentation. Di layer ini dibuatlah data sesuai format file dan dilakukan enkripsi (misalnya FTPS).
3. Selanjutnya Session Layer membuat sebuah session untuk memulai koneksi dan menjaganya sampai proses selesai.

Karena ini adalah koneksi FTP maka dipilihlah jalur koneksi reliable pada Transport Layer. Pada layer ini data yang dikirim sudah dalam bentuk segments dan diberi tambahan Transport Header. Isi terpenting dalam header ini adalah informasi protokol yang digunakan (dalam kasus ini adalah TCP port 990).

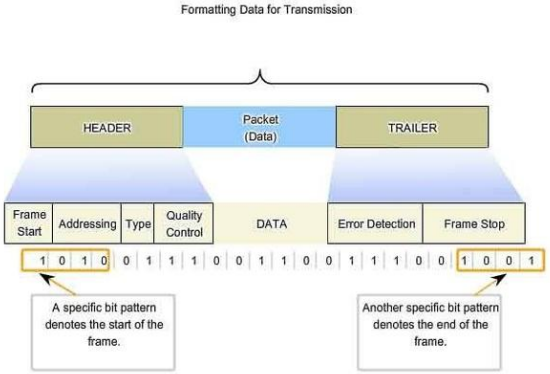
32	Sequence number										
64	Acknowledgment number (if ACK set)										
96	Data offset	Reserved	CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Window Size
128	Checksum										Urgent pointer (if URG set)
160 ...	Options (if Data Offset > 5) ...										padding

4. Selanjutnya data menuju Network Layer kemudian diberi tambahan Network Header kemudian dilakukan proses Routing. Network header berisi diantaranya sebagai berikut:



• Version : Version merupakan penanda IP versi berapa
• Internet Header Lenght : Menampilkan seberapa besar ukuran IP Header Packet. Panjang/ukurannya minimal 20 bytes, dan maksimal 60 bytes.
• Type-of-Service : header berukuran 8 bit yang digunakan sebagai mekanisme Quality-of-Service (QoS) untuk menentukan prioritas setiap paket.
• Total Length : informasi panjang dari seluruh paket, jika Header Length mengidentifikasi besar ukuran IP Header Packet, jika Total Length akan mengidentifikasi besar ukuran seluruh paket termasuk data yang dikirim.
• Identifications, Flags, Fragment Offset : Ketiganya membahas tentang fragmentasi, Fragmentasi sendiri adalah saat IP Packet harus di pecah menjadi packet yang lebih kecil dengan tujuan agar dapat sukses terkirim melewati sebuah jaringan. Bagian ini juga memiliki kemampuan untuk merakit kembali paket yang telah dipecah belah menjadi utuh kembali.
• Time-to-Live(TTL) : angka berukuran 8 bit yang menunjukkan 'sisa hidup' sebuah paket. Nilai ini akan selalu dikurangi 1 satuan setiap kali paket melewati sebuah router (hop). Ketika nilai TTL mencapai angka = 0, maka paket akan di drop oleh router.
• Protocol, Menunjukkan tipe protokol apa yang ada pada segmen yang akan dienkapsulasi.
• Header Checksum : Memiliki panjang 16 bit yang digunakan untuk menyimpan checksum dari header.
• Source Address : Informasi IP address pengirim.
• Destination Address : Informasi IP address tujuan.
• IP Option : Parameter ini jarang digunakan. Parameter ini menyimpan sebuah nilai untuk opsi tertentu misalnya security, record route, time stamp, dll.

5. Setelah itu packets dari network layer masuk ke Data-Link layer, dan disini packet dienkapsulasi dalam sebuah frame dan ditambahkan data-link header.



6. Selanjutnya frame diteruskan ke Physical layer untuk diconvert ke dalam bentuk bit kemudian ditransmisikan ke device tujuan melalui media transmisi.

7. Saat masuk ke device tujuan atau device perantara, layer pertama yang dilalui adalah physical layer. Disini bits diconvert menjadi segment berupa frame dan diteruskan ke Data-link layer.

8. Pada data-link layer, data-link akan membaca data-link header kemudian menghapusnya. Jika ip device tujuan ada dalam ARP table, maka data langsung dikirim ke device tujuan (hal ini terjadi pada switch). Jika tidak maka akan dilanjutkan ke layer 3 yaitu network layer.

9. Pada network layer akan dibaca network header-nya. Untuk mengecek apakah perlu routing lagi atau memang device tersebut tujuannya (terjadi pada router). Namun pada kasus ini, jaringanya berupa peer to peer, yaitu PC ke PC secara langsung tanpa device perantara berupa switch ataupun router, jadi akan langsung diteruskan ke Transport Layer.

10. Pada transport layer, layer ini akan menggabungkan segment-segment yang ada dan mengecek apakah datanya error dan memberikan feedback (laporan), bahwa data sukses atau gagal diterima). Kemudian segment tersebut dikonversi ke bentuk data dan diteruskan ke layer berikutnya.

11. Masuk ke Session Layer, di sini data hanya diarahkan sesuai protokolnya untuk ditindak lanjuti oleh presentation layer.

12. Presentation layer melakukan dekripsi jika diperlukan kemudian meneruskan ke layer berikutnya (Dalam kasus perlu dekripsi karena tadi kita menggunakan FTPS). Kemudian terakhir,

13. Application layer, yang tugasnya menyampaikan data ke aplikasi untuk mengubah data ke bentuk aslinya.

Itu dia gambaran umum tentang Model OSI dan TCP/IP. Sebagai networker, kita harus memahami konsep masing-masing layer khususnya layer 1-4. Hal ini sangat dibutuhkan dalam praktik nanti, implementasi yang paling sering yaitu pada saat troubleshoot. Teman-teman akan menemui error dan mencari di mana errornya serta memperbaikinya.

H. Internet Protocol version 4 (IPv4).

Internet Protocol (IP) adalah protokol jaringan yang menyediakan pengalamatan untuk setiap host dalam jaringan komputer. IP merupakan protokol yang bekerja pada Layer 3 yaitu Network Layer.

IP Addresss adalah deratan angka binner berukuran 32 bit atau 128 bit yang digunakan sebagai alamat suatu perangkat dalam jaringan komputer. Jika dalam kehidupan nyata IP Address bisa diibaratkan sebagai alamat rumah yang dibutuhkan saat mengirim surat atau barang. Saat ini terdapat dua jenis IP Address, yakni IP Address versi 4 (IPv4) dan IP Address versi 6 (IPv6). Dan yang akan kita bahas di sini adalah IPv4.

1. Struktur IPv4

Internet Protocol version 4 atau IPv4 adalah pengalamatan IP berukuran 32 bit yang dibagi menjadi 4 oktet. Jadi setiap oktet terdiri dari 8 bit. Akan tetapi agar mempermudah user (manusia) dalam penulisanya digunakanlah bilang desimal (0-9) dan setiap oktet dipisahkan dengan tanda titik (.). Contoh IPv4 adalah 192.168.10.1.

	Oktet 1	Oktet 2	Oktet 3	Oktet 4
Binary	11000000	10101000	00001010	00000001
Desimal	192	168	10	1

Dalam IP Address ada istilah-istilah seperti ini :

Network ID : IP yang digunakan sebagai alamat jaringan. Kalo di dunia yata kita bisa ibaratkan Network ID atau Network Address ini dengan nama jalan atau nama perumahan

Host ID : IP yang dugunakan sebagai alamat suatu perangkat jaringan (seperti router, pc, dll). Nah kalo ini bisa diibaratkan sebagai nomor rumah dalam suatu jalan/perumahan (jaringan).

Broadcast ID : IP yang digunakan untuk mengirim ke emua host.

Network Mask (Netmask) : Penulisannya seperti format penulisan IP, Netmask sederet angka yang menentukan network address dan host address dari suatu ip address. Contoh netmask 255.255.255.0, 255.255.0.0, dsb. Kita akan pelajari hal ini di materi subnetting.

Prefix : Angka yang mewakili nilai netmask. Contoh ada ip 192.168.1.28/16. Penulisan "/16" menandakan ip tersebut prefixnya adlah"16" yang artinya 16 bit pertama IP tersebut adalah Network ID. Jika ditulis dalam format ip menjadi 255.255.0.0. Kita akan belajar tentang prefix ini juga di materi subnetting.

2. Pembagian Class IPv4

Berdasarkan kelas-nya (class) IPv4 digolongkan menjadi beberapa class sebagai berikut :

IPv4 Address Classes

Class	Range IP Address (desimal)	Range IP Address (binary)	Penggunaan
A	0.0.0.0 - 126.255.255.255	00000000.00000000.00000000.00000000 - 01111110.11111111.11111111.11111111	Unicast
B	128.0.0.0 - 191.255.255.255	10000000.00000000.00000000.00000000 - 10111111.11111111.11111111.11111111	Unicast
C	192.0.0.0 - 223.255.255.255	11000000.00000000.00000000.00000000 - 11011111.11111111.11111111.11111111	Unicast
D	224.0.0.0 - 239.255.255.255	11100000.00000000.00000000.00000000 - 11101111.11111111.11111111.11111111	Multicast
E	240.0.0.0 - 255.255.255.255	11110000.00000000.00000000.00000000 - 11111111.11111111.11111111.11111111	Experimental

IP Address class A memilik default netmask 255.0.0.0 atau prefix 8. Artinya 8 bit pertama (oktet 1) dari IP Class A adalah Network ID. Ini netmask default yang bisa berubah jika kita menerapkan subnetting, prefixnya akan diganti sesuai kebutuhan.

IP Address Class B memiliki default netmask 255.255.0.0 atau prefix 16. Artinya 16 bit pertama (oktet 1 dan 2) dari IP Class B adalah Network ID.

Sedangkan IP Address Class C memiliki default netmask 255.255.255.0 atau prefix 24. Artinya 24 bit pertama (oktet 1,2 dan 3) dari IP Class C adalah Network ID.

Apa itu unicast, multicast, broadcast? Begini penjelasan singkatnya.

Unicast adalah alamat ip yang digunakan pada setiap host (perangkat) untuk saling berkomunikasi poin to point (one to one).
Multicast adalah alamat ip yang digunakan untuk mengirim paket ke beberapa host yang sama-sama *listen* di ip multicast group yang sama (one to many). Biasanya digunakan pada protokol routing.
Broadcast adalah alamat ip yang digunakan untuk mengirim paket ke semua host (one to all).

3. IPv4 Reserved Address

IPv4 jug ", alamat ini tidak digunaka rtentu atau dengan tujuan ter

IPv4 Reserved Address

0.0.0.0	Umumnya digunakan untuk medefinisikan invalid ip, default route ip yang tidak diketahui.
127.0.0.0 - 127.255.255.255	Loopback Address, biasanya digunakan untuk localhost (IP di dalam satu komputer) sebagai ip untuk debuging di localhost
169.254.0.0 - 169.254.255.255	Link-local Address, IP yang biasanya diberikan saat request DHCP gagal.
255.255.255.255	Broadcast Address, untuk mengirimkan oaket secara broadcast.

4. IPv4 Private Address

Selain itu, ada juga istilah IP Private. Karena di internet banyak sekali komputer yang terhubung. Maka disediakan IP Private yang g tidak terhubung langsung ke internet, biasa disebut jaringan lokal. Jadi, ediakan khusus untuk digunakan pada jaringan lokal. Range IP Private c

IPv4 Private Address

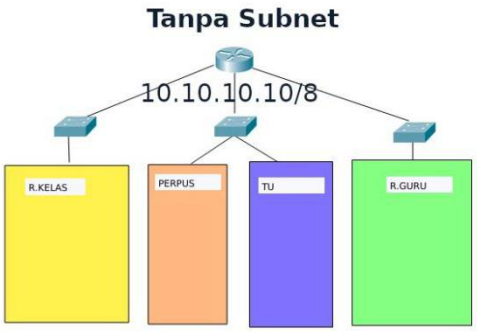
Class	Range IP Address
A	10.0.0.0 - 10.255.255.255
B	172.16.0.0 - 172.31.255.255
C	192.168.0.0 - 192.168.255.255

Tabel di atas adalah IP private, IP class A, B, dan C yang tidak termasuk IP di atas disebut IP Public. IP Public yaitu IP yang digunakan di jaringan internet, menghubungkan beberapa ISP dan server di internet sehingga bisa diakses secara public.

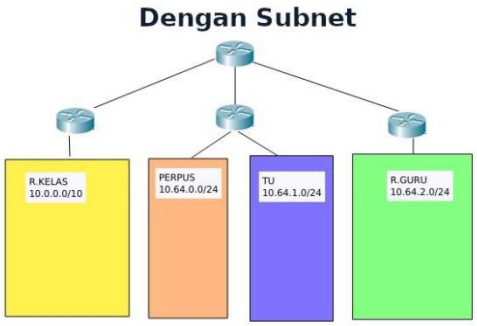
I. IPv4 Subnetting

1. Apa itu Subnetting?

Subnetting adalah membagi jaringan (network) menjadi jaringan yang lebih kecil (subnetwork, disingkat subnet). Salah satu nilai dasar yang perlu diperhatikan dalam mebuat jaringan yang baik adalah optimal. Penggunaan IP adalah salah satu aspek yang perlu dioptimalkan, salah satu caranya adalah memakai ip sesuai kebutuhan dan membagi jaringan dalam kelompok-kelompok jaringan yang lebih kecil.

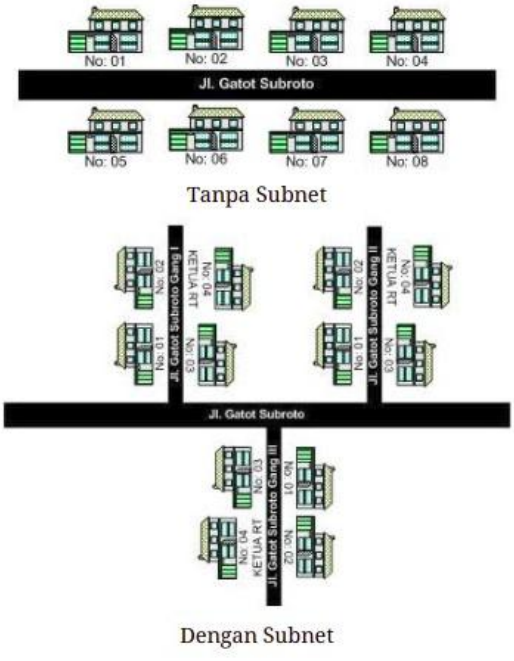


Penerapan subnetting kurang-lebih seperti ini. Misalnya kita punya jaringan sekolah yang butuh ratusan komputer. Jika ratusan komputer tersebut terhubung dengan jaringan yang sama. Selain memberatkan traffic, manajemennya pun akan tercampur aduk.



Oleh karena itu kita perlu membaginya ke jaringan-jaringan yang berbeda berdasarkan ruangan atau sesuai tugasnya. Contohnya kita bagi jaringan sekolah tersebut menjadi beberapa jaringan misalnya : Guru, Tata Usaha, Perpusatakaan, Ruang Kelas.

Jika diilustrasikan dalam kehidupan nyata, subnetting seperti membuat gang-gang kecil sehingga memudahkan dalam pengiriman data ke tujuan.



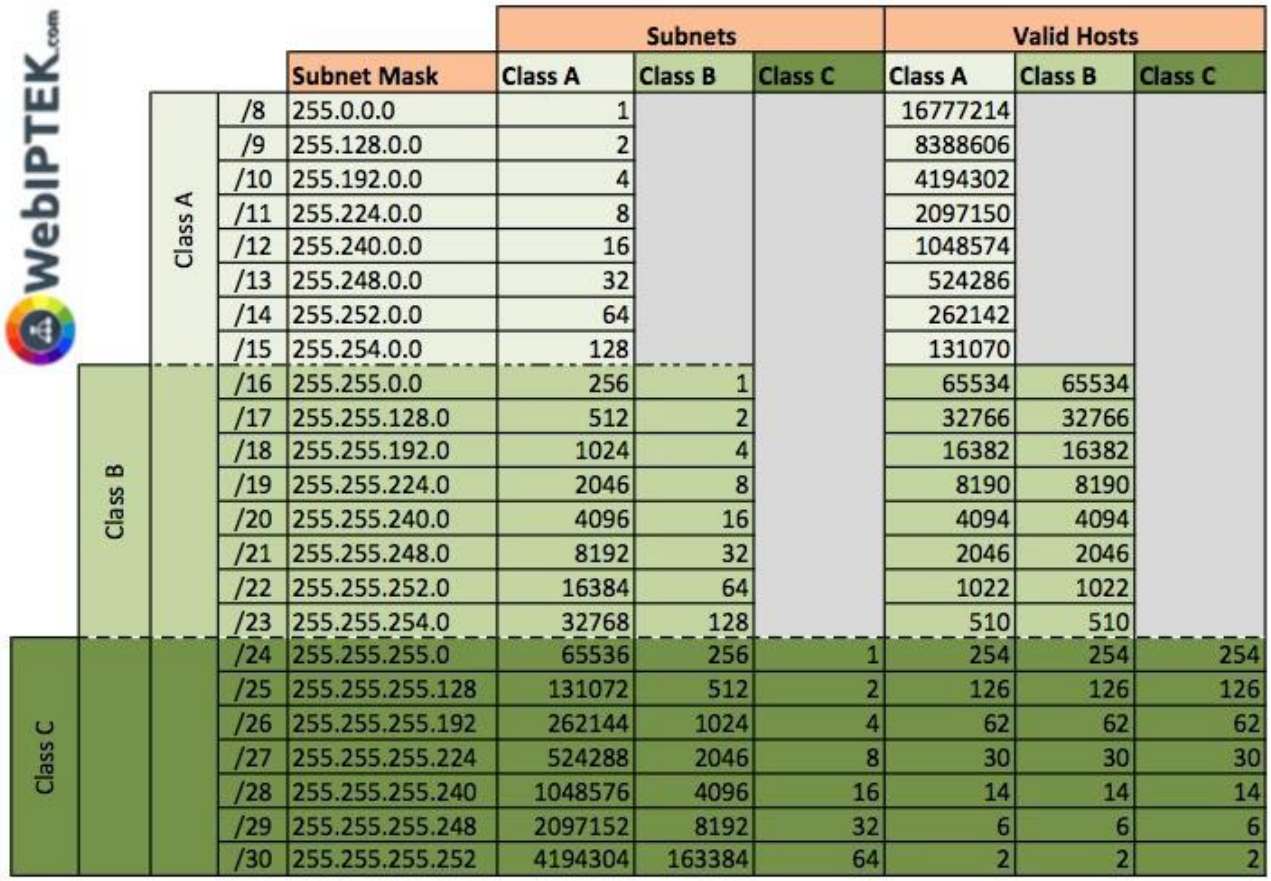
Ada beberapa keuntungan membagi jaringan ke dalam subnet. Yang pertama, memudahkan manajemen. Dengan membagi jaringan kita bisa menerapkan aturan yang berbeda setiap subnetnya (sub-jaringan). Misalnya di Subnet Ruang Kelas tidak diberikan akses internet, hanya akses ke jaringan lokal saja. Sementara di perpustakaan diperbolehkan akses internet hanya saja dibatasi beberapa situs aja, dll.

Yang kedua meringankan traffic. Contoh kasusnya saat ada broadcast, jika jaringan tidak dibagi-bagi maka broadcast akan dikirim ke ratusan komputer. Sedangkan jika sudah dibagi-bagi ke dalam subnet, broadcastnya hanya dikirimkan ke beberapa atau puluhan komputer saja

2. Classless Inter-Domain Routing (CIDR)

CIDR (Classless Inter-Domain Routing) adalah metode alokasi IP Address tanpa diperngaruhi class IP. Jadi dengan CIDR, kita bisa menggunakan netmask di luar class IP tersebut. Misal IP Class

A bisa menggunakan netmask IP class A, B, dan C. IP Class B bisa menggunakan netmask iIP Class B dan C. Sedangkan IP Class C hanya bisa mengunakan netmask IP Class C.



			Subnet Mask	Subnets			Valid Hosts		
				Class A	Class B	Class C	Class A	Class B	Class C
Class A		/8	255.0.0.0	1			16777214		
		/9	255.128.0.0	2			8388606		
		/10	255.192.0.0	4			4194302		
		/11	255.224.0.0	8			2097150		
		/12	255.240.0.0	16			1048574		
		/13	255.248.0.0	32			524286		
		/14	255.252.0.0	64			262142		
		/15	255.254.0.0	128			131070		
	Class B	/16	255.255.0.0	256	1		65534	65534	
		/17	255.255.128.0	512	2		32766	32766	
		/18	255.255.192.0	1024	4		16382	16382	
		/19	255.255.224.0	2046	8		8190	8190	
		/20	255.255.240.0	4096	16		4094	4094	
		/21	255.255.248.0	8192	32		2046	2046	
		/22	255.255.252.0	16384	64		1022	1022	
		/23	255.255.254.0	32768	128		510	510	
Class C		/24	255.255.255.0	65536	256	1	254	254	254
		/25	255.255.255.128	131072	512	2	126	126	126
		/26	255.255.255.192	262144	1024	4	62	62	62
		/27	255.255.255.224	524288	2046	8	30	30	30
		/28	255.255.255.240	1048576	4096	16	14	14	14
		/29	255.255.255.248	2097152	8192	32	6	6	6
		/30	255.255.255.252	4194304	163384	64	2	2	2

Pertanyaan tentang subnetting IP metode CIDR diantaranya: ada berapa jumlah subnet? berapa jumlah IP atau host per subnet? berapa ukuran subnet (block size)? berapa network address masing-masing subnet? berapa broadcast address masing-masing subnet? Berapa range IP atau host yang valid?

Sebelum kita masuk ke contoh, untuk menjawab pertanyaan di atas, kita perlu tahu yang namanya netmask. Netmask inilah yang nantinya akan menentukan jawaban persoalan di atas. Kita mungkin bisa menggunakan tabel di atas, tetapi kita perlu tahu konsep dasarnya karena akan sulit jika kita menghafal tabel di atas. Kita perlu paham konsepnya nanti secara otomatis kita bisa hafal tabel di atas jika memperbanyak praktik.

Network Mask atau biasa disingkat netmask adalah sederet angka yang menentukan network address dan host address dari suatu ip address.
Contoh netmask: 255.255.255.0
Jika diubah jadi binner: 11111111.11111111.11111111.00000000

Prefix : notasi penulisan netmask.
Prefix /26 berarti 26 bit pertama dari kiri adalah angka 1 (angka 1-nya ada 26).
Contoh: 192.168.1.1/27

27 menunjukan jumlah angka 1, prefix /27 berarti ada 27 angka 1.
11111111.11111111.11111111.11100000 = 255.255.255.224

Untuk menentukan nilai desimal suatu oktet, ada rumus:
256-2n (n = j umlah angka 0)**.**

Nilai desimal netmasuk juga berpola 0, 128, 192, 224, 240, 248, 252, 254, 255. Ketika angka 1-nya tidak ada maka nilai desimalnya adalah 0, jika angka 1-nya ada 1 nilai desimalnya adalah 128, dan seterusnya sampai semuanya angka 1 (ada 8) maka nilai desimalnya adalah 255.

Contoh: 10.10.10.10/14
Netmask = 11111111.11111100.00000000.00000000 = 255.252.0.0

LATIHAN
Cari netmask (desimal) dari ip berikut:
1. 192.168.10.5/29
2. 172.16.20.20/28
3. 10.1.1.100/9

Sekarang kita akan mencoba menjawab pertanyaan di awal tadi. Contoh IP yang akan kita subneting adalah 192.168.16.0/26
Kita cari netmasknya dulu dari prefix /26 yaitu:
11111111.11111111.11111111.11000000 = 255.255.255.192

x = jumlah angka 1 pada oktet yg kita ubah menjadi biner
y = jumlah angka 0 pada oktet yg kita ubah menjadi biner

1. Ada berapa jumlah subnet?

Jumlah Subnet = 2^x

Contoh :
$2^2 = 4$
Jadi, jumlah subnet yang bisa kita bentuk dari IP 192.168.16.0/26 adalah 4 subnet.

2. Berapa IP atau hosts valid per subnet?

Jumlah IP per subnet = 2^y - 2

Contoh :
$2^6 - 2 = 62$
Jadi, jumlah host per subnetnya adalah 62 host.

Jika netmask yang digunakan 255.255.XXX.0, kamu cukup menghitung oktet ke 3 kemudian dikali dengan 256.
Contoh:
172.16.0.0/22
subnetmasknya 255.255.252.0 atau 11111111.11111111.11111100.00000000.
Abaikan oktet 4, hitung saja bilangan binner di oktet 3.
(2^2 x 256) - 2 = **1022 IP/Hosts**

Demikian pula jika netmasknya 255.XXX.0.0, berarti dikali 256^2. Contohnya ini:
10.0.0.0/14
subnetmasknya 255.252.0.0 atau 11111111.11111100.00000000.00000000.
Abaikan oktet 3 dan 4, hitung saja bilangan binner di oktet 2.
(2^2 x 256 x 256) - 2 = **262142 IP atau Hosts**

3. Berapa block sizenya?

Block Size = 256 - XXX = 2^y

XXX adalah nilai netmask pada block yang terdapat angka 0 (dalam binner).
Block size ini digunakan
Subnetmask: 255.255.255.192

Contoh :
256 - 192 = 64
Atau 2^6 =64

Jadi, ukuran block setiap subnetnya adalah 64. Ukuran subnet biasa sebut juga increment size, atau besar interval

4. Network Address (Network ID) per subnet

kelipatan interval/block size adalah network address.

Contoh :
Tadi ukuran block sizenya adalah 64. Berarti network idnya adalah kelipatan 64 dimulai dari 0, 64, 128, dan 192.

Jika ditulis lengkap:
Subnet 1 : 192.168.16.0/26
Subnet 2 : 192.168.16.64/26
Subnet 3 : 192.168.16.128/26
Subnet 4 : 192.168.16.192/26

5. Broadcast Address (Broadcast ID) per subnet

Network ID subnet berikutnya dikurangi 1

Contoh :
Subnet 1 : 64-1 = 63
Subnet 2 : 128-1 = 127
Subnet 3 : 192-1 = 191
Subnet 4 : 256-1 = 255
Jika ditulis lengkap
Subnet 1 : 192.168.16.63/26
Subnet 2 : 192.168.16.127/26
Subnet 3 : 192.168.16.191/26
Subnet 4 : 192.168.16.255/26

6. Range host yang valid atau IP yang bisa digunakan

Range di antara Network ID dan Broadcast ID

Contoh : Subnet 1 misalnya networknya 192.168.16.0, sedangkan broadcastnya 192.168.16.63. Maka range host validnya adalah 192.168.16.1 - 192.168.16.62.
Subnet 1 : 192.168.16.1 - 192.168.16.62
Subnet 2 : 192.168.16.65 - 192.168.16.126
Subnet 3 : 192.168.16.129 - 192.168.16.190
Subnet 4 : 192.168.16.193 - 192.168.16.254

Ada juga soal yang bentuknya sepert ini:
Berapa Network Address, Broadcast Address, dan Range Valid Host dari IP 200.100.100.50/27?
Cara menghitungnya begini.
Karena prefix /27 netmasknya 255.255.255.224 maka kita hanya perlu otak-atik oktet ke-4. Cari block sizenya (interval) terlebih dahulu.
256-224 = 32

Kemudian kita buat daftar Network ID-nya yaitu mulai dari 0 dan cari dimana letak angka oktet ke-4 yaitu 50.
0, 32, 64, 96,dst.
Jika kamu sudah menemukan dimana letak angka yang dicari yaitu 50, tidak perlu dilanjut sampai 256.

