



Advanced Mikrotik Training User Manager (MTCUME)



Certified Mikrotik Training - Advanced Class (MTCUME)

Organized by: Citraweb Nusa Infomedia
(Mikrotik Certified Training Partner)



Schedule - Module

| | Sesi 1 | Sesi 2 | Sesi 3 | Sesi 4 |
|---------------|-------------------------------------------|----------------|--------------------------------|---------------|
| Hari 1 | Basic Config, PPTP & PPPoE | | BCP Bridging & MLPP | |
| Hari 2 | L2TP & IPSEC | HOTSPOT | | |
| Hari 3 | RADIUS / USER MANAGER | | | |
| Hari 4 | LAB | | | TEST |



Schedule

- Sessi 1 08.30 – 10.15
- Coffee Break 10.15 – 10.30
- Sessi 2 10.30 - 12.15
- Lunch 12.15 – 13.15
- Sessi 3 13.15 – 15.00
- Coffee Break 15.00 – 15.15
- Sessi 4 15.15 - 17.00



New Training Scheme 2009

- **Basic / Essential Training**

- MikroTik Certified Network Associate (MTCNA)

- **Advanced Training**

- Certified Wireless Engineer (MTCWE)
- Certified Routing Engineer (MTCRE)
- Certified Traffic Control Engineer (MTCTCE)
- Certified User Managing Engineer (MTCUME)
- Certified Inter Networking Engineer (MTCINE)

Certification Test

- Diadakan oleh **Mikrotik.com** secara online
- Dilakukan pada sesi terakhir
- Jumlah soal : **25** Waktu: **60 menit**
- Nilai minimal kelulusan : **60%**
- Yang mendapatkan nilai **50%** hingga **59%** berkesempatan mengambil “***second chance***”
- Yang lulus akan mendapatkan sertifikat yang diakui secara internasional





Trainers

- **Novan Chris**

- MTCNA (2006), Certified Trainer (2008)
- MTCWE (2008), MTCRE (2008)
- MTCTCE (2011), MTCUME (2012)
- MTCINE (2012)

- **Pujo Dewobroto**

- MTCNA (2009), MTCTCE (2009)
- MTCWE (2010), MTCRE (2011)
- MTCUME (2012), Certified Trainer (2011)



Perkenalkan

- Perkenalkanlah :
 - Nama Anda
 - Tempat bekerja
 - Kota / domisili
 - Apa yang Anda kerjakan sehari-hari dan fitur-fitur apa yang ada di Mikrotik yang Anda gunakan



Thank You !



info@mikrotik.co.id

Dijinkan menggunakan sebagian atau seluruh materi pada modul ini, baik berupa ide, foto, tulisan, konfigurasi, diagram, selama untuk kepentingan pengajaran, dan memberikan kredit dan link ke www.mikrotik.co.id



PPTP & PPPoE



Certified Mikrotik Training - Advanced Class (MTCUME)

Organized by: Citraweb Nusa Infomedia

(Mikrotik Certified Training Partner)



Outline

- VPN Overview
- PPTP
 - PPTP Server
 - PPTP Client
- PPPoE
 - PPPoE Client
 - PPPoE Server
- PPPoE Large Network



Overview

- Seiring perkembangan jaman, maka pertukaran data antar lokasi yang berjauhan dilakukan menggunakan jaringan internet
- Internet = **UNSECURE !!**
- VPN atau Virtual Private Networking merupakan suatu metode untuk melakukan autentikasi pada perangkat yang akan berkomunikasi dan membuatkan jalur khusus (tunnel) secara virtual diatas jalur yang sudah ada
- Untuk meningkatkan keamanan, VPN juga bisa ditambahkan enkripsi untuk pertukaran datanya
- PPTP & PPPoE adalah contoh interface untuk implementasi VPN