Nah, angka 50 berada di antara 32 dan 64. Maka sudah bisa simpulkan dengan rumus mencari network dan broadcast yang dijelaskan sebelumnya.
Network = 200.100.100.32/27
Broadcast = 200.100.100.63/27
Range IP = 200.100.100.33 - 200.100.100.62

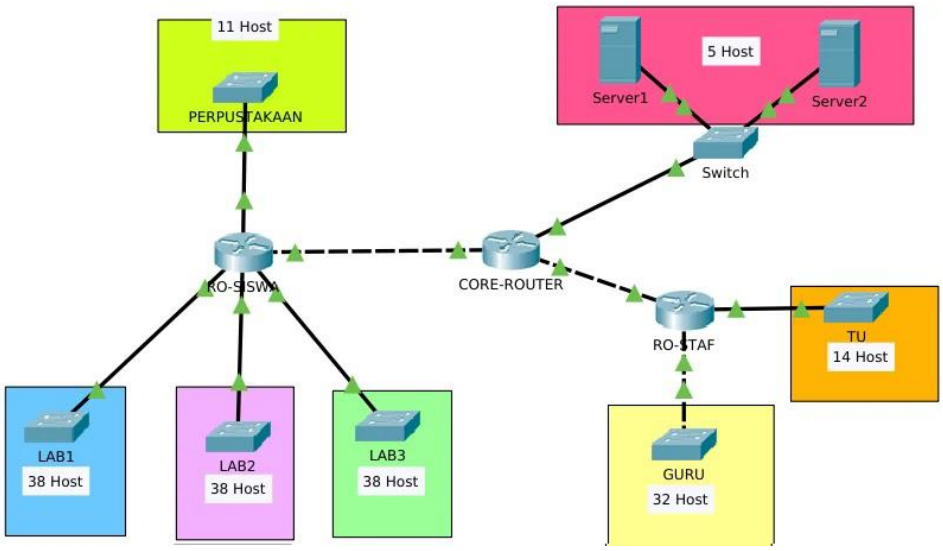
LATIHAN
Carilah jumlah subnet, valid host per subnet, block size, network, broadcast, dan range ip masing-masing subnet dari IP berikut.
1. 192.168.23.0/25

Cari network, broadcast, dan range IP yang bisa digunakan dari IP:
2. 200.2.2.20/29
3. 172.16.30.30/22
4. 192.168.103.103/28

3. FLSM dan VLSM

- Fixed Length Subnet Mask, FLSM adalah teknik pembagian network yang mana setiap subnet memiliki ukuran subnetmask yang sama.
- Variable Length Subnet Mask, VLSM adalah teknik pembagian network yang mana setiap subnet memiliki ukuran subnetmask yang berbeda tergantung jumlah host yang ada di network tersebut.

Berikut ini adalah topologi yang akan kita gunakan untuk mengimplementasikan subnetting metode FLSM dan VLSM.



a. Subnetting metode FLSM

Sekarang kita mulai menghitung pengalamatan IP untuk jaringan bagian kiri dari CORE-ROUTER. Kita lihat spesifikasi yang diperlukan:
PERPUSTAKAAN = 11 hosts
LAB 1 = 38 hosts
LAB 1 = 38 hosts
LAB 1 = 38 hosts
Bonus Catatan:
*Jumlah komputer di dalam lab fixed 37 ditambah 1 ip untuk router, tidak ada rencana penambahan komputer, kecuali bikin lab baru.
*Untuk perpustakaan ada rencana penambahan komputer.

Di situ kan jumlah hostnya kebanyakan sama (38), bahkan bisa dibilang sama kecuali perpustakaan. Kita lihat juga ada catatan bahwa jumlah komputer pada lab tidak ada rencana penambahan komputer, artinya kita tidak perlu mengira-ngira lagi berapa jumlah tambahan komputernya, fixed 38 hosts sudah termasuk 1 Host untuk gateway (IP Router). Soal penambahan lab baru, kita bisa gunakan ip lain.

Sedangkan untuk perpustakaan kita bisa konfirmasi berapa yang akan ditambah, misal si kepala sekolah atau project managernya bilang "tidak tahu, yang jelas tidak akan lebih dari 30". Angka 30 tentunya tidak lebih besar 38. Nah dari sini kita bisa menyimpulkan kita bisa menggunakan metode FLSM.

Host yang paling banyak yaitu 38 Hosts. Kemudian "Berapa Subnetmask yang jumlah host sama dengan 38 atau yang lebih besar paling mendekati 38?".
Kita harus paham konsep netmask/subnetmask untuk menjawab pertanyaan tersebut. Atau bisa menggunakan rumus dari konsep bahwa subnetmask itu berpola dari angka 0, 1, 2, 4, 8, 16, 32, 64, 128, 255. Rumus menghitung jumlah hostnya yaitu:
Jumlah host = 256 - n (n adalah value subnetmask tersebut)

Dari rumus tersebut kita bisa tentukan berapa netmasknya:
n = 256 - Jumlah host
n = 256 - (39+2) = 215

Kemudian berapa pola netmask yang mendekati lebih kecil atau sama dengan hasil tersebut (215), yaitu 192. Maka subnetmasknya adalah 255.255.255.192

Atau ada rumus lagi seperti ini:
2^y - 2 >= 38
>= artinya lebih besar mendekati atau sama dengan. Berapa nilai y? 6 kan, 2^6 - 2 = 62.
Kalo belum hafal perpangkatan, hitung saja seperti ini:
2x2 = 4
2x2x2 = 8
2x2x2x2 = 16
2x2x2x2x2 = 32
2x2x2x2x2x2 = 64
Berhenti menghitung saat nilainya sudah melebihi atau sama dengan 38.

Kemudian 256 - 64 = 192.

Konversi ke desimal jadi 255.255.255.192. (sama kan dengan rumus sebelumnya)

Kita kembali lagi ke spesifikasi jaringan yang akan dibuat yaitu 3 jarigan berukuran 38 Host dan 1 jaringan berukuran 11 host yang rencanaya akan ditambah, total ada 4 jaringan. Prefix /24 mempunyai 256 IP yan jika kita bagi hasil subnetting kita tadi yaitu 64 (62+2). Maka hasilnya 4 kan, pas untuk jumlah jaringan (yaitu 4) dan jumlah ip untuk host yang diperlukan (yaitu 62 untuk 38 host). Jadi hasilnya begini:
PERPUSTAKAAN = 192.168.100.0/26
LAB 1 = 192.168.100.64/26
LAB 2 = 192.168.100.128/26
LAB 3 = 192.168.100.192/26
Kalo mau nambah lab yang isinya 37 komputer, bisa gunakan ip berikutnya 192.168.101.0/26.

b. Subnetting metode VLSM

Nah sekarang kita akan menghitung jaringan di sebelah kanan CORE-ROUTER dan jaringan yang terhubung ke Core Router dengan metode VLSM, yaitu pada jaringan:

SERVER : 5 Hosts
GURU : 32 Host
TU : 14 Hosts
CORE-ROUTER -> RO-SISWA : 2 Hosts
CORE-ROUTER -> RO-STAF : 2 Hosts

Untuk metode VLSM kita akan menghitung dari jaringan yang jumlah hostsnya yang paling besar, yaitu 32, baru kemudian ke yang lebih kecil.

Kita akan bertemu lagi dengan pertanyaan “Berapa netmask yang hostsnya sama dengan atau lebih besar mendekati 32 host?”. Jika belum hafal teman-teman bisa menggunakan rumus yang dijelaskan pada FLSM.

Jawabannya adalah 62 hosts atau prefix /26 dengan 6 2hosts. Maka network untuk GURU adalah 172.16.0.0/26.

Selanjutnya kita hitung network yang terbesar setelah GURU, yaitu TU dengan 14 hosts. Lagi-lagi teman-teman harus tau, "berapa netmask yang hostnya sama dengan atau lebih besar mendekati 14 hosts?"

Jawabanya adalah prefix /28 dengan 14 hosts. Maka network address TU adalah 172.16.0.64/28.
Lalu, angka 64 itu dari mana? Kan tadi subnet pertama sudah diambil oleh GURU 172.16.0.0/26, subnet berikutnya kan 172.16.0.64/26.
Jika bingung cara menghitung IP Network berikutnya. Tambahkan saja network sebelumnya dengan jumlah hostnya + 2. Kenapa +2? Kan ada 2 ip untuk network dan broadcast yang tidak dihitung sebagai host.

Misal network sebelumnya kan 172.16.0.0/26 dengan jumlah host 62, berarti angka penambahannya adalah 62+2 = 64, seperti ini.
172.16.0.0 + 0.0.0.64 = 172.16.0.64.

Lalu kenapa prefixnya 28? Karena kita sudah subnetting dan cuma butuh 14 host, prefix yang lebih besar mendekati atau sama dengan 14 host adalah /28.

Lakukan hal serupa pada network berikutnya, ingat ya hitung terlebih dahulu network yang hostsnya lebih besar.

SERVER : 5 Host, prefix yang hostnya sama dengan atau lebih besar mendekati 5 adalah prefix /29 dengan 6 host.
172.16.0.64 + 0.0.0.16 = 172.16.0.80
Network SERVER adalah 172.16.0.80/29.

CORE-ROUTER -> RO-SISWA : 2 Host, prefix yang hostnya sama dengan atau lebih besar mendekati 2 adalah prefix /30 dengan 2 host.
172.16.0.80 + 0.0.0.8 = 172.16.0.88
Network CORE-ROUTER -> RO-SISWA adalah 172.16.0.88/30.

CORE-ROUTER -> RO-STAF : 2 Host, prefix yang hostnya sama dengan atau lebih besar mendekati 2 adalah prefix /30 dengan 2 host.
172.16.0.80 + 0.0.0.8 = 172.16.0.92

Network SERVER adalah 172.16.0.92/30.

Jadi hasilnya seperti ini,
SERVER : 172.16.0.0/26
GURU : 172.16.0.64/28
TU : 172.16.0.80/29
CORE-ROUTER -> RO-SISWA : 172.16.0.88/30
CORE-ROUTER -> RO-STAF : 172.16.0.92/30

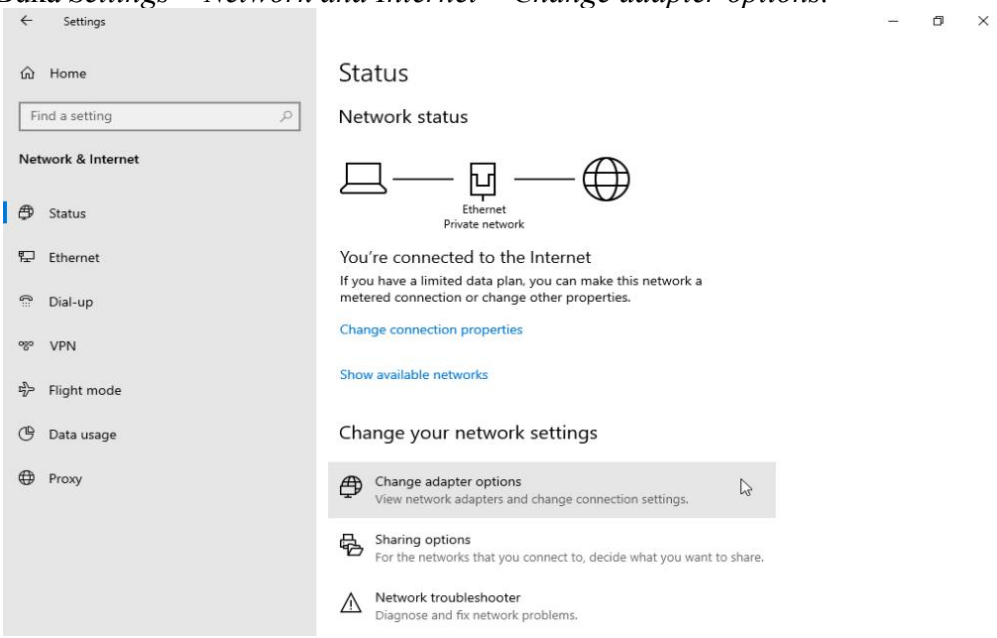
LATIHAN
Tentukan pembagian IP 192.168.111.0/24 untuk jaringan sebuah kantor berikut:
R. Karyawan : 100 Host
R. Server : 8 Host
R. Meeting : 33 Hots

BAB 2 - MEMBANGUN JARINGAN LAN

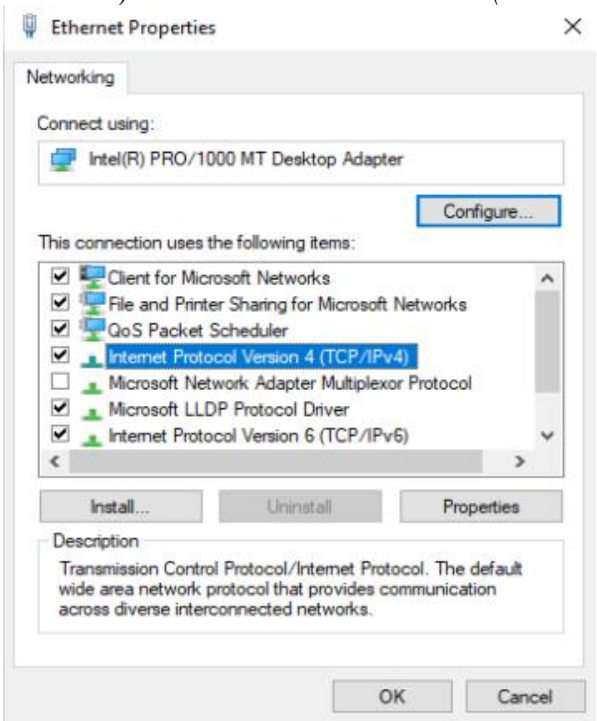
Local Area Network (LAN) adalah jaringan komputer yang berada dalam sebuah gedung, kantor, rumah, atau sekolah. Di materi ini kita akan belajar mengkonfigurasi service (layanan) yang umum digunakan pada jaringan LAN, yaitu: sharing file, sharing printer, dan web server. Dalam contoh ini kita akan mengggunakan PC dengan sistem operasi Windows 10.

Dalam membuat jaringan dengan Windows 10, kita perlu tahu konfigurasi dasar terlebih dahulu. Yang pertama adalah konfigurasi IP Address.

1. Buka *Settings > Network and Internet > Change adapter options.*

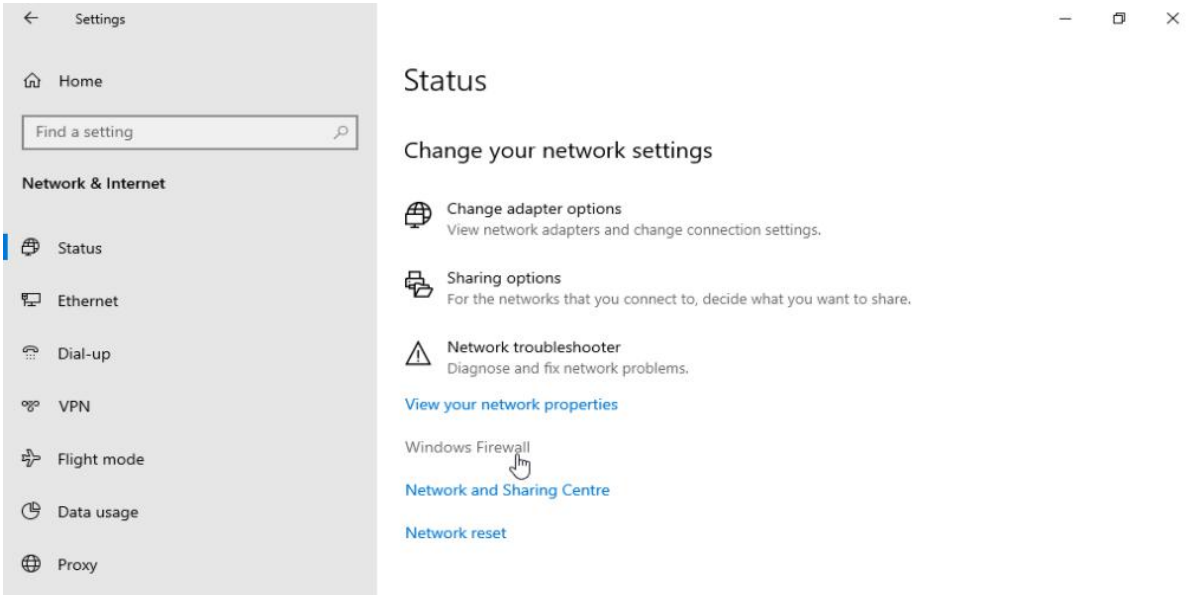


2. Klik kanan pada interface yang akan kita konfigurasi IP. Kemudian pilih *properties* lalu pilih (double-click) *Internet Protocol version 4 (TCP/IPv4).*

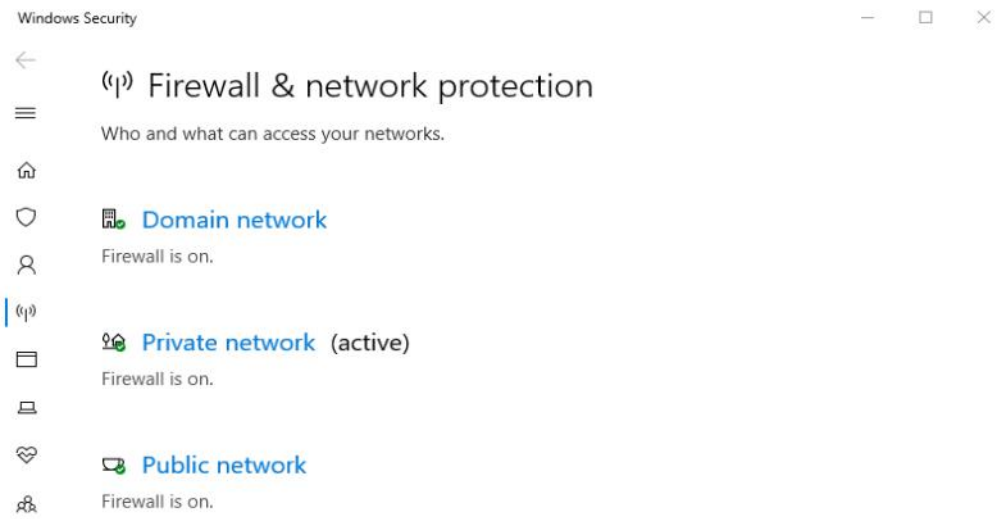


3. Ada dua pilihan dalam mengkonfigurasi IP Address yaitu statis dan dinamis. Jika kita memilih o*btain automaticaly* maka IP Address akan dikonfigurasi secara dinamis melalui DHCP, di sini PC kita perlu terhubung dengan DHCP Server. Akan tetapi jika ingin mengkonfigurasi secara manual, bisa memilih option ke dua, *use the following ip address.*

Selain konfigurasi IP address, dalam menjalankan Windows 10 sebagai server kita juga terkadang perlu menonaktifkan Windows Firewall agar service kita bisa diakses dari komputer lain. Cara menonaktifkan windows firewal, seperti biasa buka *Settings > Network and Internet.* Kemudian pilih *Windows Firewall.*



Lalu akan muncul jendela baru windows secuirty, seperti di bawah ini.

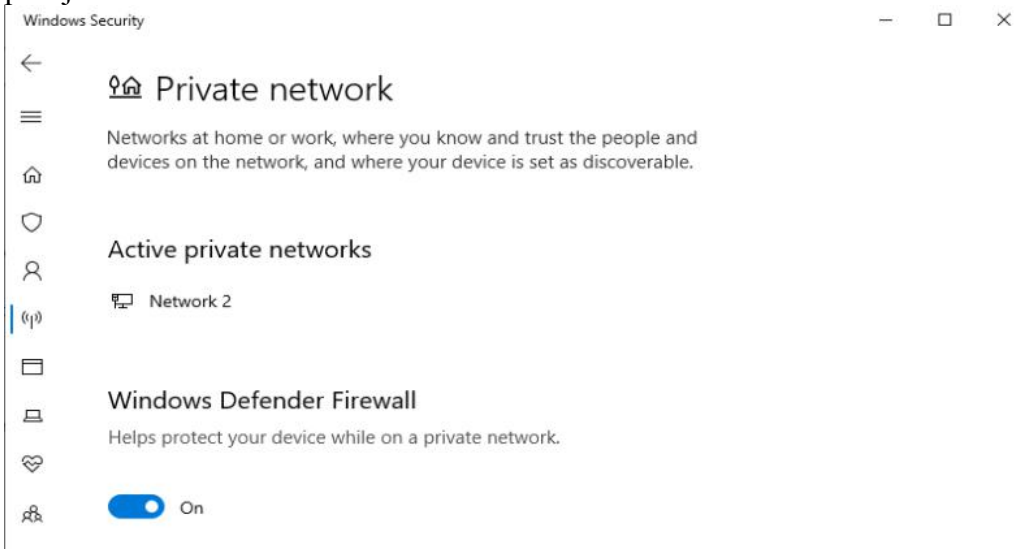


Ada 3 firewall yaitu firewall untuk Domain network, Private network, Public network.

Saat firewall **domain network** kita nonaktifkan, layanan pada kompter kita akan bisa diakses dari komputer yang memiliki domain sama dengan kita. Konfigurasi domain memerlukan windows server.
Kemudian jika firewall **private network** kita nonaktifkan, maka layanan pada komputer kita akan bisa diakses dari komputer yang satu network address dengan komputer kita (satu segmen jaringan).

Dan jika firewall **public network** yang dinonaktifkan, maka komputer kita bisa diakses dari mana saja, siapa saja, asal bisa terhubung dengan komputer kita.

Untuk mematikannya klik saja salah satu networknya (domain, private, atau public network), pada bagian widows defender firewall kita switch dari On ke Off. Jika ada muncul notifikasi konfirmasi accept saja atau klik Yes.

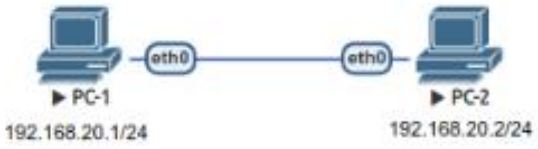


Sekarang kita akan memulai praktik konfigurasi layanan-layanan yang umum digunakan pada jaringan LAN.

A. Sharing Folder

Layanan yang pertama, yaitu sharing folder. Sharing folder ini intinya kita memberikan akses ke suatu directory yang ada pada media penyimpanan kita untuk diakses oleh pengguna (komputer lain), baik hanya sekedar akses membaca (hanya bisa mendownload atau mengambil file), ataupun bisa juga diberi akses write, sehinggu pengguna lain bisa menulis atau menghapus file di direktori kita.

Implementasi yang mungkin sering kita lihat dari layanan sharing folder di ruang kelas, yaitu ketika guru memberikan tugas dalam bentuk digital kepada siswanya, kemudian untuk mempermudah pengumpulan tugas, guru bisa memerintahkan siswa untuk mengumpulkan tugasnya melalui sharing folder ini. Cukup dengan memberi tahu alamat ip dan nama direktori/foldernya dan (jika ada) user login.

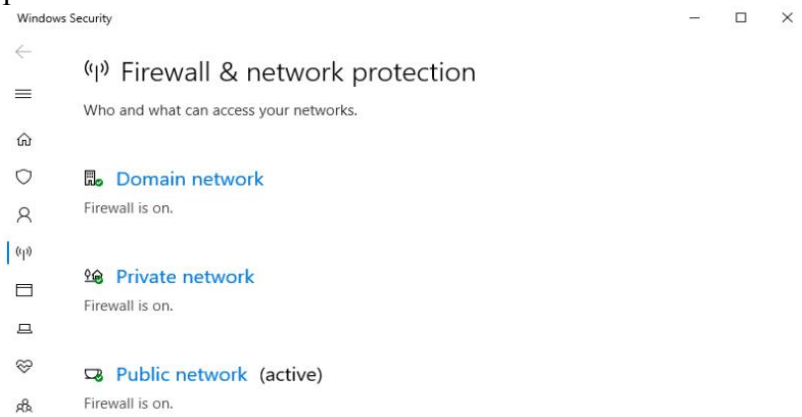


Nah, kita akan mencoba belajar konfigurasi sharing file seperti topologi di atas, salah satu PC bertindak sebagai server (contoh: PC-1) dan yang satunya lagi bertindak sebagai client (contoh: PC-2).

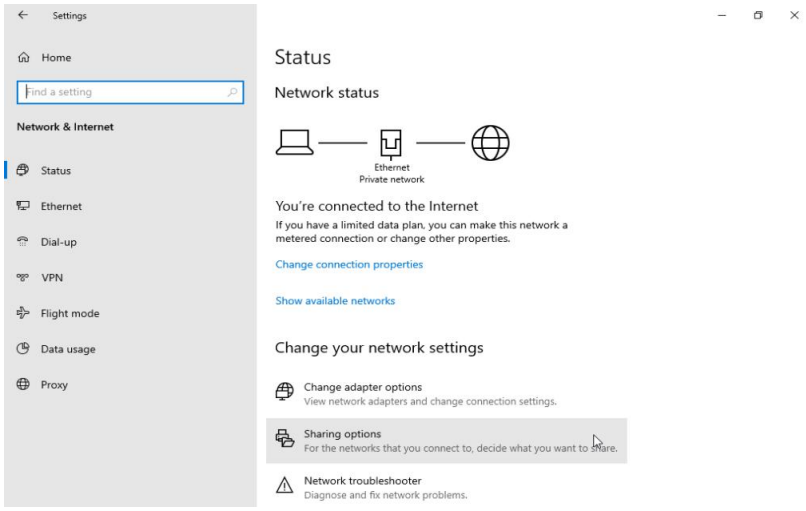
Tujuan:
1. Sharing folder dengan nama “Tugas”. Folder ini nantinya bisa ditulis tapi perlu autentifikasi. Autentifikasinya menggunakan username ***siswa*** dengan password ***123***.
2. Sharing folder dengan nama “Soal”. Folder ini bisa diakses oleh siapa saja tetapi read-only (tidak bisa ditulis).

Langkah Konfigurasi:

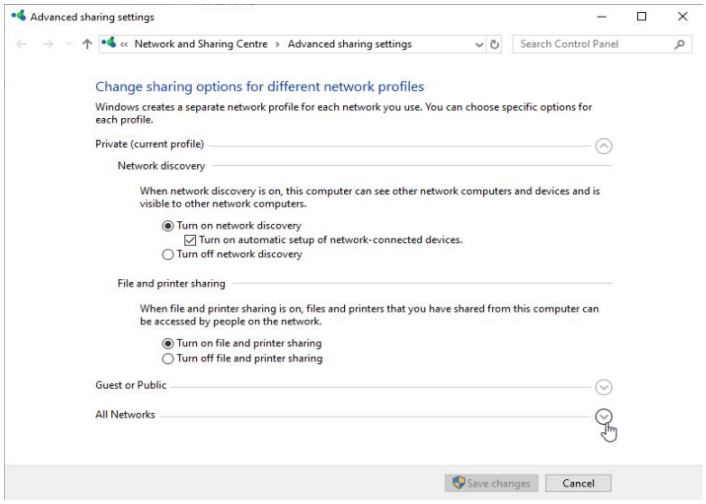
1. Kita perlu konfigurasi IP Address terlebih dahulu dan mematikan firewall di PC-1, firewall yang dimatikan adalah yang ada tulisan active. Biasanya saat uji coba point to point yang active adalah public.



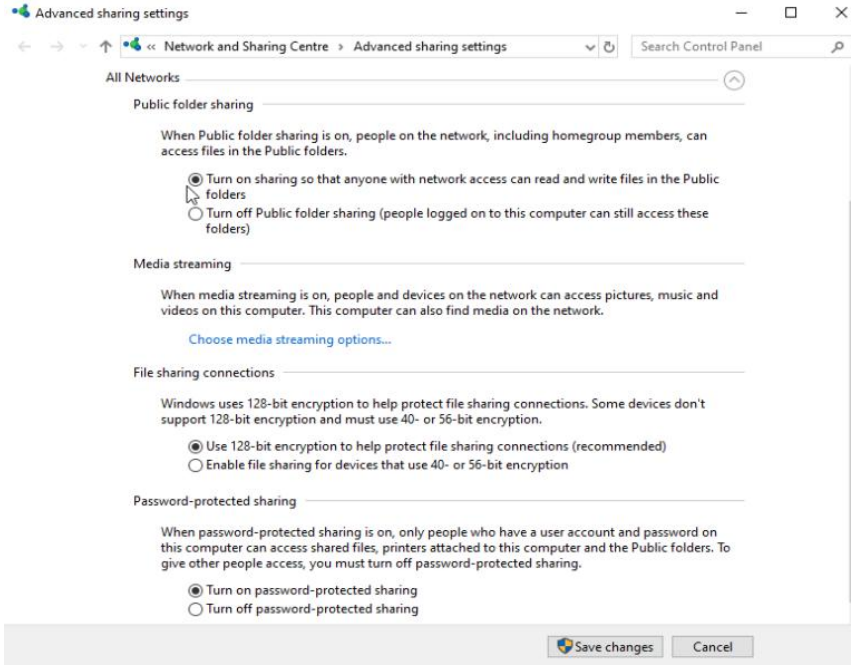
2. Jika sudah konfigurasi IP dan firewall, untuk layanan sharing folder kita juga perlu *sharing option*. Masih di *Settings > Network and Internet.* Kemudian pilih *Sharing options.*



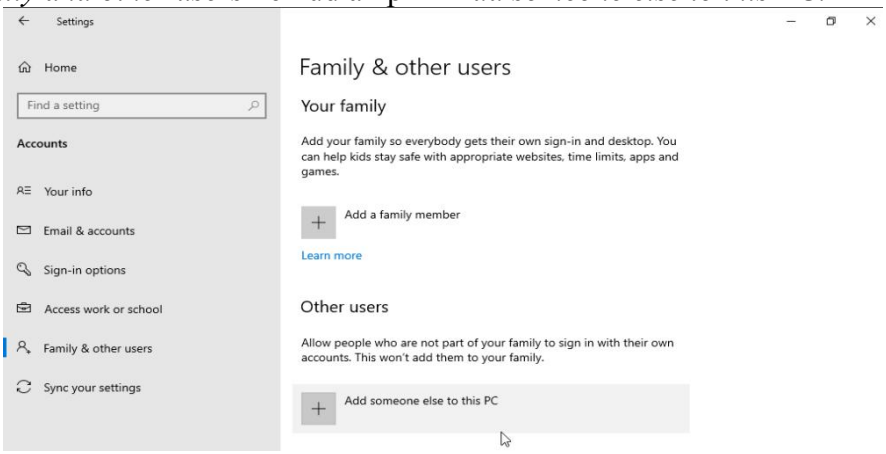
3. Akan muncul jendela baru, Advace sharing settings, klik pada icon panah di samping *All network.*



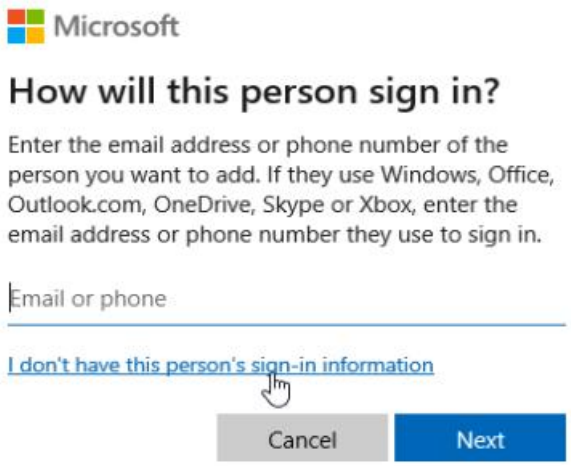
4. Kemudian pada bagian *Public folder sharing*, pilih yang *"Turn on sharing so ...."*. Dan pada *password-protected sharing* pilih *"Turn on ..."*. Lainnya biarkan default.



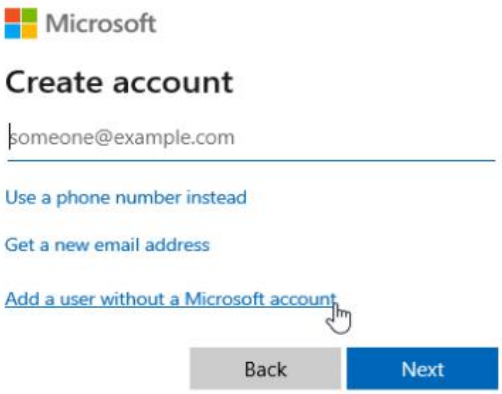
5. Selanjutnya, kita buat user untuk autentifikasi nantinya. Di contoh ini kita akan membuat local user (tanpa email). Untuk membuat user di Window 10, buka *Settings* > *Accounts*. Kemudian pilih *Family and other users* kemudian pilih *Add someone else to this PC.*



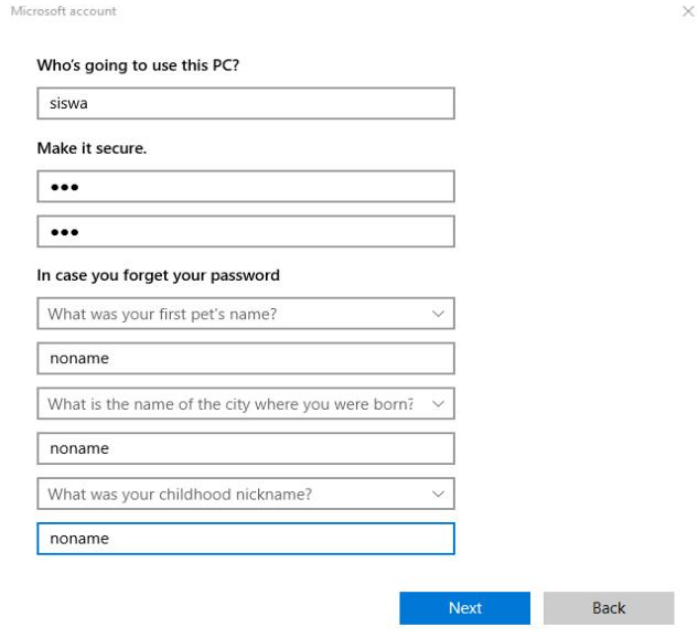
6. Jika kita tidak terkoneksi internet maka akan langsung ditampilkan form untuk membuat akun lokal. Tetapi jika kita terkoneksi internet yang tampil adalah login page akun microsoft. Jika yang tampil login page akun microsoft kita perlu pilih *I don't have this person's sign-in information.*



7. Lalu kita akan diarahkan ke halaman baru seperti berikut, kita plih *Add a user without a Microsoft account.*

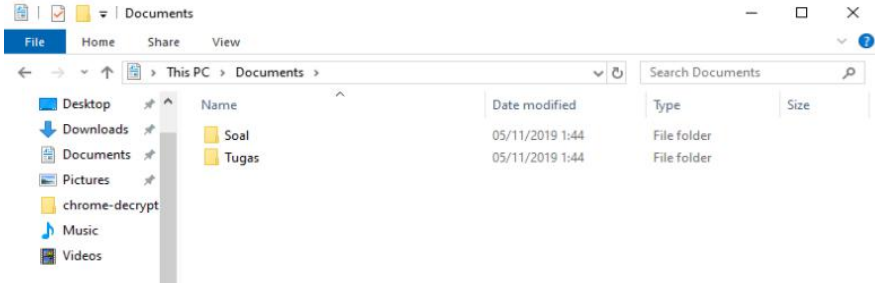


8. Lalu kita isi form akun sesuai perintah di awal tadi username *siswa* dengan password *123*. Untuk question security isi terserah saja. Kemudian klik Next.

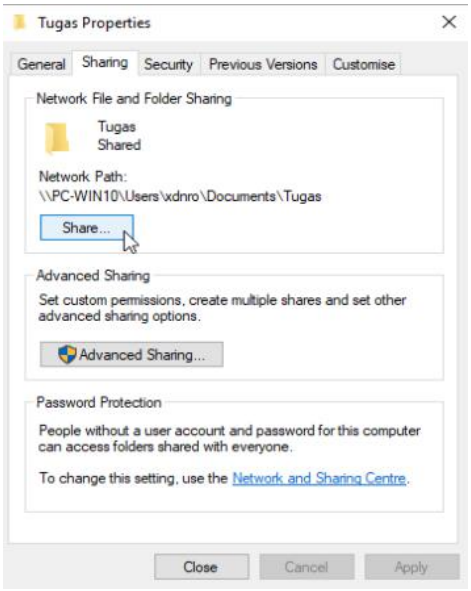


Akun untuk autentifikasi sudah dibuat.

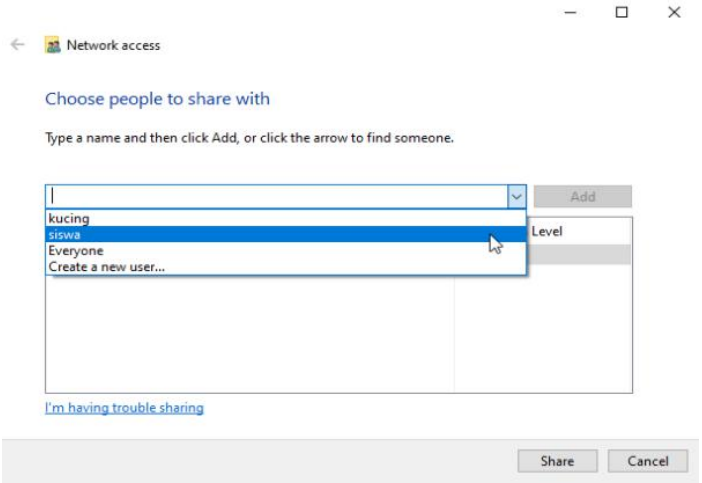
9. Selanjutnya kita buat folder "Tugas" dan "Soal" serta di dalam folder Soal dibuat file contoh-soal.txt. Karena tidak dirincikan membuat foldernya di mana kita bebas mau memmbuatnya di mana, tetapi jika di perintahnya letak foldernya di direktori tertentu kita juga harus membuatnya pada direktori tertentu tersebut.



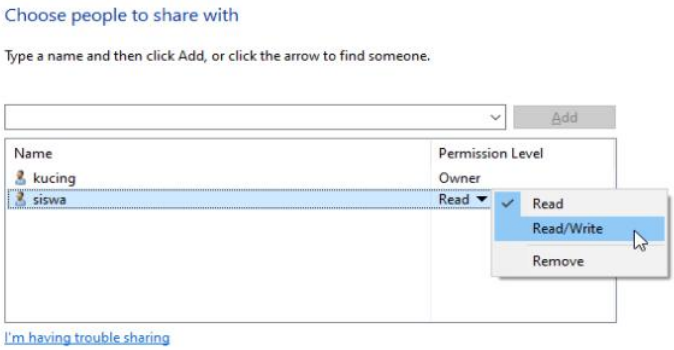
10. Kita konfigurasi folder Tugas dulu. Klik kanan pada folder "Tugas", kemudian pilih *propertieso.* Kemudian pada tab *sharing,* klik *Share.*



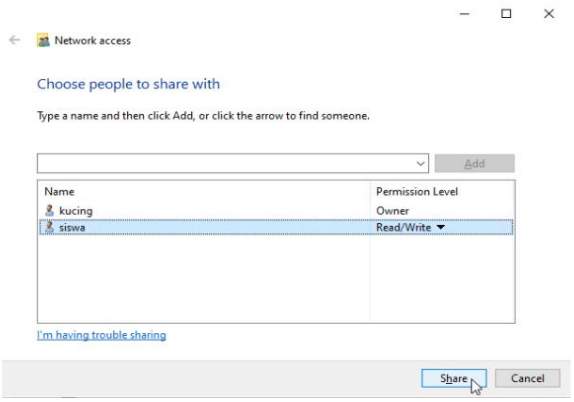
11. Karena folder "Tugas" hanya akan dibagikan kepada user *siswa* dan user *siswa* belum ada pada kolom yang besar bawah, maka kita perlu menambahkan user *siswa* terlebih dahulu. Pada select form pilih *siswa,* kemudian klik Add.



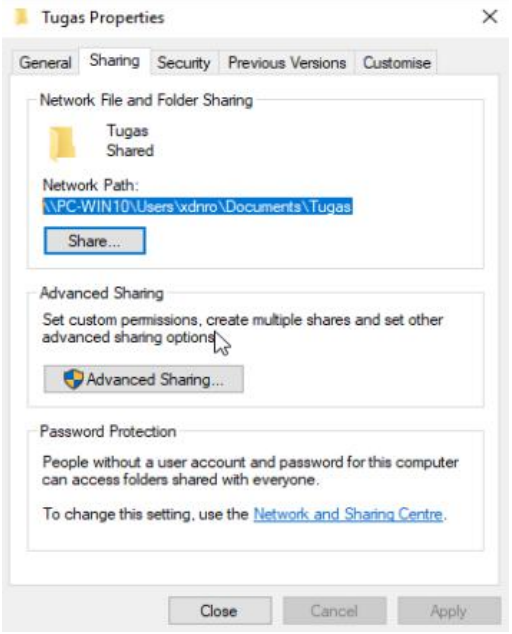
12. Sekarang user *siswa* sudah muncul di kolom yang bawah dengan permission read only. Karena siswa perlu akses write, maka kita ubah permissionnya menjadi *Read/Write* dengan klik tombol panah di samping *Read*.



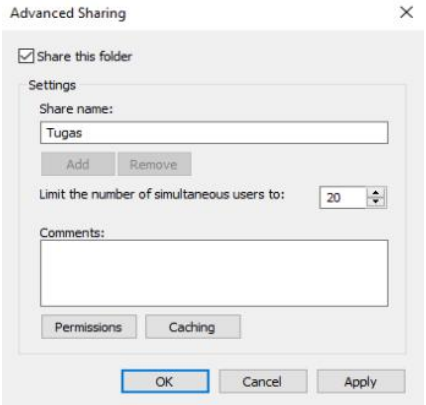
13. Jika sudah sesuai, berikutnya klik tombol *Share* dan *Done*



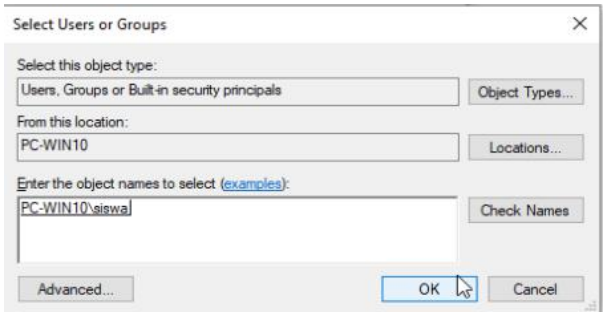
14. Kemudian, kita klik kanan lagi pilih *properties* kemudian tab *sharing*. Di situ lokasi filenya masih jauh di dalam path utama. \\PC-WIN10\User\xdnro\Documments\Tugas. Kita akan membuat lokasinya lebih mudah diakses yaitu \\PC-WIN10\Tugas.



15. Caranya, klik *Advance Sharing*. Ceklist Share this folder, kemudian OK.

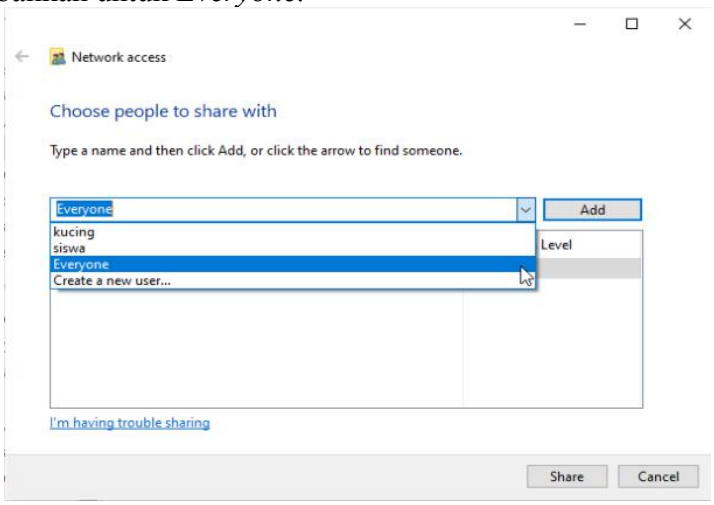


16. Kita juga perlu mengatur *permission* lagi di *Advance Sharing*. Kita tambahkan user *siswa*.

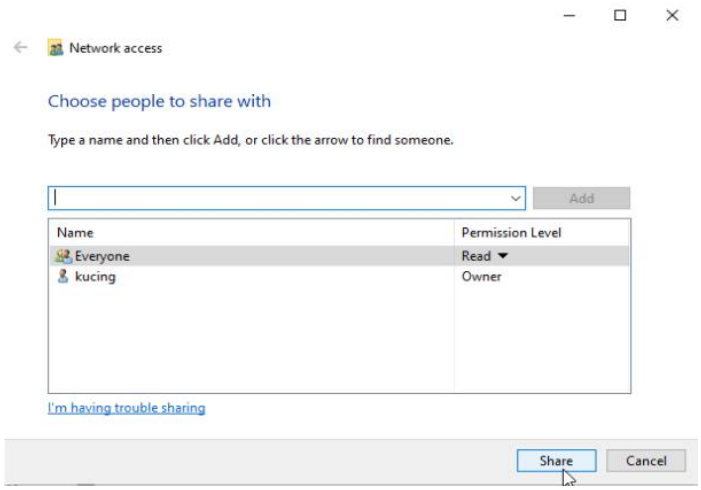


17. Dan permissionya kita set full control.

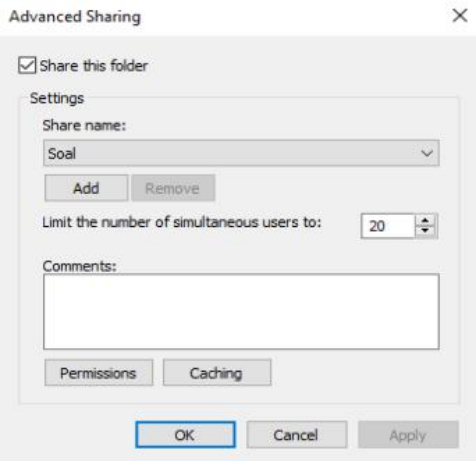
18. Selanjutnya kita konfigurasi untuk folder "Soal", sama seperti tadi, klik kanan pada folder Soal lalu pilih *properties* kemudian *sharing*. Lalu klik share. Karena folder "Soal" dibagikan ke siapa saja (semua orang), maka yang kita tambahkan bukan user tertentu seperti tadi, melainkan kita tambahkan untuk *Everyone.*



19. Dan sesuai perintah di awal, akses atau permissionnya read only. Jadi kita bisa langsung klik *Share* dan *Done*.



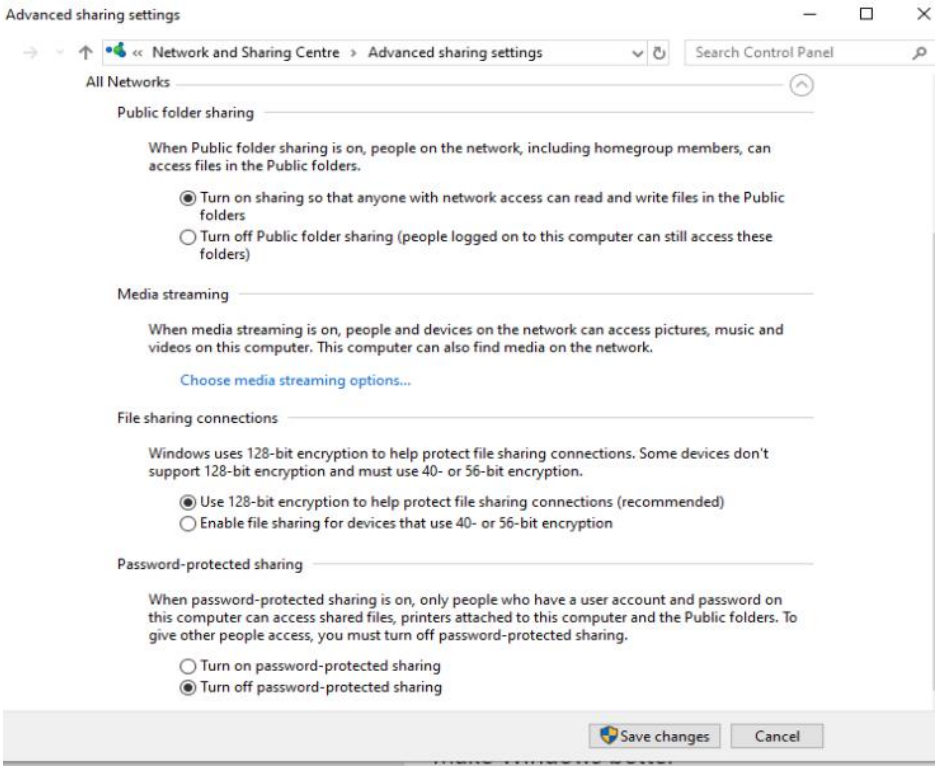
20. Kita juga akan ubah lokasi folder sharenya ke parent direktori. \\PC-WIN10\Soal
Caranya sama seperti pada folder Tugas. Klik Advance Sharing kemudian ceklist *Share this folder.*



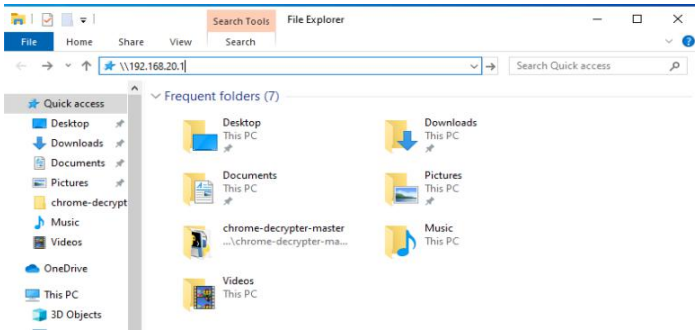
Pengujian

21. Untuk pengujian dari sisi client (PC-2), pastikan PC client berada dalam satu jaringan dengan server (PC-1).

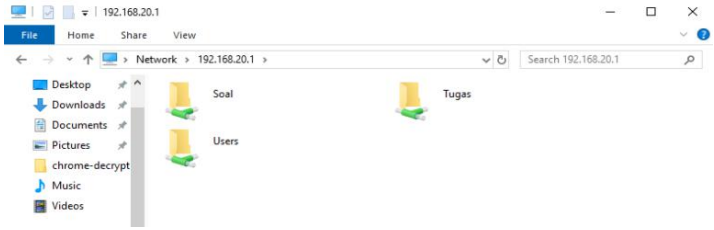
22. Untuk menguji folder "Soal", kita perlu menonaktifkan password di *Sharing options* pada server. Supaya saat pengguna client membuka layanan server tidak dimintai password.

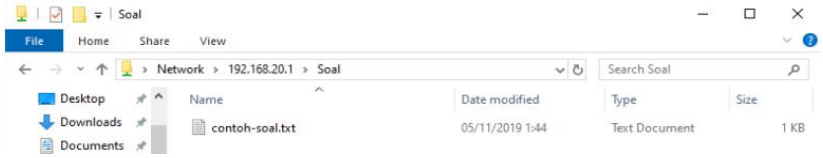


23. Langka pertama, kita buka Windows Explorer. Pada Address bar kita isi ip address server (PC-1) dengan diawali 2 blackslash, yaitu \\192.168.20.1 kemudian enter.



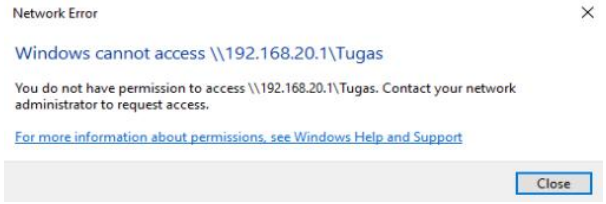
24. Jika konfigurasi sudah benar maka akan muncul daftar folder yang kita share seperti ini.





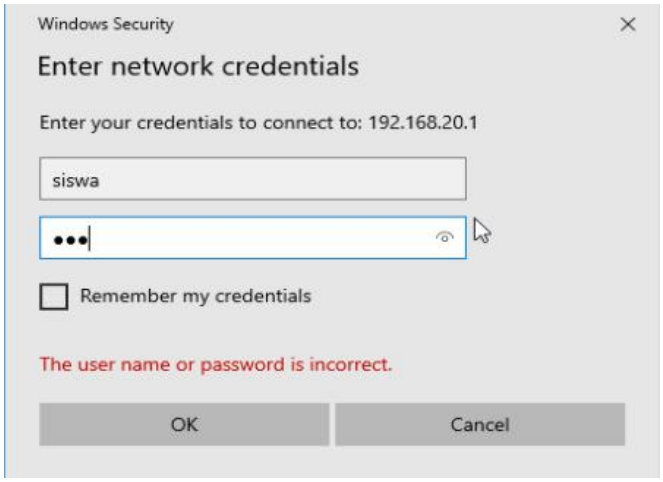
Kita bisa menguji apakah folder Soal bisa ditulis atau tidak dengan membuat folder atau file di dalamnya. Hasilnya harusnya seperti ini

Dan jika mengakses folder tugas tanpa login siswa, maka hasilnya begini:

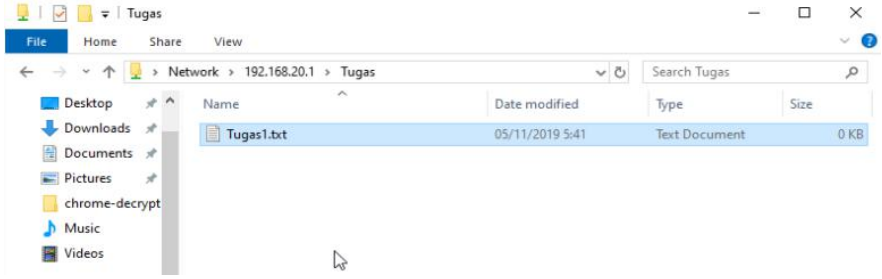


25. Sekarang kita akan menguji folder “Tugas”. Kita aktifkan lagi passwordnya melalui *Sharing options*.

26. Karena tadi kita sudah mengakses \\192.168.20.1 tanpa login, maka kita perlu relogin dari akun windows kita. Setelah relogin, coba buka \\192.168.20.1 di Windows Explorer. Harusnya muncul jendela yang berisi form login. Kita isi username: *siswa,* password: *123.*



27. Jika semua benar konfigurasinya maka harusnya kita bisa mengakses folder Tugas dan menulis file atau folder.



B. Sharing Printer

Layanan berikutnya yang sering digunakan adalah sharing printer atau perangkat tambahan lainnya. Langkah sharing printer di Windows 7 sangatlah mudah.

Berikut adalah konfigurasi di sisi server.
1. Konfigurasi firewall dan sharing options sama seperti sharing folder di atas. Untuk password sharingnya bisa diaktifkan atau dinonaktifkan sesuai kebutuhan.
2. Buka *Devices and Printer.*
3. Pilih printer yang akan dishare, lalu klik kanan.
4. Pilih *printer properties* lalu pilih tab *Sharing.*
5. Pada tab *Sharing,* kemudian klik *Share this printer.*

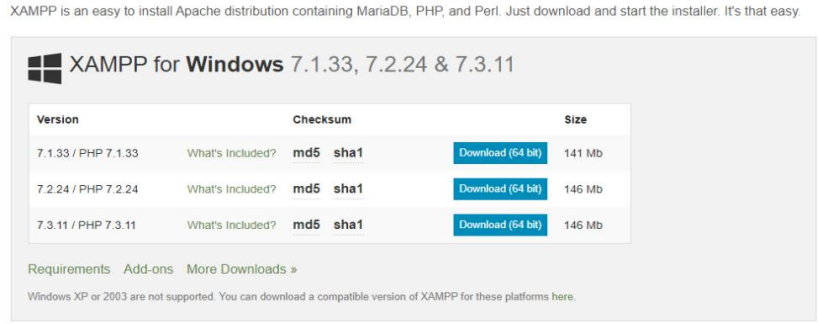
Pada sisi client.
1. Buka *Settings > Devices and Printer.*
2. Pilih *Add a printer.*
3. Pilih printer yang tadi di share. JIka tidak muncul kita bisa mencoba dengan cara memasukan alamat IP server di windows explorer
4. Lalu pilih *Add device.*

C. Menginstall Webserver

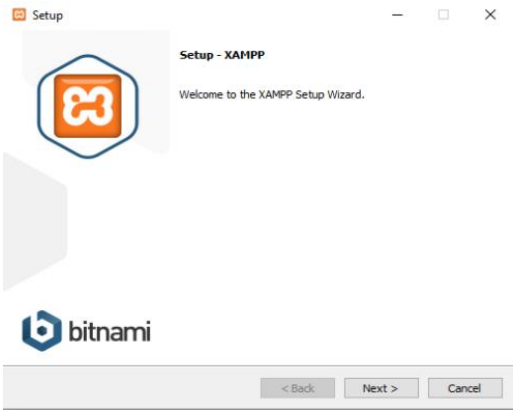
Aplikasi berbasis web adalah aplikasi yang fleksibel bisa diakses dari desktop maupun mobile. Karena itu dalam jaringan lokal, biasanya aplikasi yang digunakan rata-rata masih berbasis web. Nah untuk menjalankan aplikasi web kita perlu yang namanya web server dan database server.