PPTP

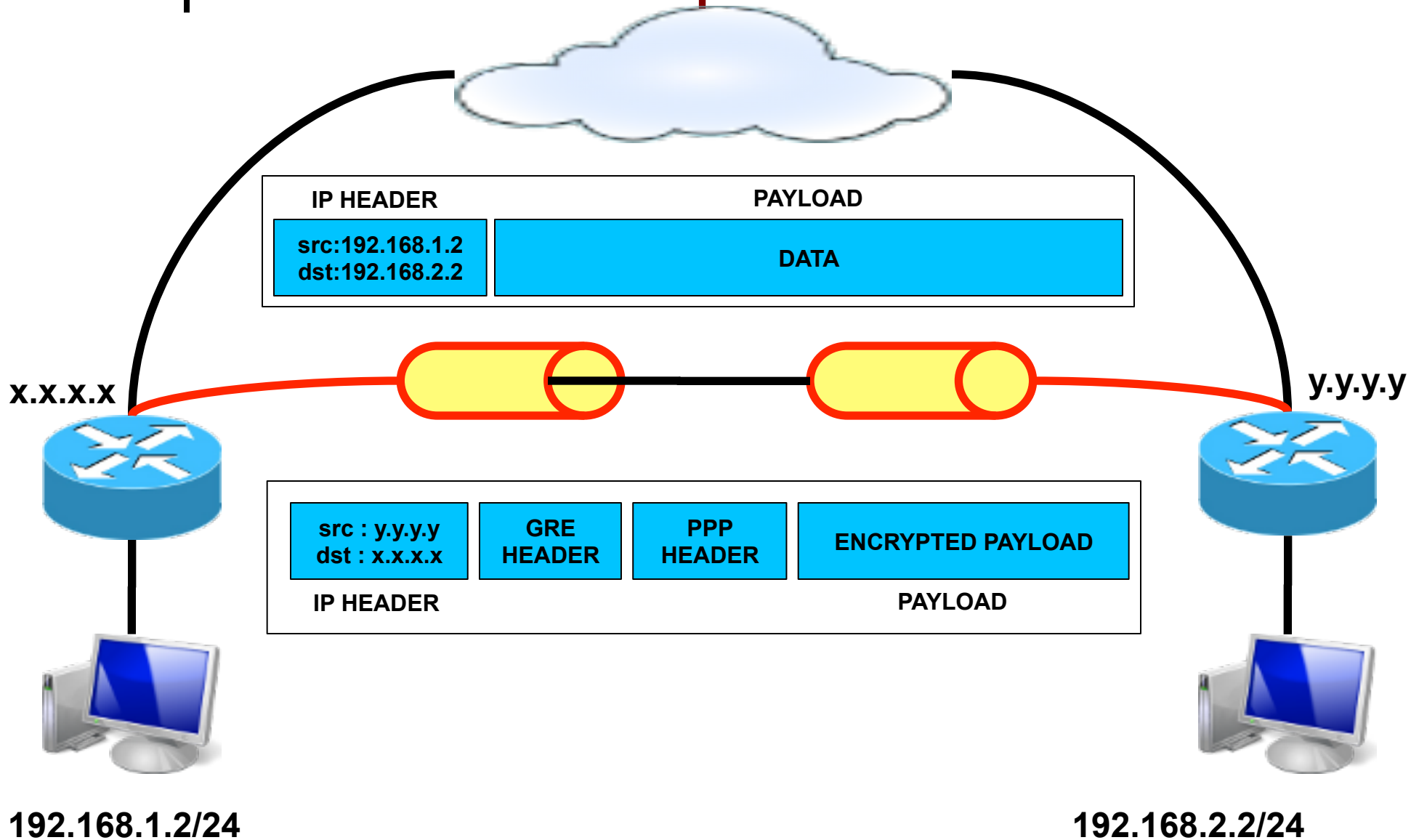
- PPTP sebenarnya merupakan pengembangan dari protocol yang sudah ada yaitu PPP. Sehingga fitur yang ada pada PPP bisa digunakan pada PPTP
- Fitur yang tersedia pada PPTP (derivative dari PPP):
 - Compression : Van Jazobson compression
 - Authentication : PAP, CHAP, MSCHAP
 - Encrpytion : MPPE
 - Data Delivery : Multi protocol bisa dilewatkan (IP, IPX, NetBEUI dsb)
 - Client Addressing



PPTP

- Sebelum tunnel terbentuk, antara client dan server akan membuat session TCP yang disebut “Control Connection”
- Control Connection ini akan bertanggung jawab terhadap pembentukan, manajemen dan pemutusan sesi yang dipertukarkan melalui tunnel
- Control Connection ini akan dipertukarkan pada protocol TCP port 1723
- Jika Control Connection sudah terbentuk, akan dibentuk tunnel menggunakan protocol GRE. Semua paket data dari aplikasi yang sudah diencap dalam segment PPP akan dipertukarkan melalui tunnel ini
- Secara sederhananya, PPTP akan membungkus packet data kedalam paket PPP dan kemudian paket PPP ini yang akan dibungkus menggunakan IP protocol 47 (GRE)