Untuk windows non-server (Windows 10), ada satu aplikasi yang menyediakan web server dan database server sekaligus, namanya adalah XAMPP. Dengan aplikasi ini kita bisa menginstall web server apache sekaligus databasenya (mysql) tanpa konfigurasi yang rumit. Dan tentunya ini free software.

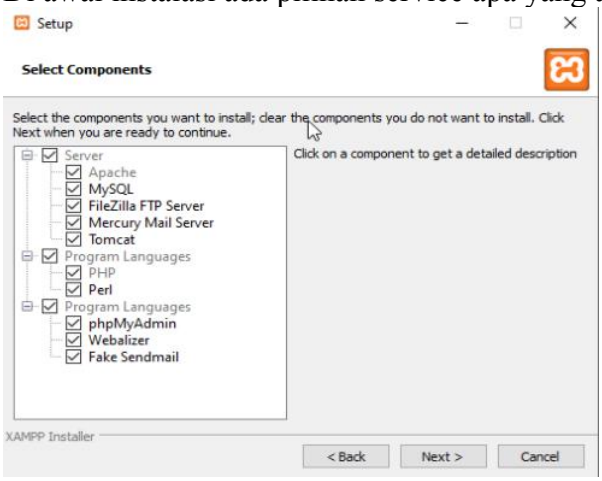
Untuk mendapatkannya, kita hanya perlu mendownload di situs resminya https://apachefriends.org/download.html atau ketik saja di search engine google "XAMPP".



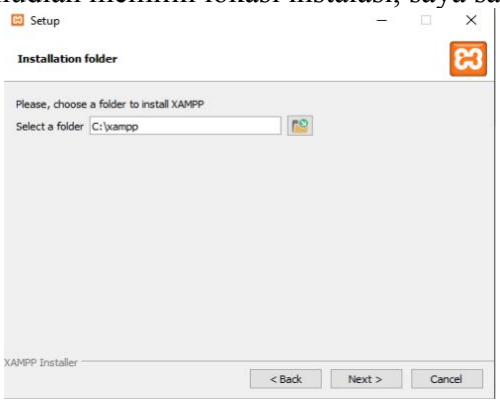
Instalasinya pun cukup mudah, hanya Next-next saja seperti aplikasi windows pada umumnya, paling hanya konfigurasi letak direktori untuk menginstall aplikasi tersebut.



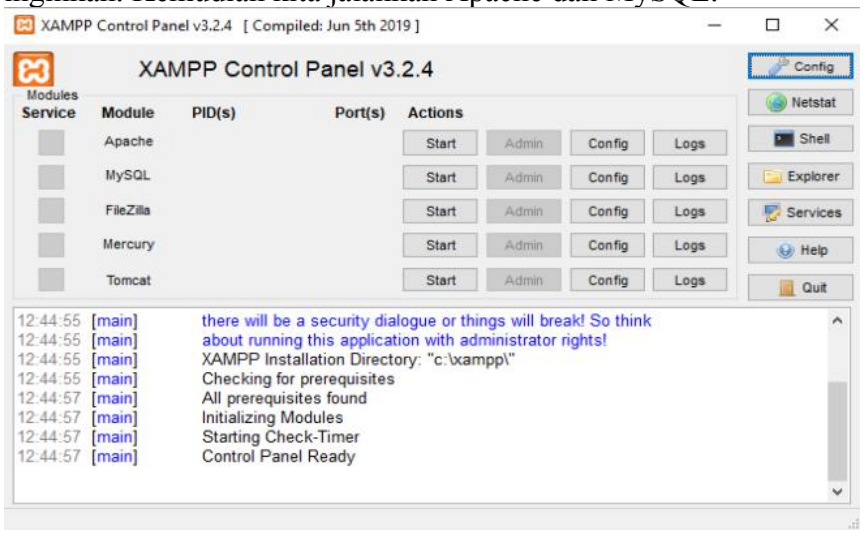
Di awal instalasi ada pilihan service apa yang akan kita install,



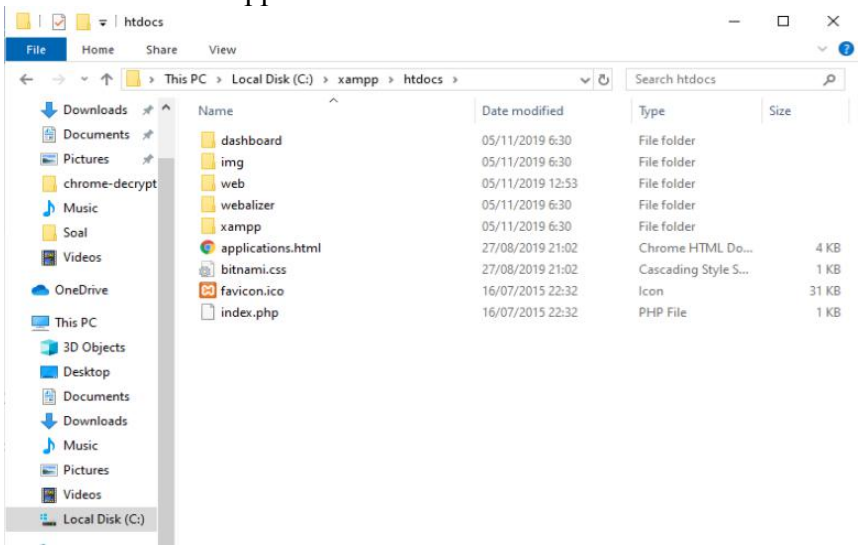
Kemudian memilih lokasi instalasi, saya sarankan jangan menginstall pada partisi sistem (C:\).



Jika sudah selesai, inilah tampilan control panelnya. Kita hanya tinggal menjalankan services yang kita inginkan. Kemudian kita jalankan Apache dan MySQL.

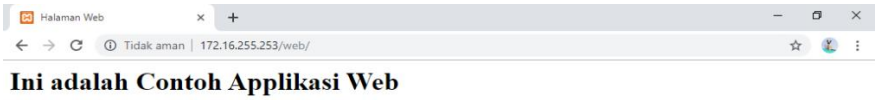


Karena kita mengkonfigurasi lokasi instalasinya di C:\xampp maka default lokasi resource aplikasi web kita ada di C:\xampp\htdocs.

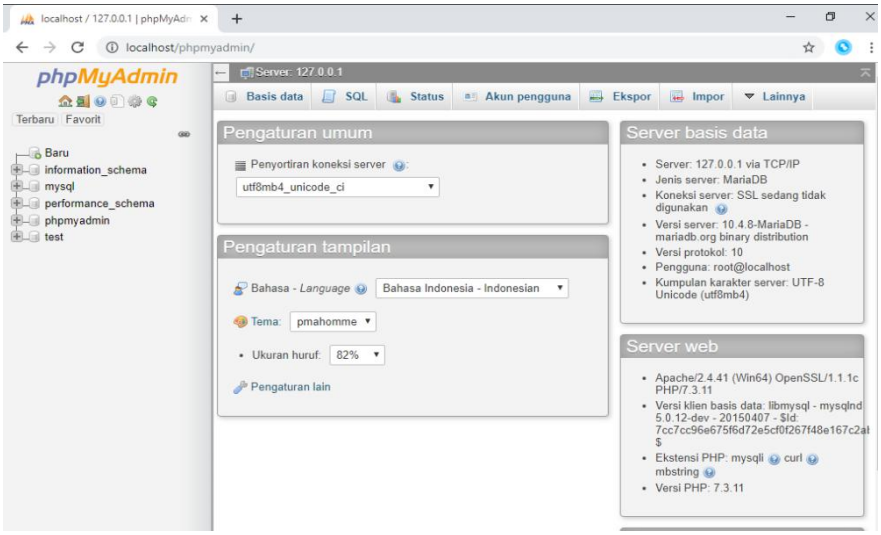


Contoh, kita akan membuat folder *web* pada htdocs. Kemdudian mengisinya dengan halaman html sederhana.

Kemudian kita coba akses dari sisi client. Untuk mengakses webnya dari sisi client, kita masukan IP server dan nama foldernya (contoh folder: web) pada web browser . Atau jika kita mengakses dari PC server tersebut cukup mengakses http://localhost/*namafolder*



Untuk databasenya kita bisa mengaksesnya dengan phpmyadmin, seperti gambar berikut:



Nah, itu dia cara install web server dan database server di Windows 10. Untuk pembuatan webnya tidak akan dibahas di sini. Teman-teman bisa mencari tutorial di internet.

BAB 3 - MIKROTIK

A. Apa itu Mikrotik?

MikroTik adalah vendor penyedia perangkat dan software jaringan komputer, katornya berpusat di kota Riga, Latvia. Perusahaan ini mulai dikembangkan sejak 1996 oleh John Trully dan Arnis Riekstins. Awalnya MikroTik ditujukan untuk penyedia jasa internet atau Internet Service Provider (ISP) yang melayani pelanggannya dengan teknologi nirkabel atau wireless. Akan tetapi saat ini mikrotik tidak hanya digunakan oleh ISP, tetapi juga digunakan untuk membangun jaringan lokal (LAN) di kantor, sekolah, ataupun rumah pribadi. Hal ini karena MikroTik memiliki fitur yang cukup lengkap tetapi harga yang relatif murah.

Produk hardware unggulan Mikrotik diantaranya Router, Access Point (Antena Wireless), Switch dan alat pendukung lainnya. Sementara software Mikrotik yang populer adalah Mikrotik RouterOS.

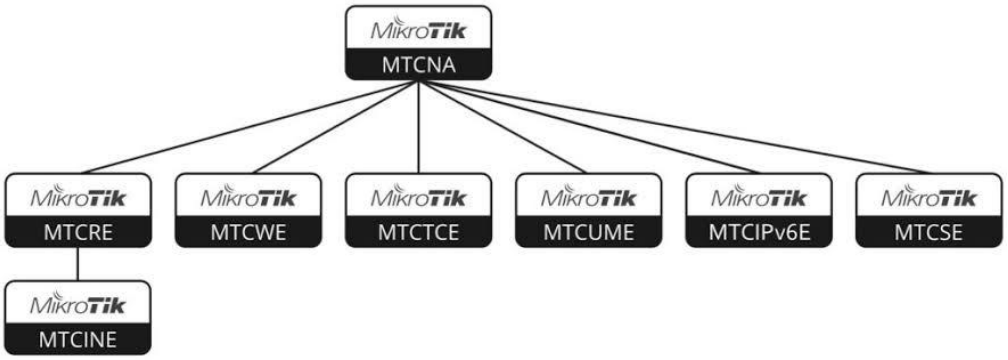
Mikrotik Router OS adalah sistem operasi yang tujuanya sebagai router. Mikrotik RouterOS bisa diinstal pada perangkat khusus yang disediakan Mikrotik yaitu Routerboard, bisa juga diinstall pada PC biasa.

Level Lisensi Mikrotik RouterOS

Level lisensi Mikrotik menentukan fitur-fitur yang didapatkan pada saat kita menggunakan perangkat Mikrotik. Level lisensi juga menentukan batasan upgrade packet. Lisensi melekat pada storage/media penyimpanan (contoh: Hardisk, NAND, USB, CD). Jadi apabila media penyimpanan diformat maka lisensi akan hilang.

Level number	0 (Trial mode)	1 (Free Demo)	3 (WISP CPE)	4 (WISP)	5 (WISP)	6 (Controller)
Price	no key	registration required	do not sell	$45	$95	$250
Initial Config Support	-	-	-	15 days	30 days	30 days
Wireless AP	24h trial	-	-	yes	yes	yes
Wireless Client and Bridge	24h trial	-	yes	yes	yes	yes
RIP, OSPF, BGP protocols	24h trial	-	yes(*)	yes	yes	yes
EoIP tunnels	24h trial	1	unlimited	unlimited	unlimited	unlimited
PPPoE tunnels	24h trial	1	200	200	500	unlimited
PPTP tunnels	24h trial	1	200	200	500	unlimited
L2TP tunnels	24h trial	1	200	200	500	unlimited
OVPN tunnels	24h trial	1	200	200	unlimited	unlimited
VLAN interfaces	24h trial	1	unlimited	unlimited	unlimited	unlimited
HotSpot active users	24h trial	1	1	200	500	unlimited
RADIUS client	24h trial	-	yes	yes	yes	yes
Queues	24h trial	1	unlimited	unlimited	unlimited	unlimited
Web proxy	24h trial	-	yes	yes	yes	yes
User manager active sessions	24h trial	1	10	20	50	Unlimited
Number of KVM guests	none	1	Unlimited	Unlimited	Unlimited	Unlimited

Sertifikasi Mikrotik:



MTCNA – MikroTik Certified Network Associate
MTCRE – MikroTik Certified Routing Engineer
MTCWE – MikroTik Certified Wireless Engineer
MTCTCE – MikroTik Certified Traffic Control Engineer
MTCUME – MikroTik Certified User Management Engineer
MTCIPv6E – MikroTik Certified IPv6 Engineer
MTCSE – MikroTik Certified Security Engineer
MTCINE – MikroTik Certified Inter-networking Engineer

Secara umum, serifikasi tersebut dibagi menjadi 3 level:
1. Level Basic: MTCNA
2. Level Advanced: MTCRE, MTCWE, MTCTCE, MTCUME, MTCIPv6E, MTCSE
3. Level Expert: MTCINE

B. Pre-config Mikrotik

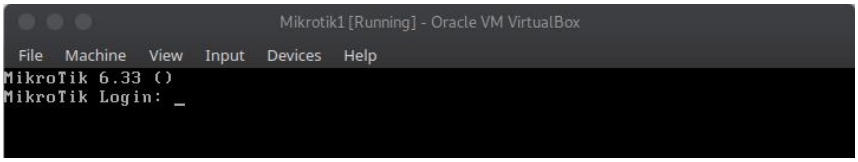
1. Mengakses Mikrotik

Ada beberapa cara untuk mengakses Router Mikrotik, bisa melalui Telnet, SSH, Winbox, FTP, API, dan Web. Masing-masing memiliki karakteristik yang berbeda.

Akses Via	Koneksi	Text Base	GUI	Need IP
Keyboard	Langsung di PC	yes		
Serial Console	Konektor Kabel Serial	yes		
Telnet & SSH	Layer 3	yes		yes
Winbox	Menggunakan OS Windows	yes	yes	
FTP	Layer 3	yes		yes
API	Socket Programing			yes
Web (HTTP)	Layer 3		yes	yes
MAC-Telnet	Layer 2	yes		

a. Keyboard

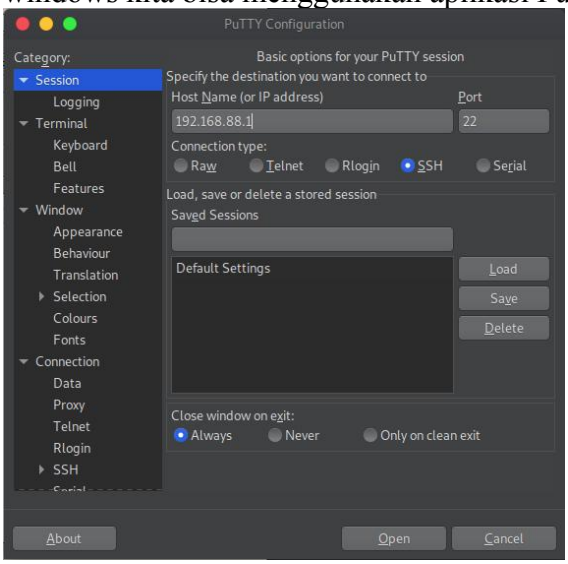
Akses ini maksudnya jika kita menginstall Mikrotik RouterOS pada virtual machine atau komputer fisik. Kita bisa mengaksesnya langsung seperti comand-prompt atau terminal.

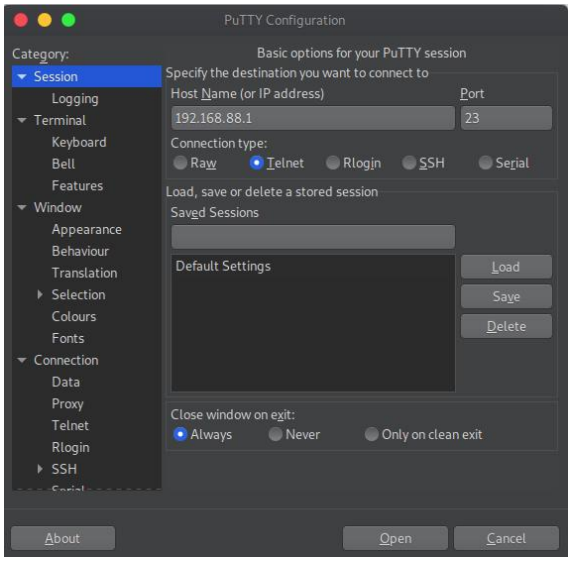


b. Serial console, kita mengakses melalui kabel serial (DB-9). Hasilnya sama, yaitu berbasi Command Line Interface (CLI) seperti gambar di atas.

c. Telnet dan SSH.

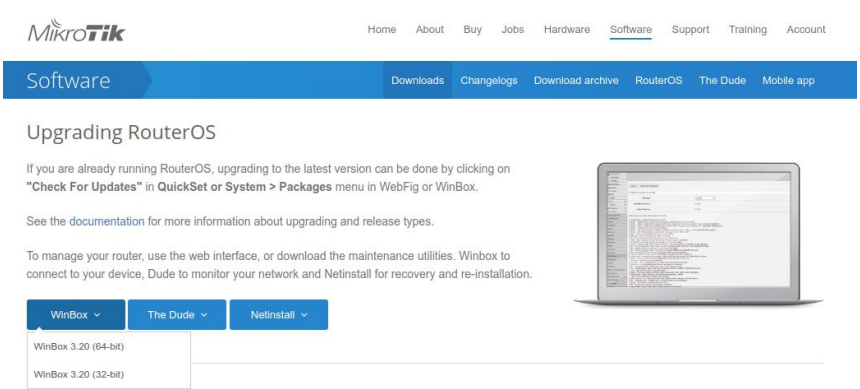
Masih menggunakan command line interface, hanya saja protokolnya kali ini menggunakan Telnet dan SSH. Keduanya (telnet dan ssh) bisa kita jalankan melalui terminal (linux), atau jika pada windows kita bisa menggunakan aplikasi Putty.

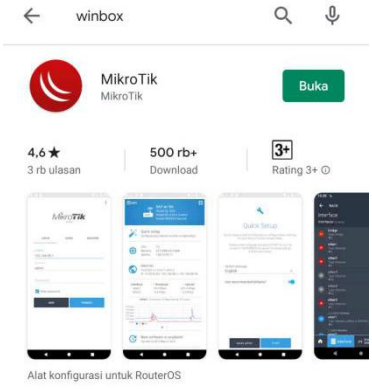




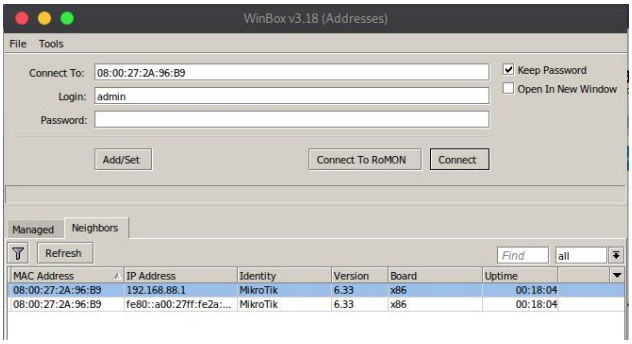
d. Winbox

Untuk aplikasinya bisa kita dapatkan melalui situs resmi mikrotik: https://mikrotik.com/download untuk versi desktop. Atau versi mobile bisa didownload di playstore, keyword: “winbox”.



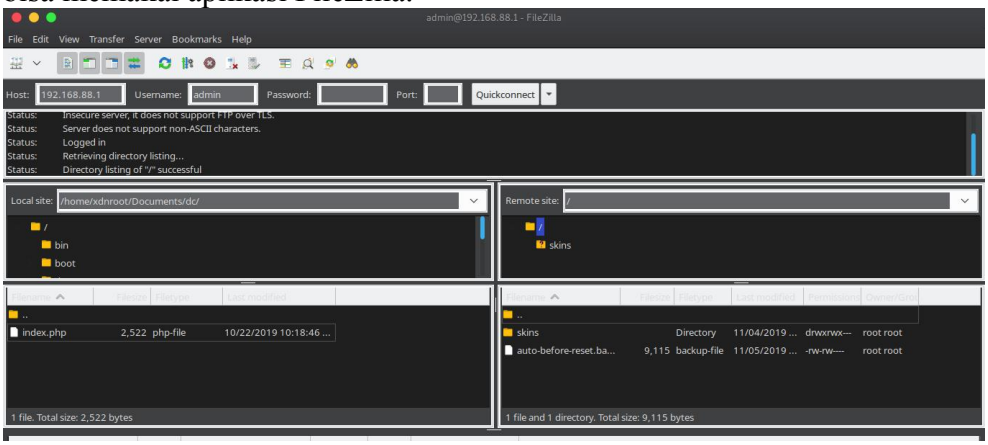


Pada winbox, kita bisa mengakses mikrotik menggunakan IP dan Mac Address.



e. FTP

Kita bisa menggunakan FTP untuk mengakses resource file mikrotik. Untuk menggunakan FTP kita bisa memakai aplikasi FileZilla.

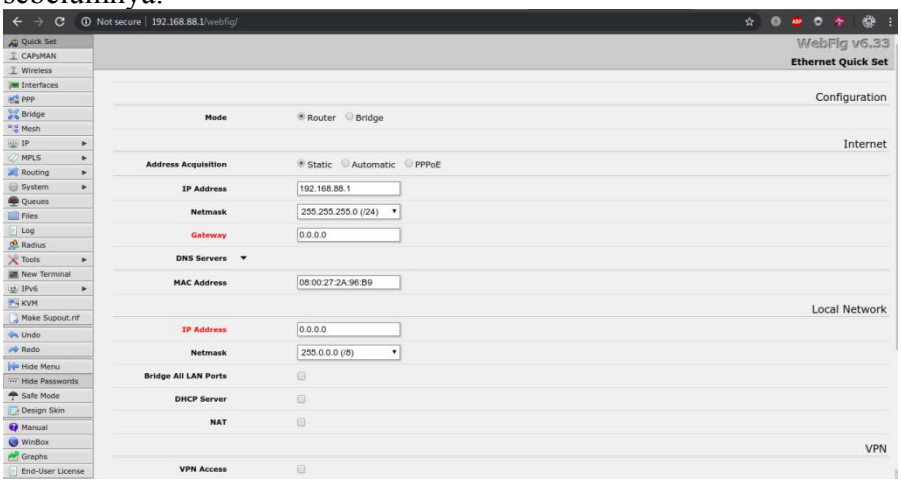


f. API

Application Programmable Interface (**API**) memungkinkan kita untuk membuat aplikasi kita terhubung dengan mikrotik. Untuk dokumentasi penggunaan API mikrotik, bisa dilihat di https://wiki.mikrotik.com/wiki/Manual:API

g. Webfig (HTTP)

Untuk mengakses web kita hanya perlu membuka IP mikrotik seperti pada materi web server sebelumnya.



h. Mac-telnet

Sama seperti telnet dan ssh, dia berbasis CLI tetapi hanya menggunakan layer 2 (mac address) tanpa perlu layer 3 (IP Address).

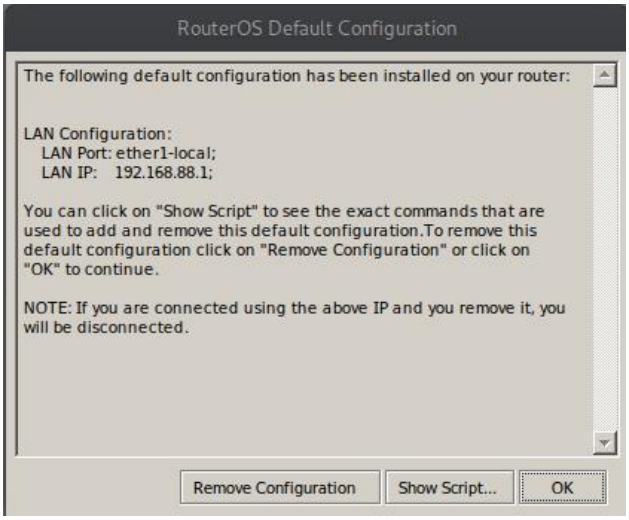
2. Default Configuration

Saat mengakses mikrotik baru atau setelah reset, ada default konfigurasi yang berjalan pada perangkat router mikrotik. Default konfigurasinya adalah semua interface mikrotik digabung menjadi interface bridge dan IP Addresnya **192.168.88.1/24**. Jadi jika ingin mengakses mikrotik baru melalui IP, kita perlu setting IP komputer kita dengan IP yang satu network dengan mikrotik. Default loginya adalah

Login: **admin**

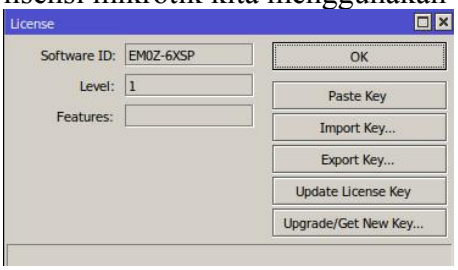
Passwod:

Saat mengakses melalui winbox, akan muncul jendela seperti ini, kita bisa menghapus konfigurasi default tersebut dengan mengklik *Remove Configuration.*

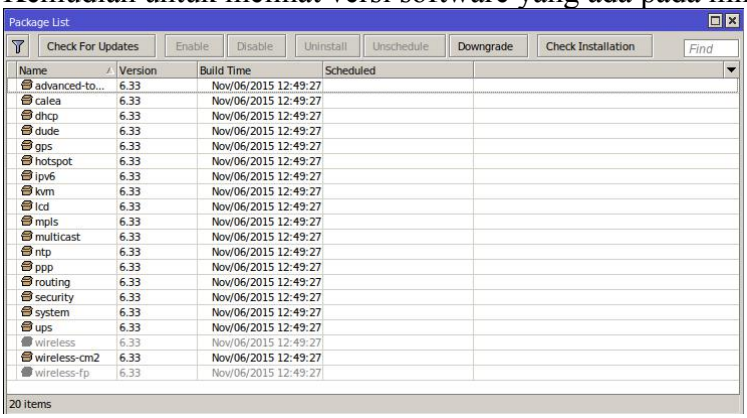


3. Lisensi dan Versi Mikrotik

Sebelumnya kita sudah membahasan tentang tingkatan lisensi mikrotik. Untuk mengecek berapa lisensi mikrotik kita menggunakan winbox. Buka *System > License.*



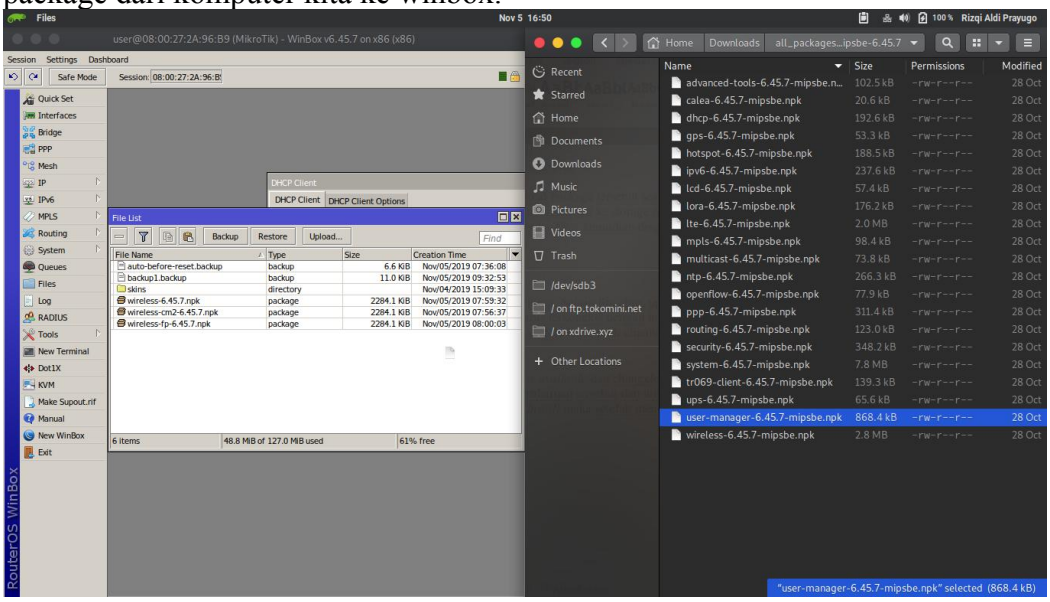
Kemudian untuk melihat versi software yang ada pada mikrotik kita, buka *System* > *Package.*



4. Install/Uninstall dan Enable/Disable Package

Untuk menonaktifkan package, pilih package yang akan dinonaktifkan kemudian klik *Disable* Sebaliknya untuk mengaktifkan tombol yang di klik adalah *Enable.* Untuk menguninstall pilih package yang akan diuninstall kemudian klik *Uninstall.*
Untuk menjalankan proses diatas kita harus mereboot mikrotik.

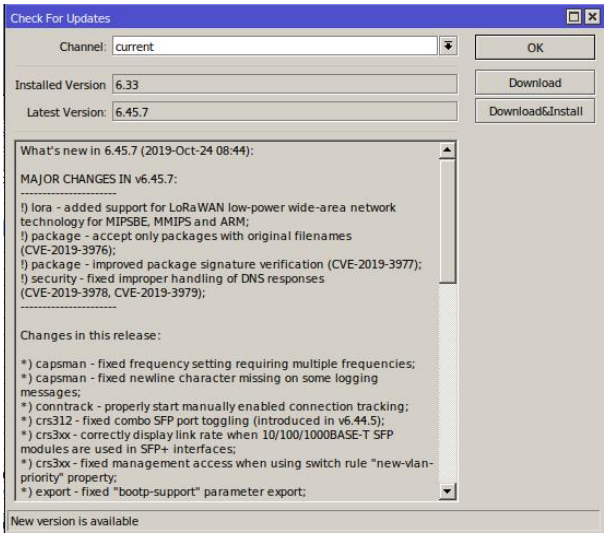
Untuk menginstall package baru, kita perlu mendownload package tersebut sesuai versi routerOS kita di: https://mikrotik.com/download. Kemudian mentransfernya ke storage mikrotik kita. Caranya bisa melalui FTP atau bisa juga dari winbox buka *Files* kemudian drag and drop file package dari komputer kita ke winbox.



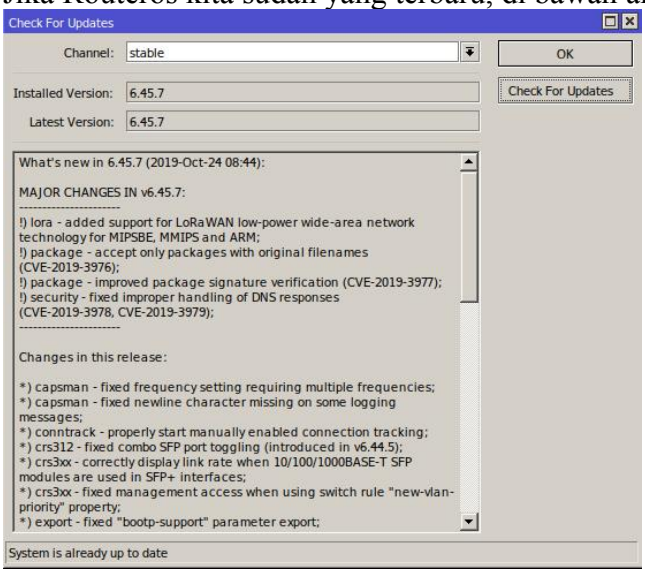
5. Upgrade/Downgrade Mikrotik

Menjaga softwate mikrotik agar tetap up to date itu penting. Selain fitu abru, update biasanya berisi patch keamanan baru juga. Untuk upgrade mikrotik harus terkoneksi dengan internet. Buka *System* > *Packages,* dan pilih *Check for updates.* Akan muncul jendela baru, pilih channel *current,* kemudian klik *Check for updates* lagi.

Jika ada versi yang terbaru akan muncul *New version is available* dan changelog-nya seperti ini. Jika kita pilih *Download* kita hanya akan mendownload pembaruan tersebut dan untuk menginstallnya kita harus rebbot manual. Jika memillih *Donwload & Install* maka setelah mendownload router akan otomatis reboot.



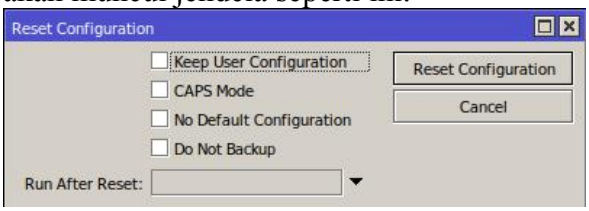
Jika Routeros kita sudah yang terbaru, di bawah akan muncul *System is already up to date*



6. Reset Konfigurasi

a. Soft Reset

Untuk mereset konfigurasi mikrotik melalui RouterOS, buka *System > Reset configuration.* Maka akan muncul jendela seperti ini.



Keep user = tidak menghapus user untuk login mikrotik.
CAPs mode = apabila mkrotik terkoneksi dengan CAPsMAN
No default = setelah reset tidak ada default konfigurasi.

b. Hard Reset

Hard reset adalah mereset mikrotik melalui tombol reset yang ada pada perangkat mikrotik.

Dengan hard reset mikrotik akan direset ke setelan pabrik (Dengan default configuration). Cara hard reset mikrotik:

1. Tekan dan tahan tobol reset dengan menggunakan pena atau lidi, karena tombol resetnya ada di dalam.
2. Sambil tetap menahan, cabut kabel power, kemudian colokan lagi.
3. Tunggu sampai LED ACT berkedip-kedip. Saat berkedip lepaskan tombol reset.
4. Tunggu sampai semua LED interface berkedip.

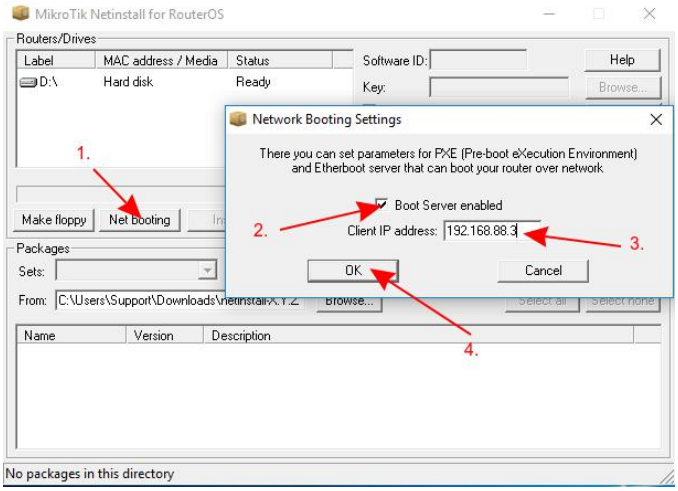
c. Install Ulang (NET Install)

Netinstall dilakukan jika cara reset di atas tidak mungkin dilakukan atau tidak berpengaruh. Caranya:

1. Download software netinstall dan main package software RouterOS di web resmi mikrotik: https://mikrotik.com/download

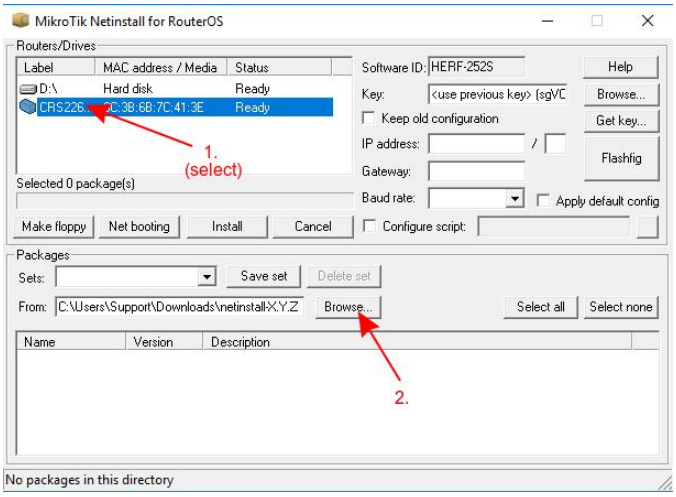
2. Ekstrack filenya, kemudian jalankan netinstall.exe

3. Konfigurasi *Net booting,* ceklist *Boot server enabled* dan isi Client IP dengan IP komputer yang kita gunakan untuk netinstall.

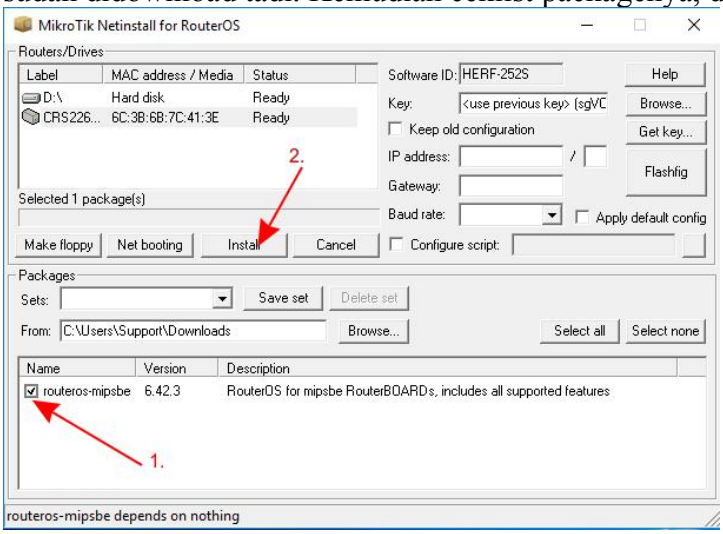


4. Hubungkan mikrotik ke PC dengan kabel ethernet.

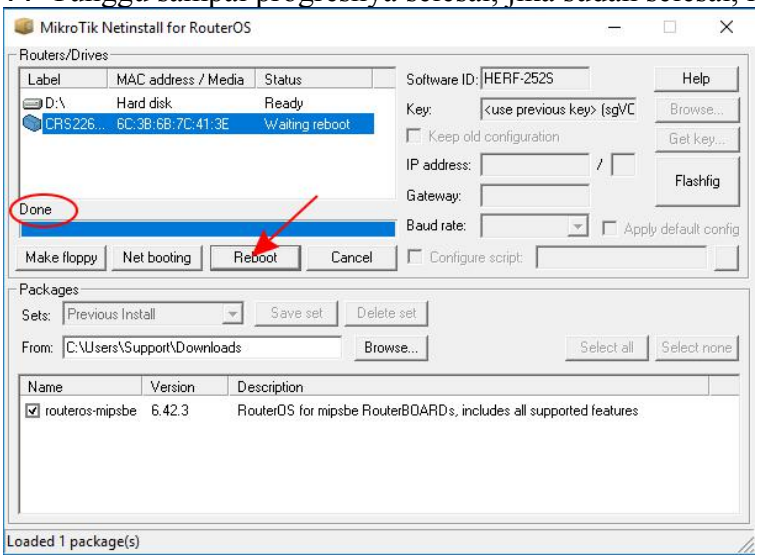
5. Tekan dan tahan tombol reset mikrotik, cabut kabel power kemudian sambungkan lagi seperti proses hard reset. Tunggu sapai mac address mikrotik muncul di aplikasi netinstall.



6. Kemdian pada bagian *package From,* browse ke main direktori main package RouterOS yang sudah didownload tadi. Kemudian ceklist packagenya, dan klik I*nstall*.



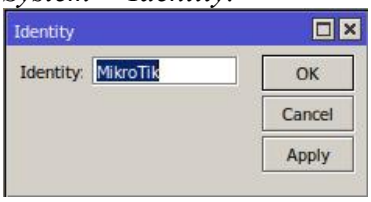
7. Tunggu sampai progresnya selesai, jika sudah selesai, reboot mikrotik.



C. Konfigurasi Mikrotik Dasar

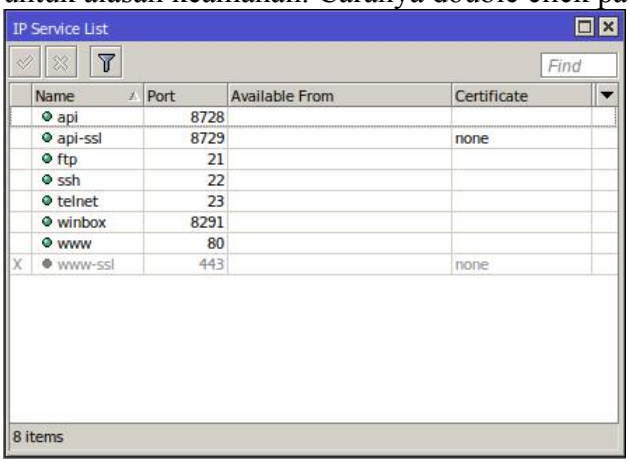
1. Identity

Identity bisa disebut sebgai hostname atau nama router kita. Untuk mengkonfigurasinya buka *System > Identity.*



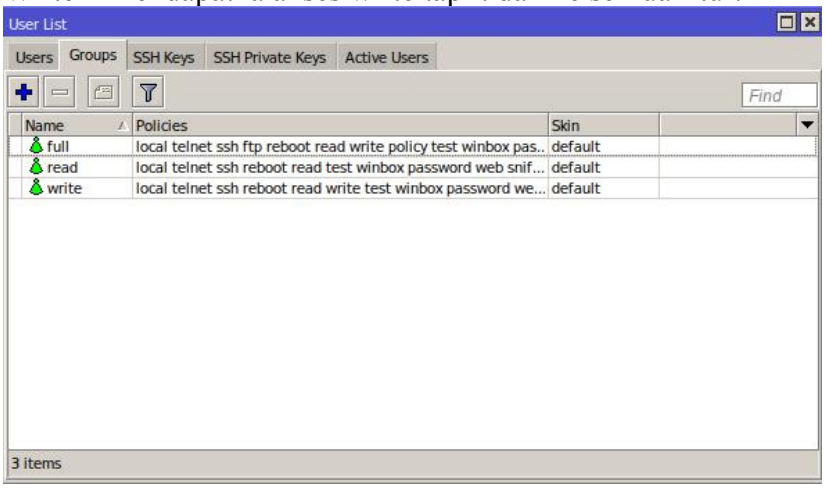
2. IP Services

Mikrotik mempunyai beberapa service yang digunakan untuk remote. Kita bisa mengkonfigurasi dari mana saja kita bisa mengkonfigurasi mikrotik. Untuk melihat daftar servicenya kita buka *IP > Services.* Di situ kita bisa menonaktifkan yang tidak perlu (caranya: pilih servicenya kemudian klik tanda x merah di pojok kiri atas). Atau merubah portnya dan membatasi IP yang bisa mengakses untuk alasan keamanan. Caranya double click pada paket.

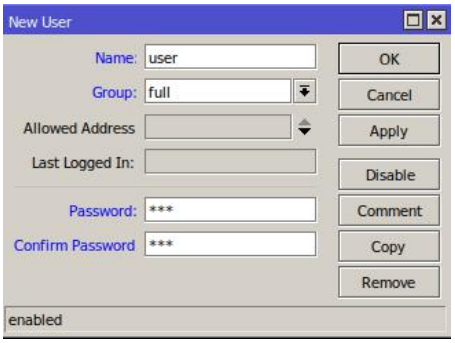


3. User Login Management

Setiap akan mengakses mikrotik kita perlua autetifikasi user, nah untuk mengaturnya ada di *System > Users.* Ada 3 group bawaan mikrotik, yaitu:
Full = mendapatkan akses write ke semua fitur
Read = hanya mendapatkan akses membaca.
Write = mendapatka akses write tapi tidak ke semua fitur.



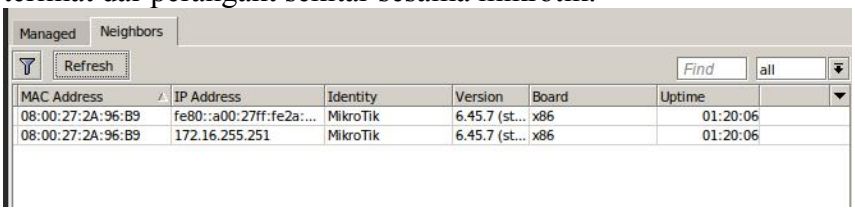
Untuk membuat user, pilih tab *Users,* klik tanda (+). Kemudian isi formnya.
Name = username
Group = grup tersebut berdasarkan keterangan sebelumnya (full, read, write)
Allowed Address = dari ip mana user diizinkan login
Password = paswword untuk login user tersebut.



Untuk melihat password pada winbox. Pada bagian atas winbox, klik *Setting,* uncheklist *Hide password.*

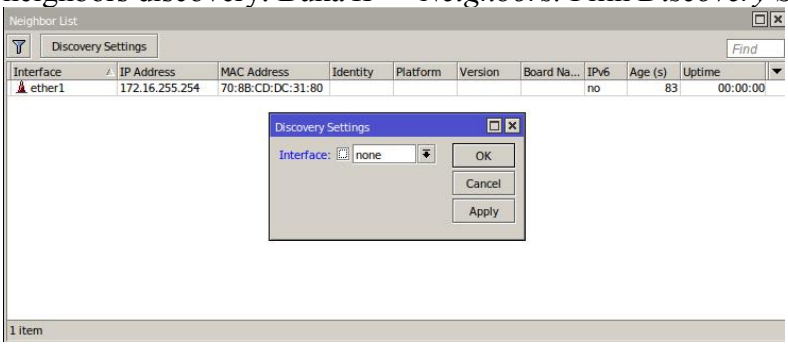
4. Mikrotik Neighbor Discovery Protocol (MNDP)

Dengan neighbor discovery, kita melihat perangkat mikrotik di sekitar kita Dan perangkat kita juga terlihat dar perangakt sekitar sesama mikrotik.



5. Block MNDP

Lalu bagaimana jika kita tidak ingin perangkat kita muncul di situ, caranya adalah menonaktifkan neighbors discovery. Buka *IP > Neighbors.* Pilih *Discovery Setting.*Pada form interface pilih *none.*



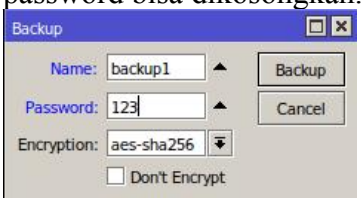
6. Backup dan Restore

Backup konfigurasi dilakukan jika kita ingin merubah konfigurasi mikrotik tapi takut salah, jadi jika error tidak ketemu solusinya kita bisa restore file backup tersebut. Ada 2 jenis backup yaitu:

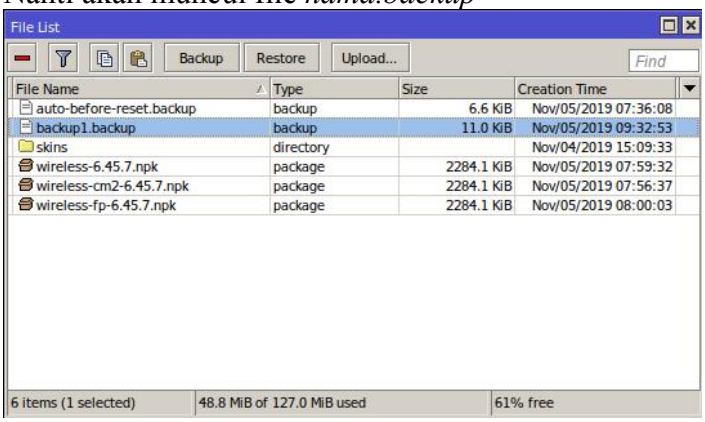
1. Binary file (.backup)
   - √ Tidak bisa dibuka dengan text editor.
   - √ Membackup keseluruhan konfigurasi router.
   - √ Create return point (akan mengembalikan ke semula sesuai data backup)

2. Script file (.rsc)
   - √ Berupa script, dapat dibaca dengan text editor.
   - √ Dapat membackup sebagian atau keseluruhan konfigurasi.
   - √ Tidak mengembalikan ke semula, melainkan menambahkan konfigurasi berdasarkan script hasil backup tersebut.

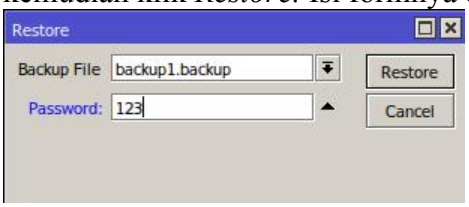
Untuk binary backup caranya, buka menu Files kemudian klik backup. Kemudian is formnya, password bisa dikosongkan.



Nanti akan muncul file *nama.backup*



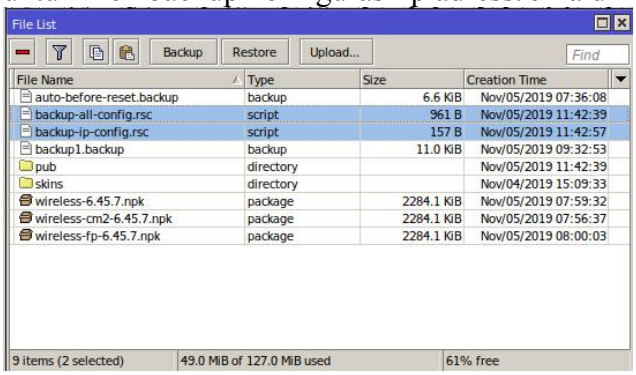
Untuk restore atau mengembalikan konfigurasi yang dibackup: klik pada file backup tersebut, kemudian klik *Restore.* Isi formnya dan klik *Restore.* Untuk restore router perlu melakukan reboot.



Untuk backup script, kita perlu menggunakan command line interface (CLI), dan menjalankan perintah:

```
[user@MikroTik] > export file=backup-all-config
[user@MikroTik] > /ip address export file=backup-ip-config
```

Perintah yang pertama adalah membackup semua konfigurasi, sedangkan perintah yang kedua hanya untuk membackup konfigurasi ip adress. Jika dilihat pada files, maka ada dua file hasil exporttadi.

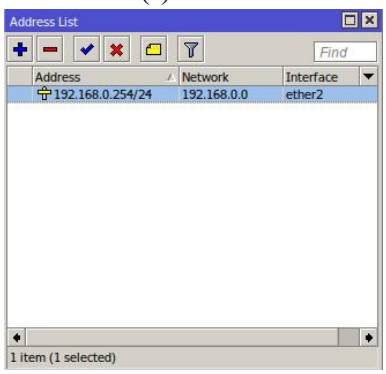


Untuk restore, perintahnya adalah

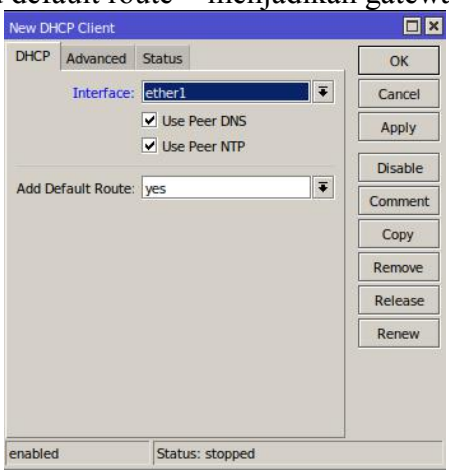
```
[user@MikroTik] > import backup-ip-config.rsc

Script file loaded and executed successfully
[user@MikroTik] >
```

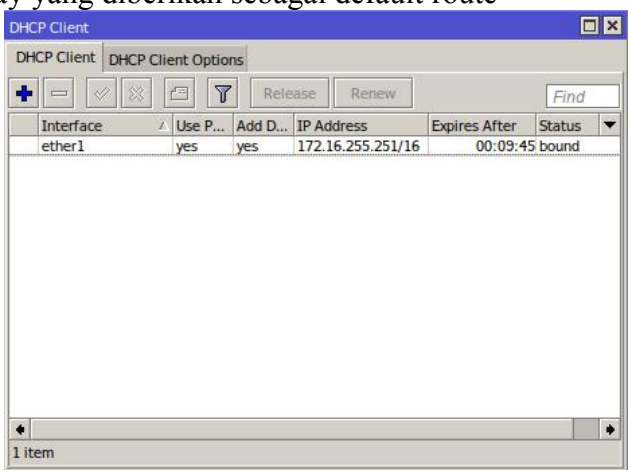
7. Konfigurasi IP statis dan Dinamis (DHCP Client)

Konfigurasi IP pada interface mikrotik bisa dilakukan secara static maupun dinamis, secara statis kita buka menu *IP > Addresses.* Lalu kita tambahkan IP pada interface tertentu dengan menekan tombol (+). Untuk menghapusnya kita gunakan tombol (-).

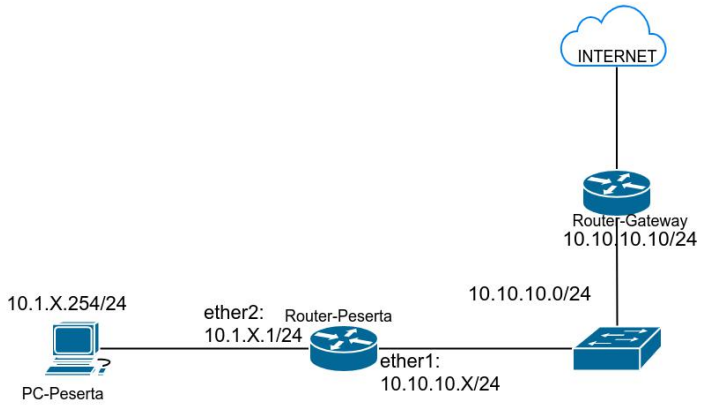


Untuk konfigurasi IP Dinamis, kita perlu server dhcp, dan mikrotik kita jadi clientnya. Caranya masuk ke *IP > DHCP Client.* Kemudian tambahkan dhcp client pada interface yang diinginkan.
Use peer DNS = konfigurasi ip dns dinamis dari dhcp server
User peer NTP = konfigurasi NTP dinamis dari dhcp server
Add default route = menjadikan gateway yang diberikan sebagai default route





8. Menggunakan Mikrotik sebagai Router pada Jaringan LAN



Kita akan membuat jaringan seperti di atas dan mengkonfigurasi mikrotik sebagai hotspot untuk perangkat mobile. Interface mikrotik yang mengarah ke ISP (ether1) dikonfigurasi secara dinamis, sedangkan yang mengarah ke PC (ether2) dikonfigurasi. Cara konfigurasi IP bisa dilihat dilihat di tutorial sebelumnya di atas.

Pastikan mikrotik kita sudah terkoneksi internet, pada winbox buka *New Terminal,* kita coba ping ke ip public baru kemudian ke domain public. Jika sudah kita perlu setting deafult gateway, dns server, dan NAT.

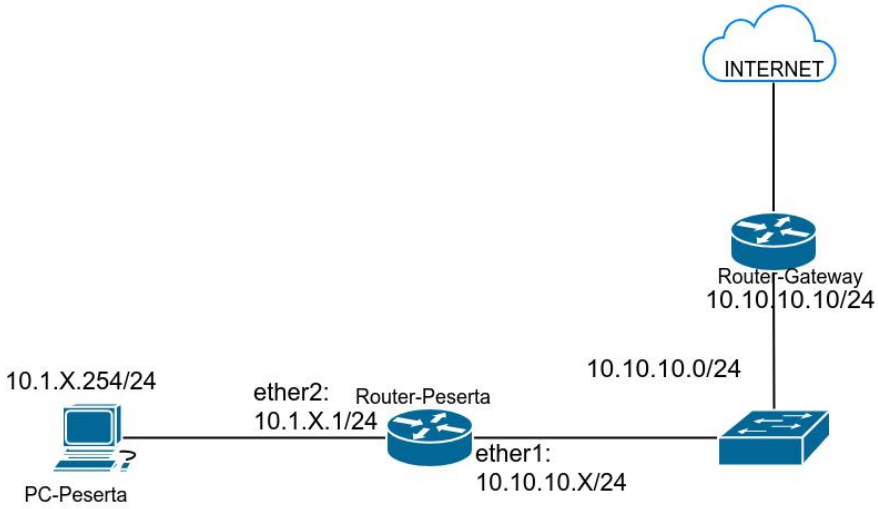
1. Konfigurasi default gateway
   ip route add ***dst-address****=0.0.0.0/0* ***gateway****=10.10.10.10*
   *) 10.10.10.10 = ip router yg menghubungkan ke internet.

2. Konfigurasi dns
   ip dns set ***servers****=8.8.8.8*
   *) 8.8.8.8 = ip dns server

3. Konfigurasi NAT
ip firewall nat add **chain**=srcnat **out-interface**=ether1 **action**=masquerade
   *) ether1 = interface yg mengarah ke public (internet),

Setting Gateway dan DNS
default gateway = 10.1.0.1
dns = 8.8.8.8
*) 10.1.0.1 = ip router yg menghubungkan ke internet.

SOAL MIKROTIK 1:



SOAL:

1. Buatlah sebuah jaringan menggunakan 1 PC sebagai PC-Peserta dan 1 router Mikrotik untuk Router-Peserta berdasarkan topologi di atas.

2. Konfigurasi IP Address **(X = nomor urut)**
   - Mikrotik
     ether1 = 10.10.10.X/24
     ether2 = 10.1.X.1/24
   - PC Client = 10.1.X.254/24

3. Buat user untuk mengakses mikrotik, dan hapus user bawaan mikrotik.
   - Full access user, login = **master**, password = **master123**
   - Read only access user, login = **pengunjung**, password = **123**

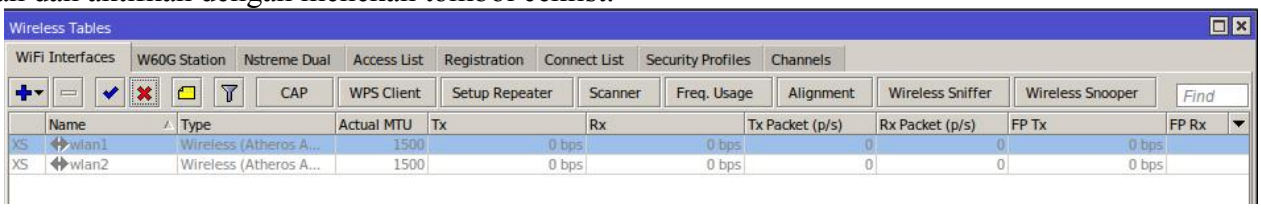
4. Matikan semua IP services kecuali winbox dan ftp.

5. Pastikan PC client bisa terhubung ke internet, dengan diuji ping ke google.com

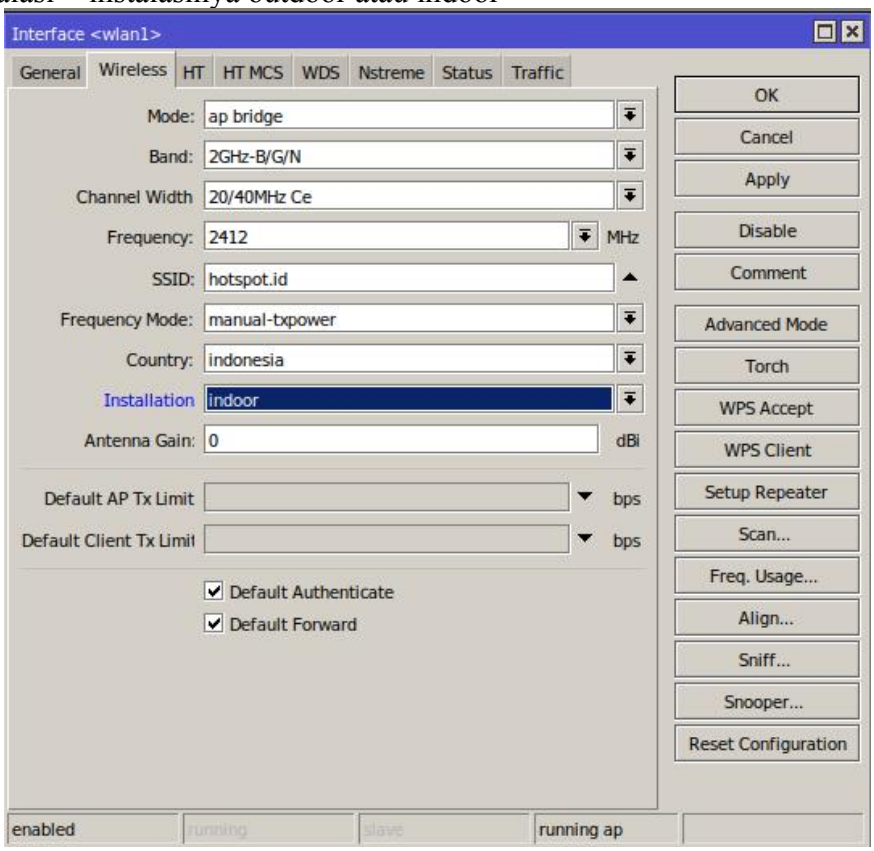
9. Konfigurasi Wireless

Salah satu produk yang sering digunakan adalah wireless yang emberikan layanan jaringan tanpa kabel. Meskipun tidak semua mikrotik terdapat wireless interfacenya. Nah, berkut ini adalah cara konfigurasi WiFi di interface wireless mikrotik.

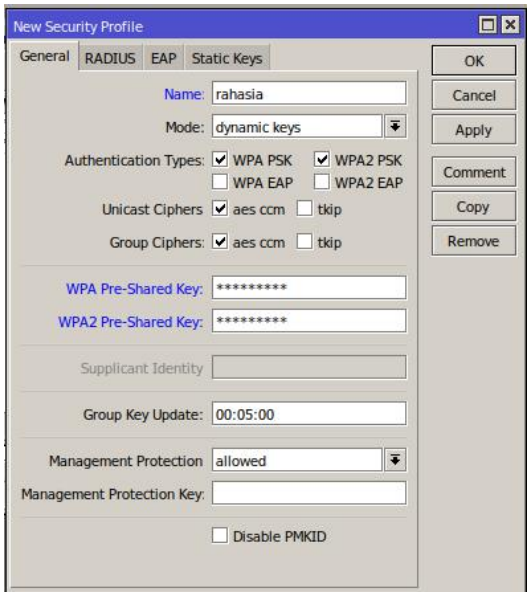
1. Buka menu *wireless*. Akan muncul interface wireless yang ada. Pilih Wifi interface yang akan digunakan dan aktifkan dengan menekan tombol ceklist.



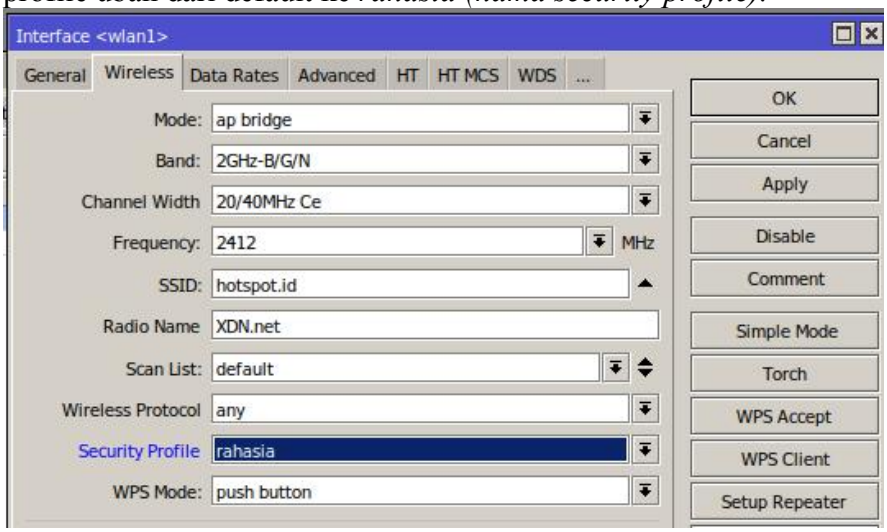
2. Klik interface wireless tersebut. Konfigurasi seperti berikut,
Mode = mode wireless (ap_bridge, station, station_bridge, dll)
Band = standar protokol yang digunakan
Channel width = lebar channel
Frequency = channel atau frekuensi central
SSID = nama wifi
Country = negara kita
Instalasi = instalasinya outdoor atau indoor



Jika ingin membuat kata sandi untuk hostpot:
1. Buat security profil. Buka *Wireless > Security profile.* Kemudian tambah baru. Password minimal berukuran 8 karakter.



2. Setting security profil pada wireless. Buka Wireless, pada Wifi Interface pilih interface yang wifinya akan diberi kata sandi. Akan muncul jendela baru, klik *Advance Mode.* Pada bagian security profile ubah dari default ke *rahasia (nama security profile).*



3. Sekarang kita akan dimintai password saat konek ke Wifi.

10. DHCP Server

Dynamic Host Configuration Protocol (DHCP) merupakan service yang memungkinkan perangkat dapat mendistribusikan/assign IP Address secara otomatis pada host dalam sebuah jaringan. Cara kerjanya, DHCP Server akan memberikan response terhadap request yang dikirimkan oleh DHCP Client.

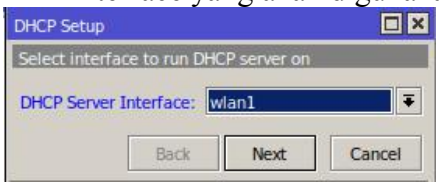
Selain IP Address, DHCP juga mampu mendistribusikan informasi netmask, Default gateway, Konfigurasi DNS dan NTP Server serta masih banyak lagi custom option (tergantung apakah DHCP client bisa support).

Mikrotik dapat digunakan sebagai DHCP Server maupun DHCP Client atau keduanya secara bersamaan.

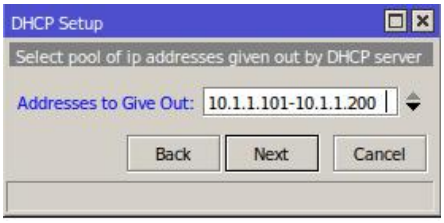
Cara konfigurasi DHCP Server.
Karena kita akan menjadikan DHCP server ini untuk wifi/ hotspot, yang kita setting adalah interface yang digunakan untuk membuat hostpot yaitu *wlan1*.

1. Konfigurasi terlebih dahulu IP wlan1 contoh kita akan menggunakan IP 10.1.1.1/24

2. Selanjutnya konfigurasi dhcp server. Buka *IP > DHCP Server.* Klik *DHCP-Setup.*
   a. Pilih interface yang akan digunakan untuk DHCP Server, yaitu *wlan1*.



   b. Berikutnya Address space, dhcp network, biarkan default. Untuk Addresses to give out adalah range ip yang digunakan untuk dialokasikan ke client. Di sini contohnya dari 10.1.1.101 - 10.1.1.200



   c. Konfigurasi juga DNS server dan leases time atau biarkan default, dan selesai.

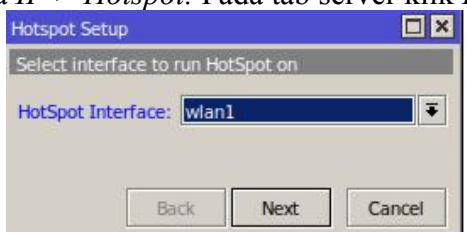
11. Hotspot Server

Router Mikrotik memiliki banyak fitur, salah satu fitur yang cukup populer dan banyak digunakan adalah Hotspot. Kita sering menemukan sinyal internet wifi yang di password. Jadi jika ingin mengakses wifi tersebut harus tahu password-nya terlebih dahulu. Namun berbeda dengan Hotspot, kebanyakan wifi hotspot tidak di password dan semua user bisa connect dan akan diarahkan ke halaman login di Web Browser. Tiap user bisa login dengan username dan password yang berbeda-beda. Metode semacam inilah yang sering kita temukan di Kampus, wifi Cafe, Sekolah, Kantor, maupun area publik lainnya.

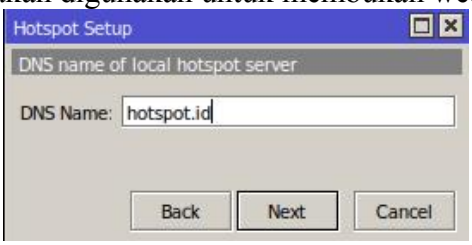
Sebenarnya hotspot tidak hanya bisa diaplikasikan untuk jaringan wireless saja, namun juga bisa untuk jaringan kabel. Kelebihan Hotspot adalah kita dapat mengkonfigurasi jaringan yang hanya bisa digunakan dengan username dan password tertentu. Kita juga dapat melakukan manajemen terhadap user-user tersebut. Misalnya, mengatur durasi total penggunaan hotspot per user, membatasi berapa besar data yang dapat di download tiap user, mengatur konten apa saja yang boleh diakses user, dll.

Konfigurasi Hotspot Server

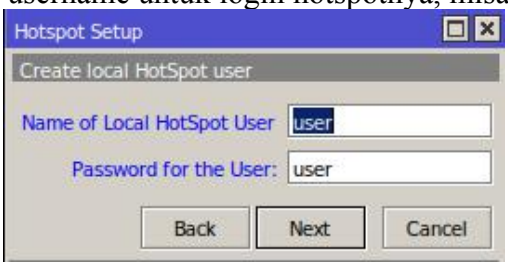
1. Buka *IP > Hotspot.* Pada tab server klik *Hotspot Setup*. Lalu pilih inteface yang akan digunakan.



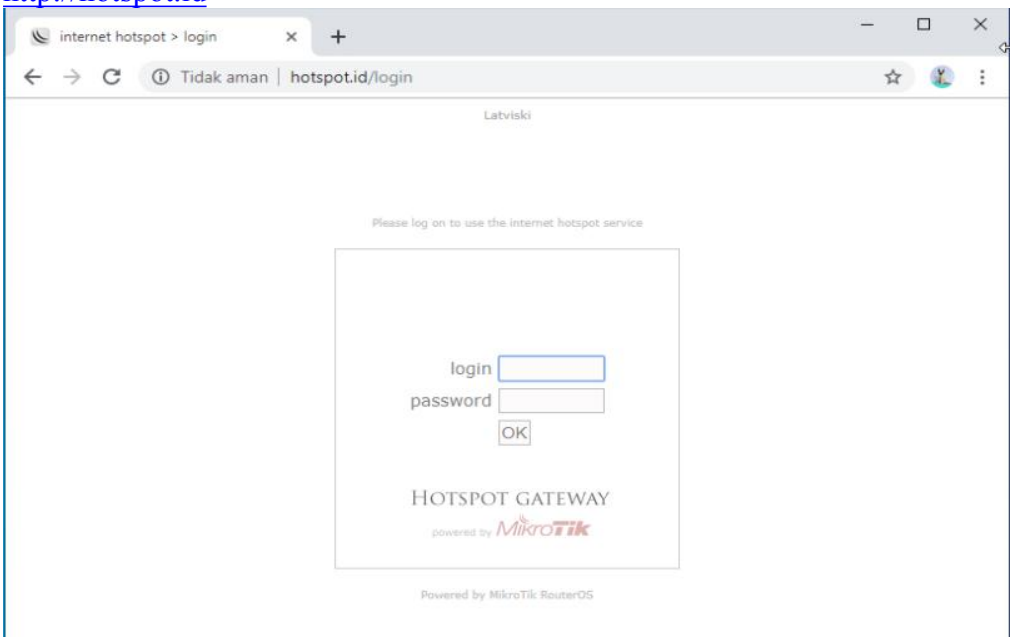
2. Local address of network sampai DNS server biarkan default. DNS name kita isi *hotspot.id* (domain ini akan digunakan untuk membukan weblogin hotspot kita).



3. Kita buat username untuk login hotspotnya, misal *user*, passwordnya *user. Dan selesai.*

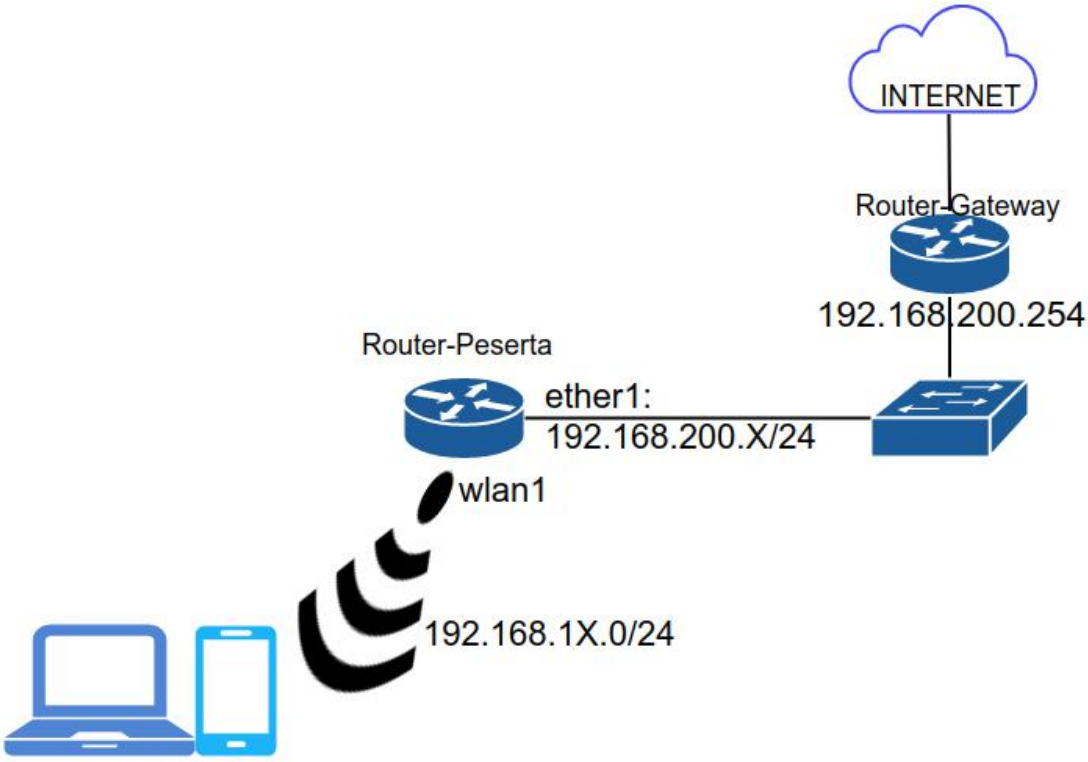


4. Selanjut coba koneksikan komputer/smartphone kita ke SSID wifi yang kita buat tadi, yaitu hotspot.id. Harusnya akan muncul halaman login. Jika tidak muncul kita perlu membukanya manual, http://hotspot.id



5. Kita coba login dengan user yang kita buat, barulah sekarang kita bisa mengakses internet.

SOAL MIKROTIK 2 :



6. Buatlah sebuah jaringan wifi menggunakan router Mikrotik (Router-Peserta) berdasarkan topologi di atas. Konfigurasi hostname/identity mikrotik **Router-X** (dengan X = nomor urut)

7. Buat user full access dengan login: **garuda,** password = **aman**, lalu hapus user bawaan.

8. Konfigurasi IP Address **(X = nomor urut)** pada Mikrotik
   ether1 = 192.168.200.X
   wlan1 = ip **terendah** dari network 192.168.1X.0/24

9. Buat DHCP Server untuk interface wlan1
   Range IP DHCP: 192.168.1X**.101-120**

10. Setting WLAN (wifi) di wlan1 dengan ketentuan **(X = nomor urut)**
    SSID: **WIFI-X**

11. Buat hotspot server untuk wlan1
    DNS Name = **wifi-X.net**
    Login: **siswa**, password= **siswa**

12. Supaya mempermudah konfigurasi,
    a. setting agar ketika user logout kemudian login kembali perlu memasukan data login lagi.
    b. Setting user bisa digunakan untuk login di 3 perangkat.

13. Pastikan Laptop/handphne client bisa terhubung ke internet, dengan diuji browsing ke google.com

CATATAN KONFIGURASI

1. Setting identity (identity berikut hanya contoh)
   system identity set ***identity****=Router-0*

2. Konfigurasi user login
   system users add ***name****=garuda* ***group****=full* ***password****=aman* ***confirm-password****=aman*

3. Konfigurasi IP (ip address berikut hanya contoh, sesuaikan dengan IP Address yang kamu gunakan)
   ip address add ***address****=192.168.200.254/24* ***interface****=ether1*
   ip address add ***address****=192.168.10.1/24* ***interface****=wlan1*

   Konfigurasi agar terhubung ke internet

   a. Default gateway
   ip route add ***dst-address****=0.0.0.0/0* ***gateway****=192.168.200.254*

   b. DNS
   ip dns set ***servers****=8.8.8.8*

   c. NAT
   ip firewall nat add ***chain****=srcnat* ***out-interface****=ether1* ***action****=masquerade*

4. Membuat DHCP Server interface wlan1 (ip address berikut hanya contoh)
   ip dhcp-server setup
   dhcp server interface: wlan1
   dhcp address space: 192.168.10.0/24
   gateway for dhcp network: 192.168.10.1
   address to give out: 192.168.1.101-192.168.1.120
   dns server: 8.8.8.8
   lease time: 10 menit

5. Konfigurasi wifi interface
   interface wireless set name=wlan1
   Mode = ap_brige
   Band = 2GHz-B/G/N
   Channel-width = 20 MHz
   SSID = WIFI-0
   Country = Indonesia
   Instalasion = indoor

6. Membuat Hotspot Server di wlan1
   ip hotspot setup interface = wlan1
   Local-address-of-network = 192.168.10.1/24
   Address-pool-of -network = 192.168.10.101-192.168.10.254/24
   Select-certificate = none
   SMTP-Server = 0.0.0.0
   DNS-Server = 8.8.8.8

DNS-Name = wifi-0.net
Hotspot-user = siswa, password=siswa

7. Konfigurasi user login

a. setting agar ketika user logout kemudian login kembali perlu memasukan data login lagi.
ip hotspot server-profiles set name=hsprof1
Pilih tab login, unceklist "Cookie"

b. Setting user bisa digunakan untuk login di 3 perangkat.
ip hotspot users-profiles set name=default
shared-users = 3

CARA LIMIT BANDWIDTH PER USER HOTSPOT MIKROTIK

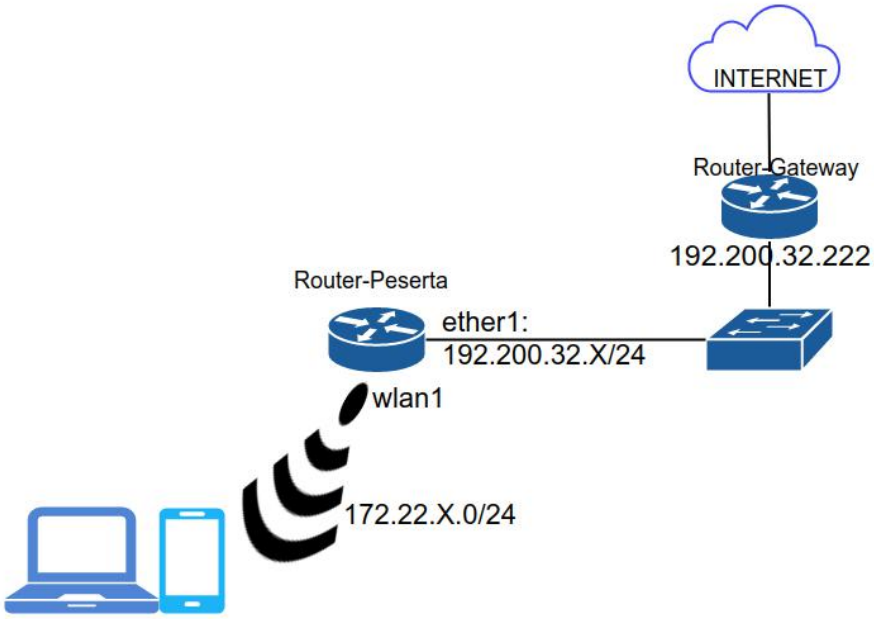
Contoh: Buat 2 user untuk ogin hotspot, yaitu: **guru** dan **siswa**. Kemudian setting limit bandwidth untuk user guru **upload: 1Mbps**, **download: 3Mbps.**

1. Kita harus membedakan user profil kedua user tersebut. Misal:
guru = **profile1** sedangkan **siswa** = **profile2**

tx = client's download atau router's upload = pengiriman data dari Router ke Client
rx = client's upload atau router's upload = pengiriman data dari Client ke Router

2. Kita setting user profile dari user yang akan dilimit (profile1).
isi **Rate limit (rx/tx)** dengan nilai limit yang diinginkan, contoh
Rate limit (rx/tx): 1M/3M

SOAL MIKROTIK 3 :



1. Konfigurasi hostname/identity mikrotik **RX** (dengan X = nomor urut)

2. Buat user full access dengan login: **garuda,** password = **sakti**, lalu hapus user bawaan.

3. Konfigurasi IP Address **(X = nomor urut)** pada Mikrotik
   ether1 = 192.200.32.X
   wlan1 = ip **tertinggi** dari network 172.22.X.0/24 (172.22.100.254)

4. Buat DHCP Server untuk interface wlan1
   Range IP DHCP (DHCP Pool): 172.22.X**.1-8**

5. Setting WLAN (wifi) di wlan1 dengan ketentuan **(X = nomor urut)** dan buat hotspot servernya juga dengan ketentuan:
   SSID: **GARUDA-X**
   DNS Name = **garuda-X.id**

6. Buat 2 user untuk login hotspot dengan ketentuan sebagai berikut.
   1. Login: **presiden**, password = **123**
   2. Login: **rakyat**, password = **321**

7. Setting limit bandwidth untuk user **presiden** dengan batas download: **1M** dan upload: **512K**.

8. Supaya mempermudah pengujian,
   a. Setting agar ketika user logout kemudian login kembali perlu memasukan data login lagi.
   b. Setting agar 1 akun user bisa digunakan untuk login di 5 perangkat.

9. Bypass situs **http://bsnp-indonesia.org**, sehingga user tidak perlu login untuk mengaksesnya.

10. Pastikan Laptop/handphne client bisa terhubung ke internet, dengan diuji browsing ke google.com

Mengubah tampilan login.

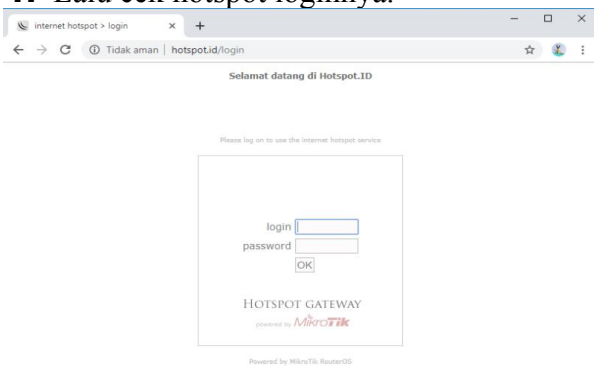
1. Jika kita hanya ingin mengedit kita harus menyalin folder hotspot pada files mikrotik ke komputer kita. Caranya bisa menggunakan drag and drop atau menggunakan FTP.

2. Misalnya kita ingin mengubah tulisan Latviski menjadi “Selamat datang di Hotspot.ID”, kita edit file login.html. Cari tulisan Latviski dan ganti.

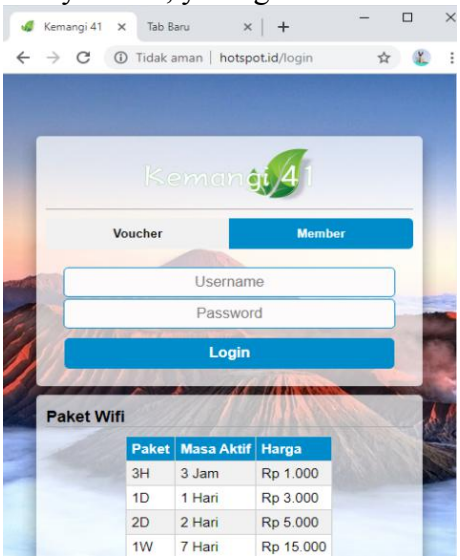
```
                document.login.password.value + '
            $(chap-challenge)');
        document.sendin.submit();
        return false;
        }
    //-->
    </script>
$(endif)

<div align="center">
<a href="$(link-login-only)?target=lv&amp;dst=$(link-orig-esc)
">Latviski</a>
</div>

<table width="100%" style="margin-top: 10%;">
    <tr>
    <td align="center" valign="middle">
        <div class="notice" style="color: #c1c1c1; font-size:
            9px">Please log on to use the internet hotspot
        service<br />$(if trial == 'yes')Free trial
        available, <a style="color: #FF8080"href="
        $(link-login-only)?dst=$(link-orig-esc)&amp;
        username=T-$(mac-esc)">click here</a>.$(endif)</div><
        br />
        <table width="280" height="280" style="border: 1px
            solid #cccccc; padding: 0px;" cellpadding="0"
        cellspacing="0">
```

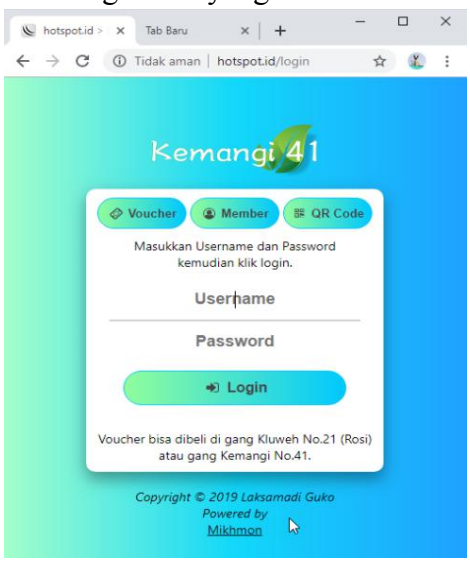
```
                document.login.password.value + '
            $(chap-challenge)');
        document.sendin.submit();
        return false;
        }
    //-->
    </script>
$(endif)

<div align="center">
<h3>Selamat datang di Hotspot.ID</h3>
</div>

<table width="100%" style="margin-top: 10%;">
    <tr>
    <td align="center" valign="middle">
        <div class="notice" style="color: #c1c1c1; font-size:
            9px">Please log on to use the internet hotspot
        service<br />$(if trial == 'yes')Free trial
        available, <a style="color: #FF8080"href="
        $(link-login-only)?dst=$(link-orig-esc)&amp;
        username=T-$(mac-esc)">click here</a>.$(endif)</div><
        br />
        <table width="280" height="280" style="border: 1px
            solid #cccccc; padding: 0px;" cellpadding="0"
        cellspacing="0">
            <tr>
```

3. Kemudian kita upload lagi ke mikrotik.
4. Lalu cek hotspot loginnya.



Jika ingin mengganti keseluruhan tampilannya, bisa download template gratis di internet. Carannya intinya sama, yaitu ganti file di mikrotik dengan file yang baru.





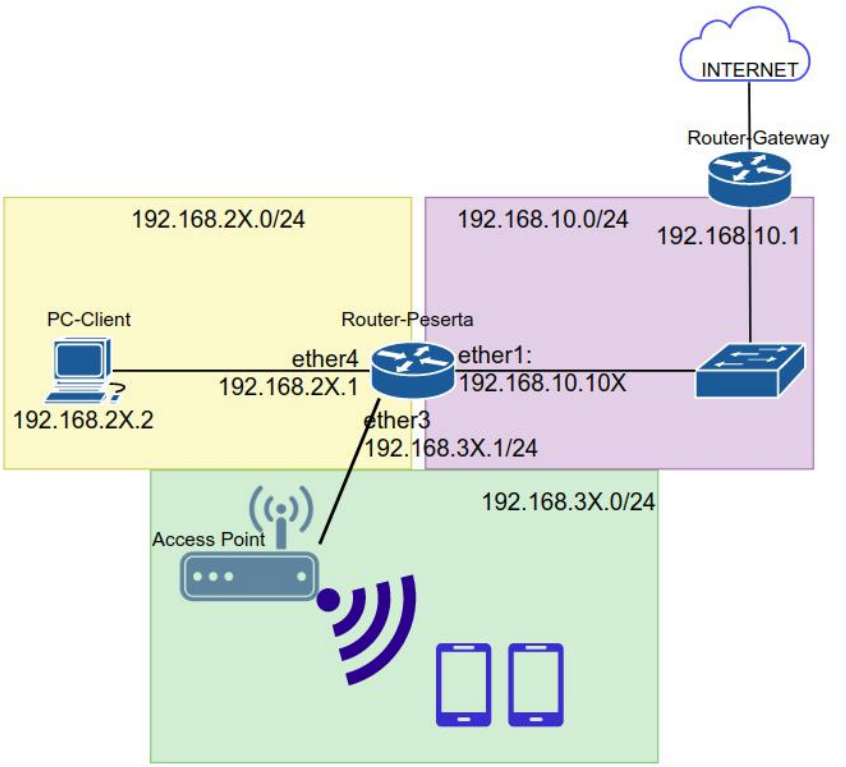
KONFIGURASI ACCESS POINT TAMBAHAN MIKROTIK

Konfigurasi Mikrotik:

1. Pastikan client bisa terkoneksi internet (setting ip route, dns, dan nat)
2. Konfigurasi IP ether3 sesuai topologi (contoh: 192.168.30.1/24)
3. Konfigurasi DHCP Server untuk ether3.
4. Konfigurasi Hotspot Server untuk ether3.

Konfigurasi Access Point:

1. Mulai konfigurasi setelah reset access point
2. Operation mode: access point
3. Wireless setting: setting SSID dan password wifi.
4. Reboot



Walled Garden Mikrotik

Walled Garden adalah fitur hotspot yang berfungsi untuk bypass akses ke sebuah host.
Bypass = melakukan sesuatu tanpa autentifikasi.
Jadi misal kita membuat hotspot server di mikrotik, pada defaultnya client tidak bisa akses internet sebelum melakukan autentifikasi (login) ke hotspot mikrotik.

Dengan walled garden ini kita bisa mengizinkan client untuk mengakses host tertentu tanpa login.
Misal yang kita bypass adalah situs linux.or.id
Maka client bisa mengakses linux.or.id tanpa perlu login hotspot.

Konfigurasi walled garden:
*ip hotspot walled-garden add **action**=allow **server**=hotspot1 **dst-host**=linux.or.id*

hotspot1 adalah nama hotspot server yang digunakan
linux.or.id adalah domain situs yang ingin bypass aksesnya

Jika yang mau kita bypass adalah berdasarkan IP pengirim dan IP tujuan, kita bisa mengisikannya di src-address dan dst-address.

Firewall sendiri adalah sistem keamanan untuk mengelola dan memantau trafik masuk dan keluar berdasarkan aturan keamanan (security rules) yang sudah ditentukan. Firewall berfungsi mencegah akses yang tidak diinginkan dari atau ke dalam jaringan atau server.

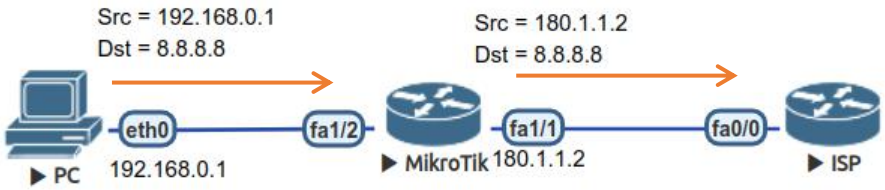
12. Network Address Translation (NAT)

Network Address Translation (NAT) adalah salah satu fungsi firewall yang bertugas melakukan perubahan (mentranslasikan) suatu IP Address ke IP Address lain, atau dari suatu port ke port lain.

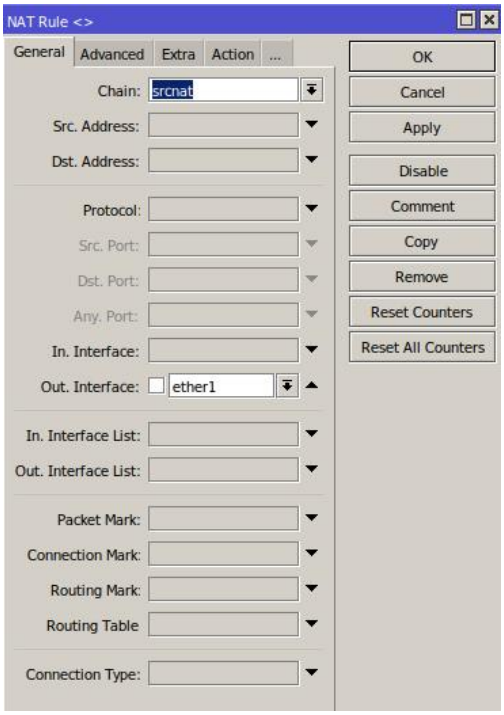
a. srcnat

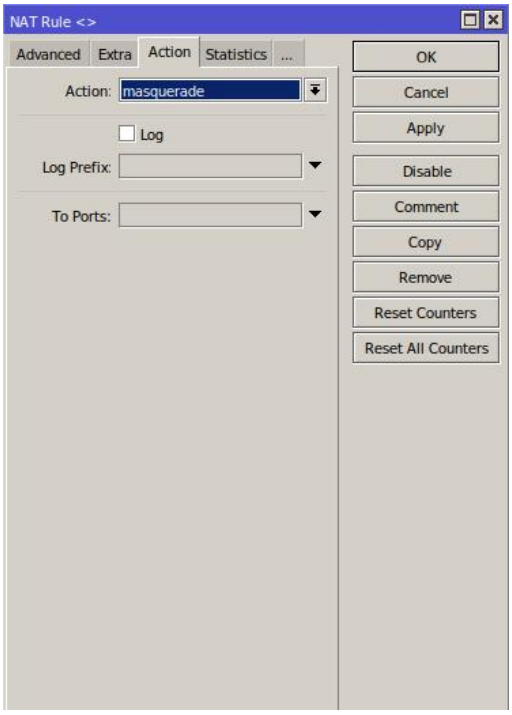
srcnat difungsikan untuk mengubah source address (IP pengirim) menjadi ip lain. Ilustrasinya seperti ini: A ingin "mengirim barang kepada C melalui perantara B. B melakukan srcnat dengan mengubah sumber pengirim, saat memberikan barang kepada C, B mengatakan “ini dari saya” atau bisa juga “ini dari si D” padahala yang mengirim adalah si A.

Sedangkan dalam jaringan komputer penerapnya mirip seperi ilustrasi di atas. Alamat IP pengirim ditranslasikan ke IP lain baik untuk alasan keamanan ataupun karena memang diperlukan. Misalnya saat ingin terkoneksi internet, internet menggunakan ip public, sedangkan jaringan lokal menggunakan ip private, maka perlu ditranslasikan agar bisa berkomunikasi dengan jaringan internet.



Pada mikrotık translası IP srcnat sepertı dı atas umumnya dıgunakan untuk menghubungkan client lokal ke internet. Caranya, buka *IP > Firewall*. Pada tab *NAT* tambahkan rule:
*ip firewall nat add chain=**srcnat** out-interface=**ether1** action=masquerade*

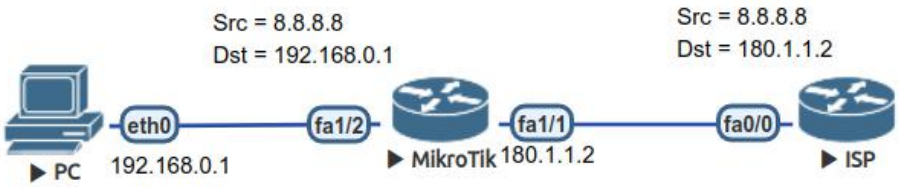




Kita bisa menspesifikasikan srcnat untuk interface tertentu saja dengan menambahkannya pada bagian *in-interface*. Bisa juga untuk jaringan atau ip tertentu, bisa ditambahkan pada *src-address*.

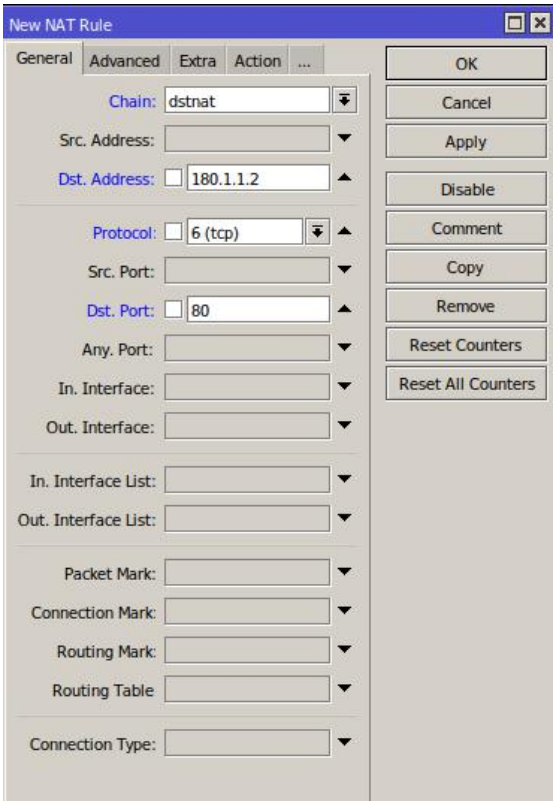
b. dstnat

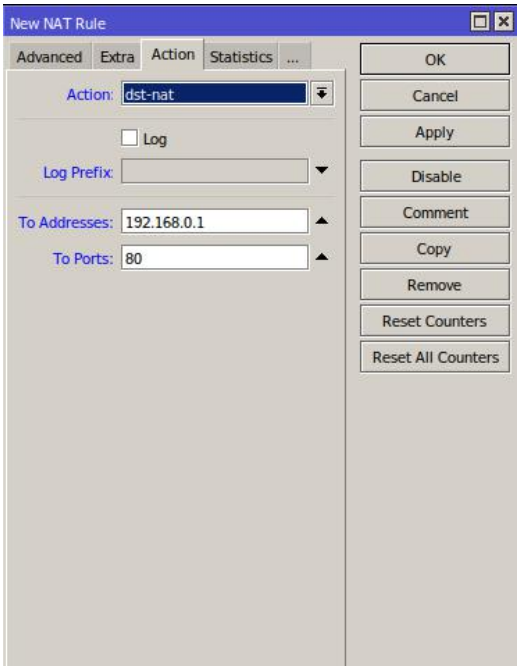
Dstnat digunakan untuk mentranslasikan destination address (IP tujuan), kebalikan dari srctnat. Biasanya digunakan agar perangkat yang tidak ip public bisa diakses dari internet. Atau hanya sekedar ingin memanipulasi IP address.



Dstnat akan digunakan saat kita mengkonfigurasi proxy, ataupun jika kita ingin meredirect traffic yang menuju router ke perangkat lain. Contohnya kita akan redirect traffic HTTP yang menuju router agar redirect ke PC-1

Cara konfigurasinya:
Buka *IP > Firewall*. Pada tab *NAT* tambahkan rule:
*ip firewall nat add chain=**dstnat** dst-address=**180.1.1.2** protocol=**tcp** dst-port=**80** action=**dst-nat** to-address=**192.168.0.1** to-ports=**80***





(sesuaikan alamat ip-nya dengan topologi kalian)

Sekarang jika mengakses http://180.1.1.2 maka yang tampil adalah web server dari PC-1

13. Firewall Filter

Salah satu fitur mikrotik yang sering digunakan adalah firewall filter. **Firewall** sendiri adalah sistem keamanan untuk mengelola dan memantau trafik masuk dan keluar berdasarkan aturan keamanan (security rules) yang sudah ditentukan. Firewall berfungsi mencegah akses yang tidak diinginkan dari atau ke dalam jaringan atau server.

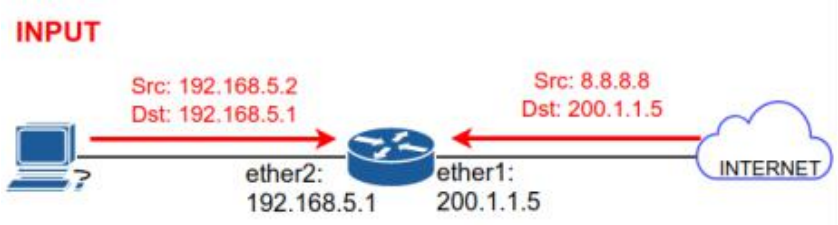
Dengan firewall filter pada mikrotik kita bisa melakukan blocking terhadap suatu traffic, misal memblock traffic ping yang masuk ke router, atau memblock traffic yang mengakses situs tertentu, memblokir usaha login secara brute-force, dsb.

IP > Firewall > Filter

Saat membuat rule firewall filter, parameter yang wajib diisi adalah chain.
Ada 3 jenis **chain** yang ada, yaitu: **input**, **output** dan **forward**.
Selain itu ada **action** yang juga wajib diisi. Value parameter action ada 11 tapi akan kita bahas hanya 3 yaitu **accept**, **drop**, dan **reject**.

- Accept = paket/traffic diizinkan (diterima)
- Drop = paket/traffic dibuang (tidak dibalas)
- Reject = paket/traffic ditolak (dibalas dengan balasan icmp)

Apa bedanya reject dan drop?
Drop akan menolak paket dengan cara mengabaikan (tidak merespon), sedangkan reject menolak paket dengan menjawab pesan balasan bisa berupa unreachable atau prohibit.



Input = traffic yang destinationnya adalah router kita, misal dari PC ke Router

Contoh:

1. kita akan memblokir ping yang masuk ke router.

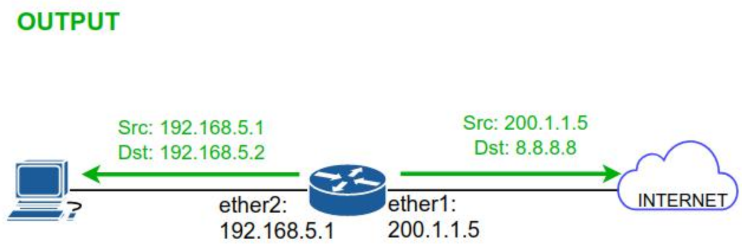
ip firewall filter add ***chain****=input* ***protocol****=icmp* ***action****=drop*
atau
ip firewall filter add ***chain****=input* ***protocol****=icmp* ***action****=reject*
reject-with*=icmp-network-unreachable*

2. Kita akan memblokir ping yang berasal dari jaringan luar (interface yang mengarah ke internet)

ip firewall filter add ***chain****=input* ***in-interface****=ether1* ***protocol****=icmp* ***action****=drop*

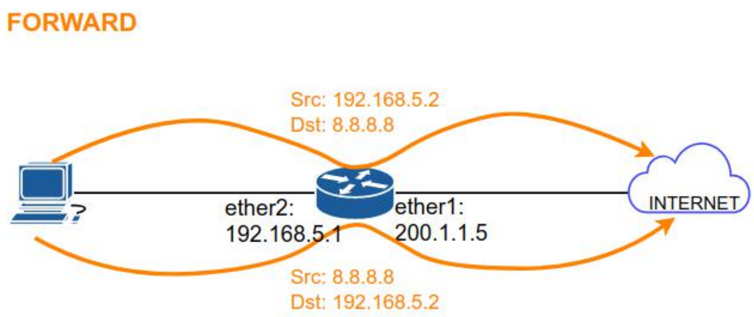
3. Kita akan memblokir ping ke router kita dari jaringan atau spesifik ip tertentu.

ip firewall filter add ***chain****=input* ***src-address****=192.168.5.0/24* ***protocol****=icmp* ***action****=drop*
atau
ip firewall filter add ***chain****=input* ***src-address****=192.168.5.2* ***protocol****=icmp* ***action****=drop*



Output = taffic dari router kita menuju ke luar, misal dari Router ke PC

1. Memblokir traffic ping dari router atau balasan ping oleh router
ip firewall filter add chain=output protocol=icmp action=drop
atau
ip firewall filter add chain=output protocol=icmp action=reject reject-with=icmp-network-unreachable



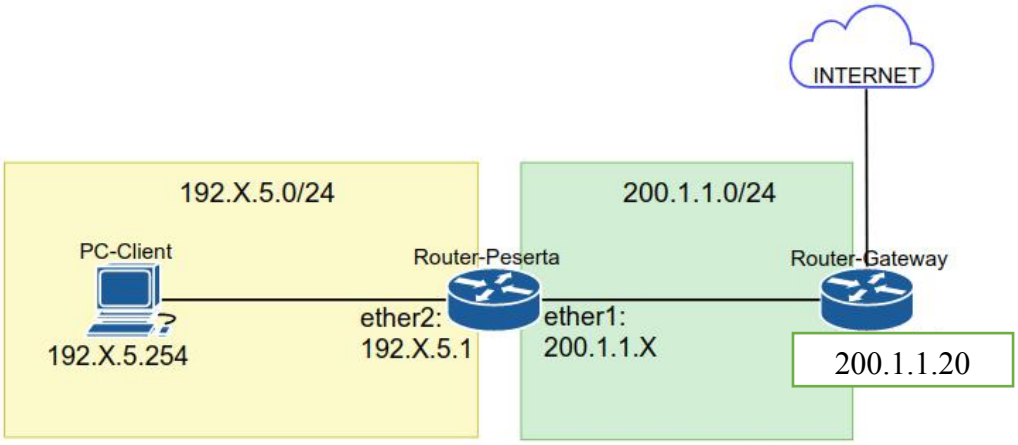
Forward = traffic yang melewati router kita, misal dari PC ke internet

1. Blokir ping ke 8.8.8.8
ip firewall filter add chain=forward dst-address=8.8.8.8 protocol=icmp action=drop

2. Blokir website tertentu (misal: facebook.com)
ip firewall filter add chain=forward content=facebook.com protocol=tcp dst-port=80,443 action=drop

SOAL MIKROTIK 4:

1. Buatlah topologi jaringan berikut. Pastikan client terhubung ke internet



2. Buat firewall filter untuk memblokir hal berikut:
   a. Block semua traffic **icmp (ping)** yang masuk ke router.
   b. Block akses **FTP, SSH, Telnet** yang menuju router dari IP **192.X.5.254**
   c. Block akses ke situs **youtube.com** dan **xdrive.xyz** sehingga semua client tidak bisa membuka situs-situs tersebut.
   d. Block akses ke situs **facebook.com** jika diakses selain dari **IP Client 192.X.5.10** (jika diakses dari client dengan ip 192.X.5.10 maka bisa).

SKEMA KEBIJAKAN FIREWALL

1. Izinkan semua block beberapa

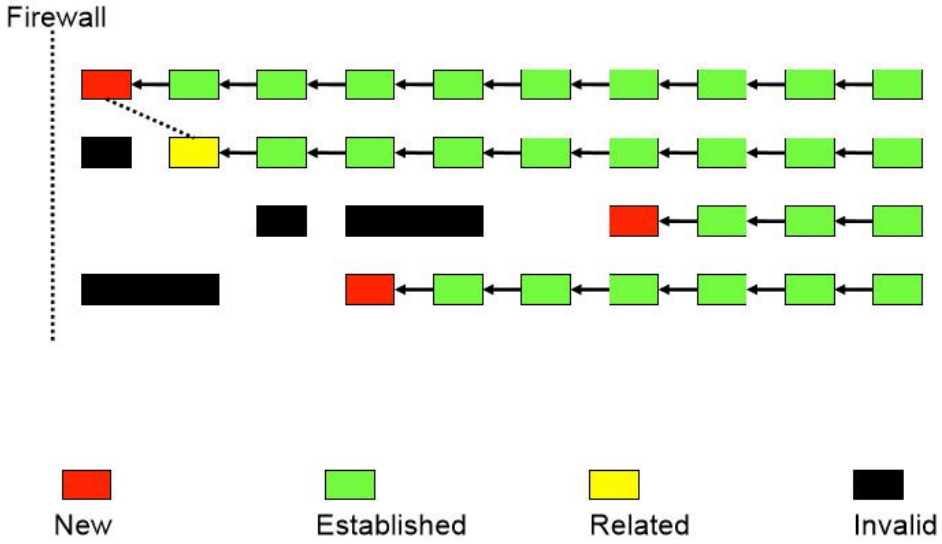
Semua traffic secara default diizinkan, sampai ada rule firewall yang memblokirnya.
Skema ini biasanya diterapkan oleh penyedia internet atau internet service provider (ISP).
Skema izinkan semua block beberapa hanya memerlukan rule untuk block traffic seperti dicontohkan sebelumnya.

Misalnya kita mau mengizinkan semua traffic, kecuali traffic icmp yang masuk ke router.
Dari permis tersebut, kita bisa simpulkan bahwa:
- semua traffic diizinkan
- blokir input icmp

Maka kita hanya perlu menambahkan rule untuk memblokir traffic input icmp.
ip firewall rule add chain=input protocol=icmp action=drop

2. Block semua izinkan beberapa

Semua traffic secara default ditolak, sampai ada rule firewall yang mengizinkannya.
Skema ini biasanya diterapkan di server atau data center dengan tujuan meningkatkan keamanan, bisa juga ditemukan di sekolah atau kantor supaya siswa/pegawainya tidak mengakses hal-hal yang tidak diinginkan.



- New : Paket baru yang memulai koneksi.
- Established : Paket data yang sudah dikenali (lanjutan paket new).
- Related : Paket yang memulai koneksi baru tetapi sudah terkait dengan koneksi yang sudah ada sebelumnya.
- Invalid : Paket yang tidak sesuai standar TCP/IP

Skema ini memiliki struktur (urutan firewall) tambahan yaitu:
Di bagian awal harus didefinisikan rule untuk mengizinkan paket **established dan related.**
Setelah itu, baru kita buat rule firewall yang menerima (accept) traffic yang diizinkan.

Dan di akhir harus didefinisikan rule firewall untuk memblokir semua traffic kecuali yang sudah diizinkan.

*ip firewall filter add **chain**=input **connection-state**=established,related **action**=accept*
*ip firewall filter add **chain**=output **connection-state**=established,related **action**=accept*
*ip firewall filter add **chain**=forward **connection-state**=established,related **action**=accept*

// rule traffic yang diizinkan,
*// hanya mengizinkan traffic browsing **web (http, https)** dari client ke internet.*
ip firewall filter add chain=forward in-interface=ether2 out-interface=ether1 protocol=udp dst-port=53 action=accept
ip firewall filter add chain=forward in-interface=ether2 out-interface=ether1 protocol=tcp dst-ports=80,443 action=accept

*ip firewall filter add **chain**=input **action**=drop*
*ip firewall filter add **chain**=output **action**=drop*
*ip firewall filter add **chain**=forward **action**=drop*

Contoh:
Kita akan memblokir semua traffic kecuali traffic berikut:

a. Client ke Router
- Winbox
ip firewall filter add chain=input protocol=tcp dst-port=8291 ***in-interface****=ether2 action=accept*

b. Router ke Client
- ICMP
ip firewall filter add chain=output protocol=icmp ***out-interface****=ether2 action=accept*

c. Router ke Internet
- ICMP
- DNS
ip firewall filter add chain=output protocol=icmp ***out-interface****=ether1 action=accept*
ip firewall filter add chain=output protocol=udp dst-port=53 ***out-interface****=ether1 action=accept*

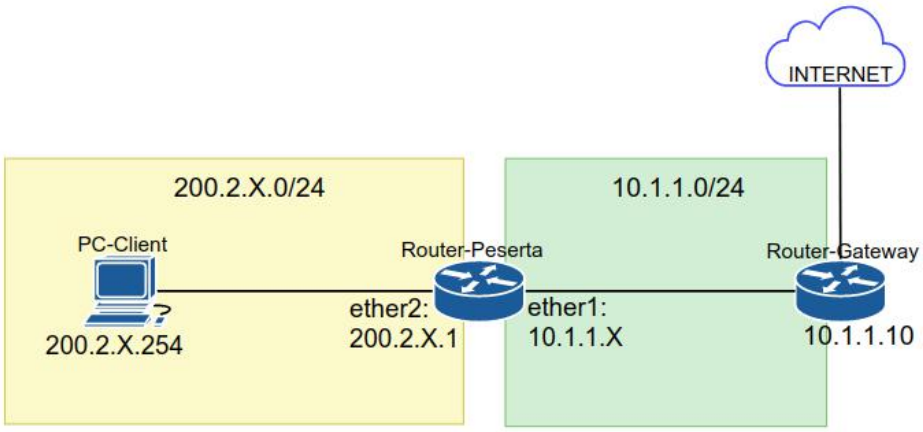
d. Internet ke Router
- HTTP, HTPPS
ip firewall filter add chain=input protocol=tcp dst-port=80,443 ***in-interface****=ether1 action=accept*

e. Client ke Internet
- DNS
- HTTP, HTTPS
ip firewall filter add chain=forward protocol=udp dst-port=53 ***in-interface****=ether2*
out-interface*=ether1 action=accept*
ip firewall filter add chain=forward protocol=tcp dst-port=80,443 ***in-interface****=ether2*
out-interface*=ether1 action=accept*

Nah, rule tersebut kita susun dengan struktur rule yang dijelaskan sebelumnya:

ip firewall filter add ***chain****=input* ***connection-state****=established,related* ***action****=accept*
ip firewall filter add ***chain****=output* ***connection-state****=established,related* ***action****=accept*
ip firewall filter add ***chain****=forward* ***connection-state****=established,related* ***action****=accept*
ip firewall filter add ***chain****=input* ***protocol****=tcp* ***dst-port****=8291* ***in-interface****=ether2* ***action****=accept*
ip firewall filter add ***chain****=output* ***protocol****=icmp* ***out-interface****=ether2* ***action****=accept*
ip firewall filter add ***chain****=output* ***protocol****=icmp* ***out-interface****=ether1* ***action****=accept*
ip firewall filter add ***chain****=output* ***protocol****=udp* ***dst-port****=53* ***in-interface****=ether1* ***action****=accept*
ip firewall filter add ***chain****=input* ***protocol****=tcp* ***dst-port****=80,443* ***in-interface****=ether1* ***action****=accept*
ip firewall filter add ***chain****=forward* ***protocol****=udp* ***dst-port****=53* ***in-interface****=ether1*
out-interface*=ether2* ***action****=accept*
ip firewall filter add ***chain****=forward* ***protocol****=tcp* ***dst-port****=80,443* ***in-interface****=ether1*
out-interface*=ether2* ***action****=accept*
ip firewall filter add ***chain****=input* ***action****=drop*
ip firewall filter add ***chain****=output* ***action****=drop*
ip firewall filter add ***chain****=forward* ***action****=drop*

SOAL MIKROTIK 5
Buat jaringan seperti berikut.



Blokir semua traffic kecuali

Client ke Router:
- ICMP (pc ping ke router)
- Winbox (pc mengakses router lewat winbox)
- FTP (pc akses router lewat filezilla)

Client ke Internet
- ICMP (client ping ke internet)
- DNS
- HTTP/HTTPS

BAB 4 - MIKHMON (MIKROTIK HOTSPOT MONITOR)

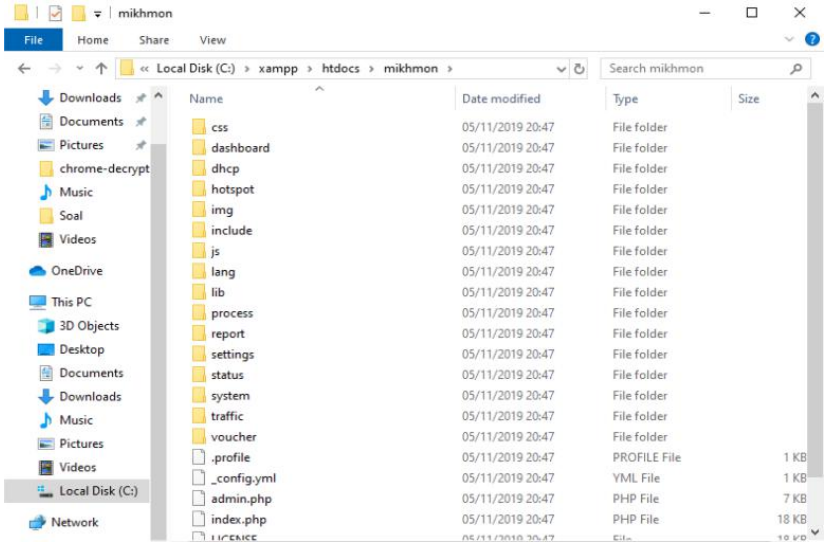
MikroTik Hotspot Monitor adalah aplikasi berbasis web (MikroTik API PHP class) untuk membantu manajemen Hotspot MikroTik. Khususnya MikroTik yang tidak mendukung User Manager. Mikhmon bukan radius server, jadi tidak harus selalu aktif. Mikhmon dapat diaktifkan saat dibutuhkan atau sesuai kebutuhan.

Agar dapat mengoperasikan Mikhmon diperlukan sebuah webserver + PHP yang bisa diinstall diberbagai sistem operasi. Mikhmon dapat dijalakan di Windows, Linux, Android maupun Openwrt. Selain itu Mikhmon juga bisa diupload ke hosting atau VPS.

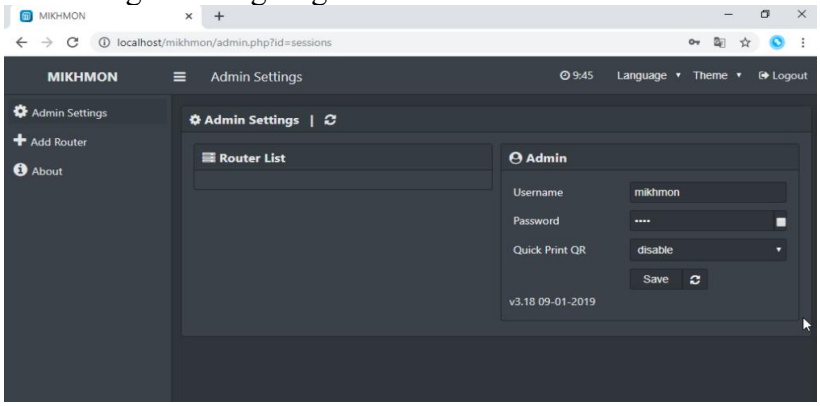
Mikhmon dikembangkan oleh orang Indonesia yaitu Gusti Komang Laksamadi. Situs resmi mikhmon adalah https://laksa19.github.io. Di situ kita bisa mendownload source codenya secara gratis dan tersedia juga tutorialnya.

A. Cara Instalasi Mikhmon

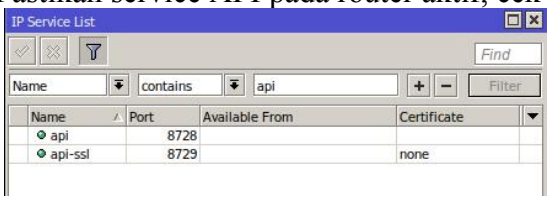
1. Buat direktori "mikhmon" di htdocs web server kita, kemudian ownload Mikhmon di https://github.com/laksa19/mikhmonv3 lalu ekstrack, simpan di directori yang tadi dibuat.



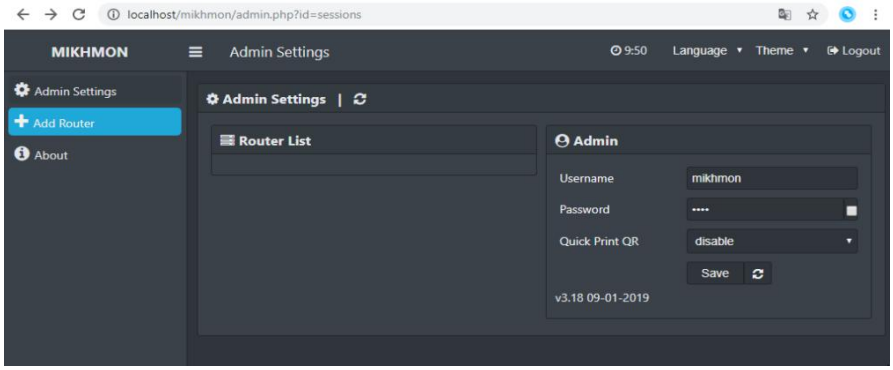
2. Buka webnya (https://localhost/mikhmon), default loginya adalah user *mikhmon,* password *1234.* Kita bisa mengubah langsung atau membiarkan default.



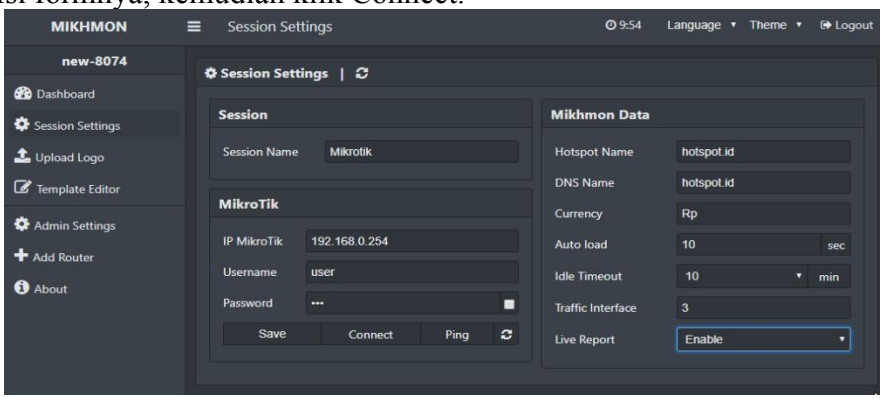
3. Pastikan service API pada router aktif, cek di *IP > Services.*



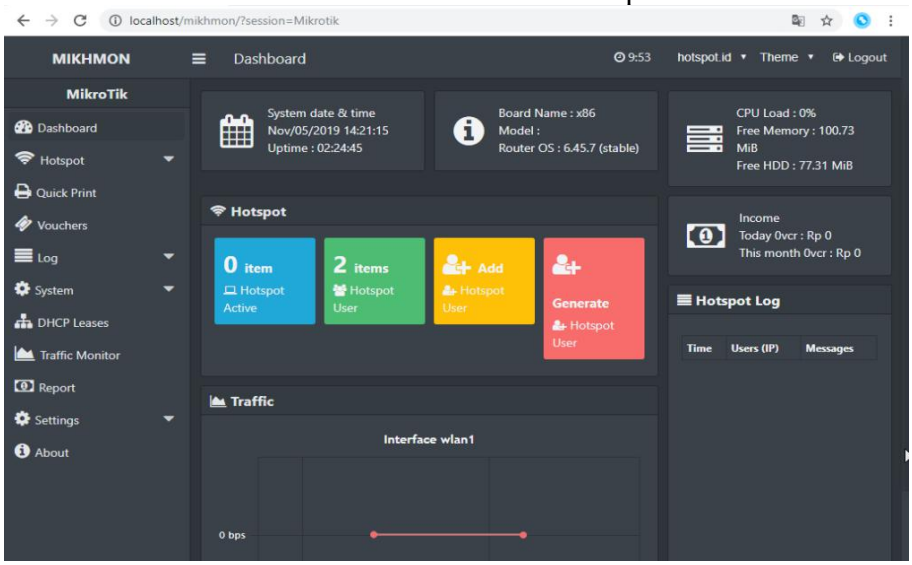
4. Kembali ke mikhmon di tampilan awal, klik *Add Router.*



5. Isi formnya, kemudian klik Connect.



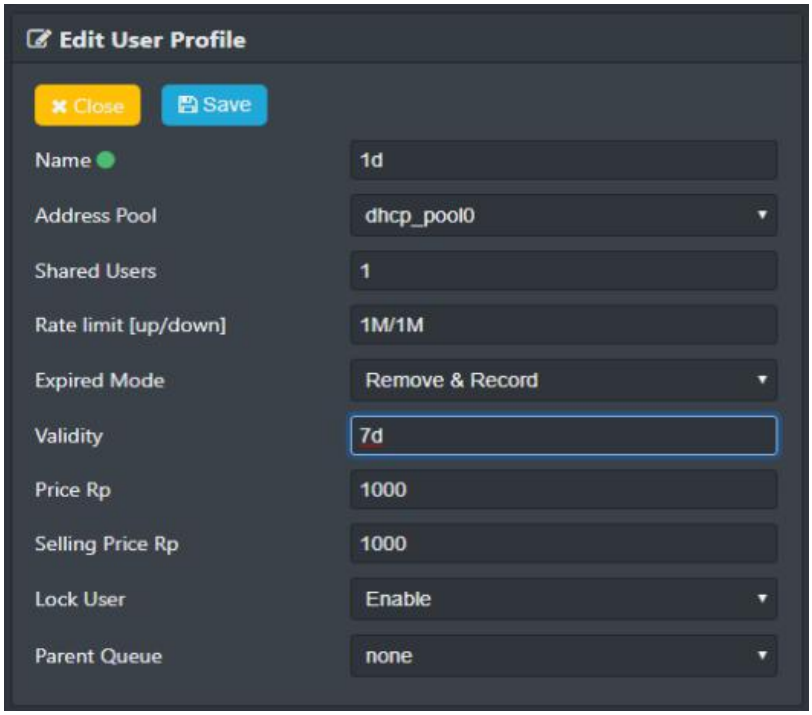
6. Kemudian kita akan diarahkan ke dashboard hotspot kita.



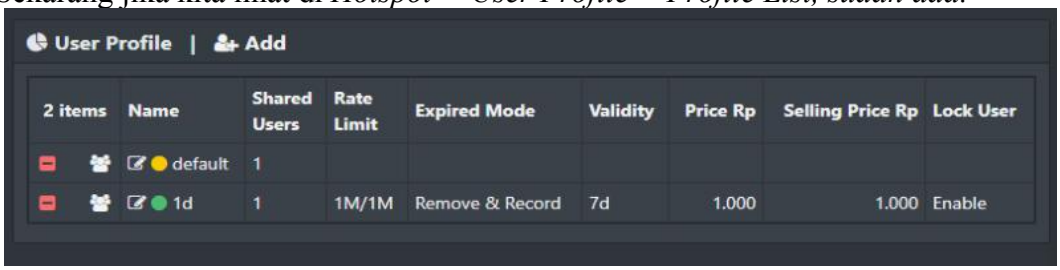
B. Cara Mengelola User

1. Pertama, kita buat user profile terlebih dahulu, Dari dashboard hotspot kita. Buka *Hotspot > User Profile > Add Profile.* Isi form kemdian Save

Name = nama profil
Address pool = IP yang akan digunakan.
Shared user = user bisa login berapa perangkat
Rate limit = batas kecepatan upload download
Expired mode = saat user expired, akan diapakan, apakah dihapus saja atau dicatat juga.
Validity = Masa berlaku user.
Price = harga.
Lock user = Apakah mac address dicatat, jika iya maka user tidak bisa dipakai di perangkat lain.
Parent queue = parent queue yang mengatur.



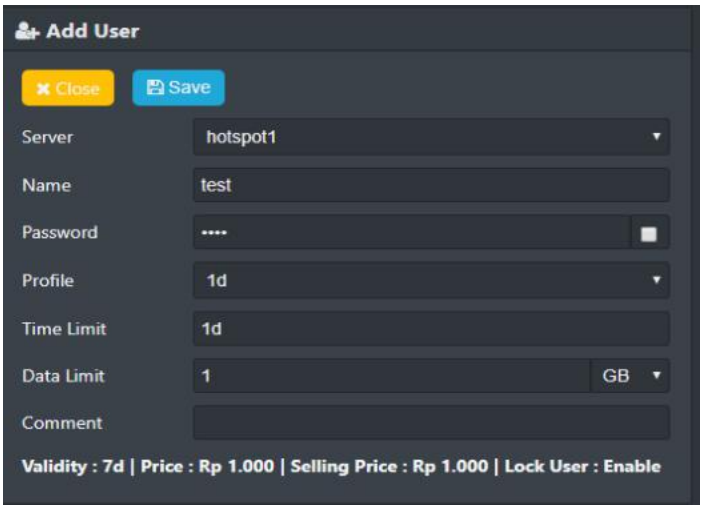
2. Sekarang jika kita lihat di *Hotspot > User Profile > Profile List, sudah ada.*



3. Tahap berikutnya adalah membuat user. Ada dua cara yaitu Add user dan generate. Add user yaitu kita menambahkan user satu per satu sedangkan generate adalah kita membuat user secara masal.

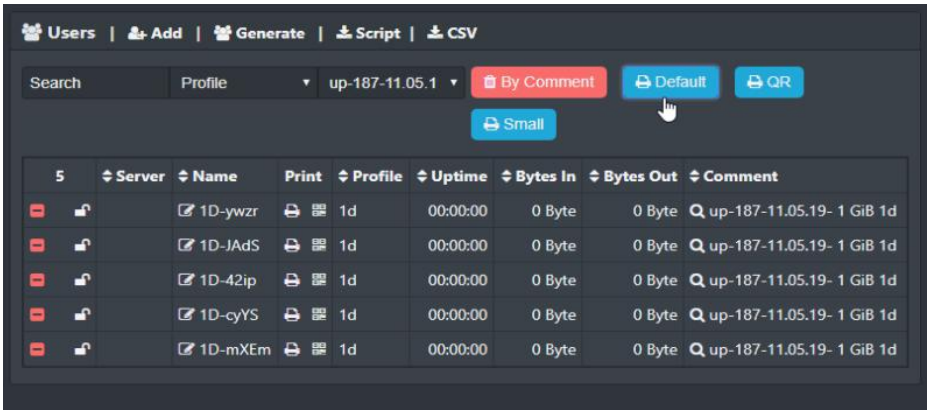
4. Membuat user dengan cara Add user. Buka *Hotspot* > *Users* > *Add User*. Isi formnya kemudian Save.

Server = server hotspot
Name = username user untuk login
Password = kata sandi user untuk login
Profile = pilih user profile
Time limit = masa berlaku (dihitung setelah login)
Data limit = kuota atau batasan pemakaian data
Comment = komentar atau catatan

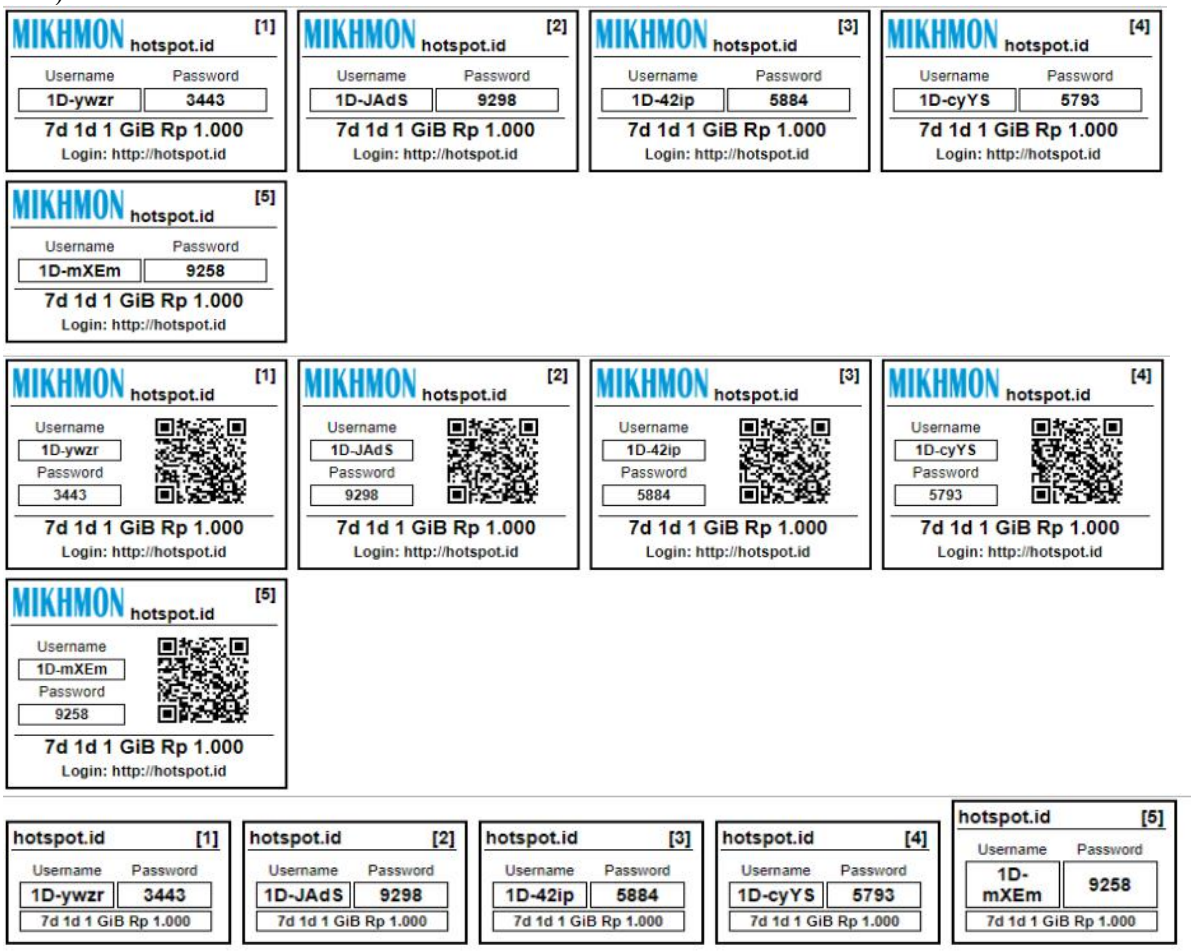


5. Membuat user secara masal atau generate user. Username dan password ibuat secara acak oleh sistem. Buka *Hotspot* > *Users* > *Generate*. Isi formnya kemudian klik Generate.
Qty = jumlah user yang akan dibuat
Server = server hotspot yang menangani user
Name Lenght = panjang username random
Prefix = awalan nama user atau username
Character = karakter yang digunakan untuk membuat random username.
Profile = pilih user profile
Time limit = masa berlaku (dihitung setelah login)
Data limit = kuota atau batasan pemakaian data
Comment = komentar atau catatan

6. Mencetak voucher. Untuk mencetak voucher buka *Hotspot* > *User* > *User List*. Filter user berdasarkan profile dan comment. Kemudian pilih salah satu metod print (default, QR untuk menampilkan QR code, small untuk tampilan versi mini).

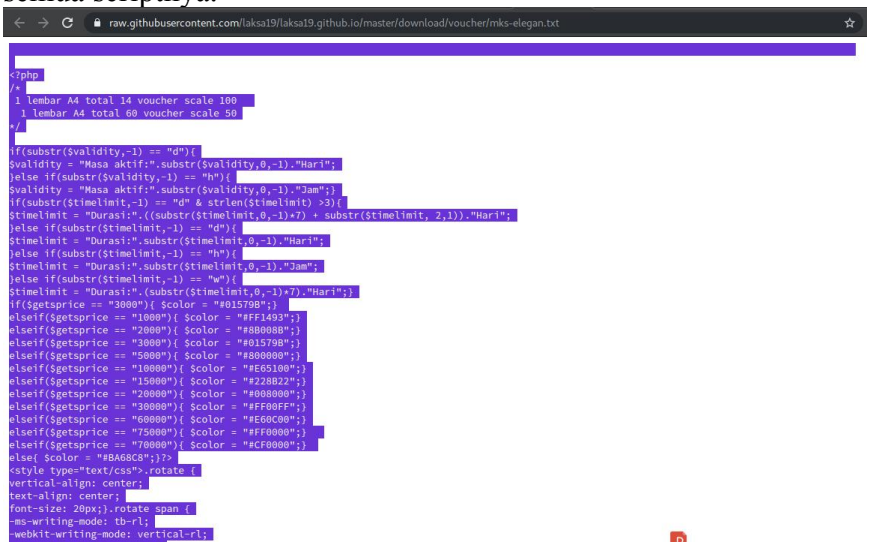


7. Maka kita akan diarahkan ke halaman printing. Ini adalah contoh default, QR, dan small (urut dari atas).

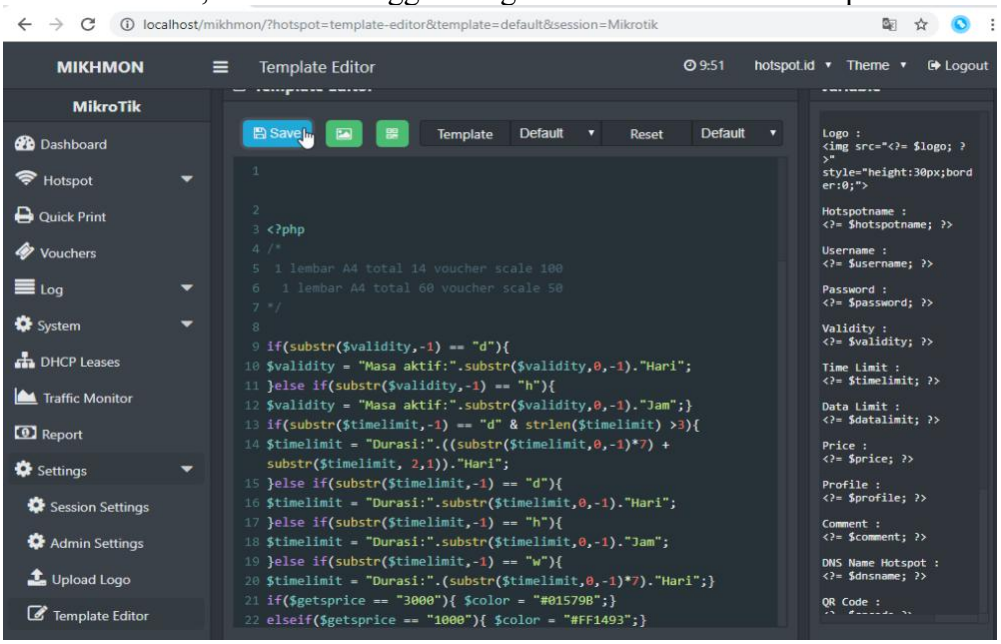


C. Cara Mengganti atau Custom Tampilan Voucher.

1. Pilih template voucher di https://laksa19.github.io/voucher.html, klik download, kemudian copy semua scriptnya.



2. Pada mikhmon hotspot. Buka *Setting* > *Template Editor*. Paste scriptnya pada form yang tersedia. Kemudian save, kita bisa mengganti logo atau tulisan melalui script tersebut.



3. Sekarang jika kita coba print lagi, tampilan vouchernya seperti ini:


Rp 1.000
HOTSPOT.ID
User: 1D-ywzr
Pass: 3443
Masa aktif:7Hari Durasi:1Hari 1 GiB
Login:hotspot.id - - Cs : 08123456789
Rp 1.000
HOTSPOT.ID
User: 1D-JAdS
Pass: 9298
Masa aktif:7Hari Durasi:1Hari 1 GiB
Login:hotspot.id - - Cs : 08123456789
Rp 1.000
HOTSPOT.ID
User: 1D-42ip
Pass: 5884
Masa aktif:7Hari Durasi:1Hari 1 GiB
Login:hotspot.id - - Cs : 08123456789
Rp 1.000
HOTSPOT.ID
User: 1D-cyYS
Pass: 5793
Masa aktif:7Hari Durasi:1Hari 1 GiB
Login:hotspot.id - - Cs : 08123456789
Rp 1.000
HOTSPOT.ID
User: 1D-mXEm
Pass: 9258
Masa aktif:7Hari Durasi:1Hari 1 GiB
Login:hotspot.id - - Cs : 08123456789

REFERENSI

https://www.webiptek.com/
https://wiki.mikrotik.com/
https://citraweb.com/
https://laksa19.github.io/