PPTP Concept



PPTP Client

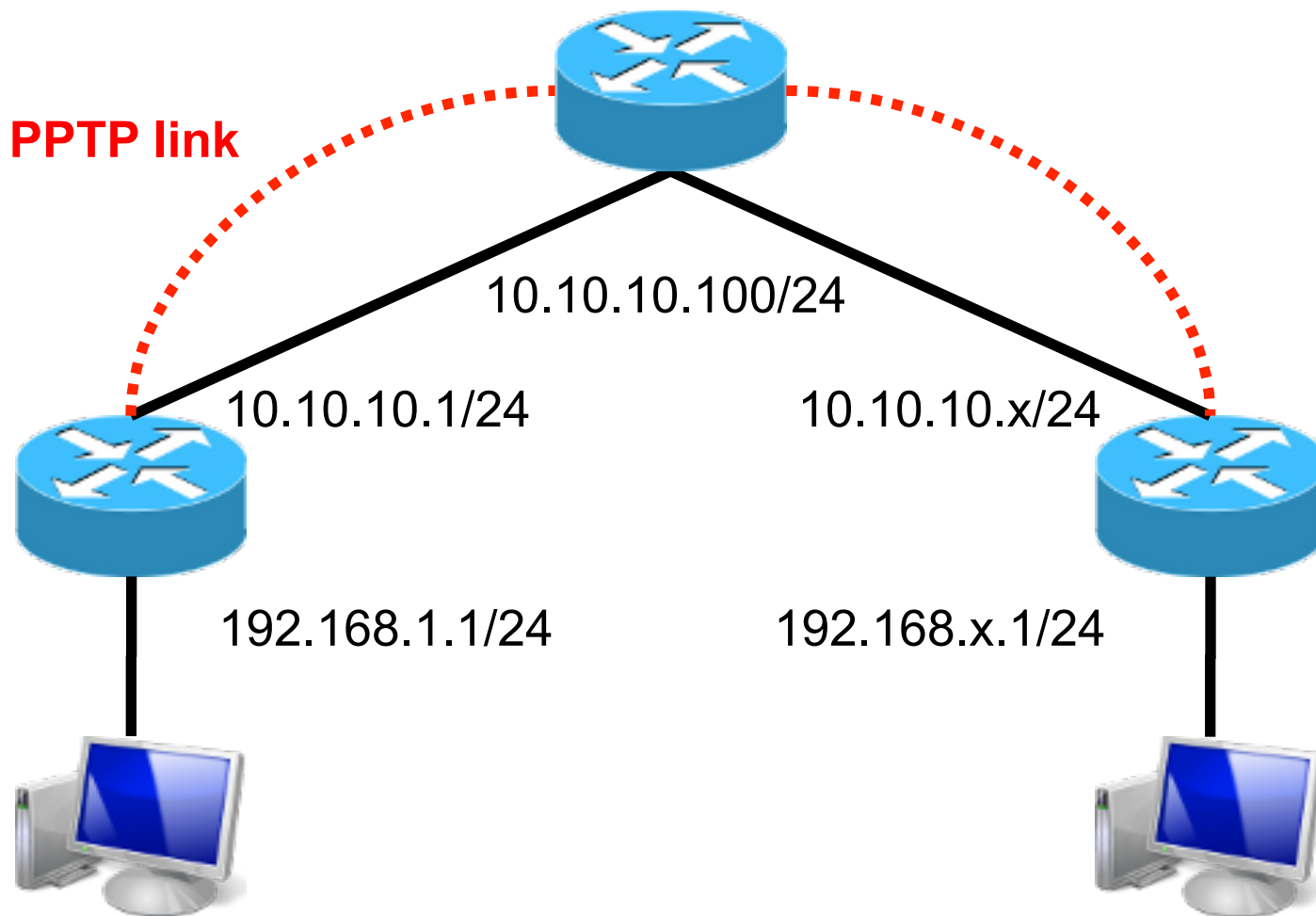
The screenshot displays the Mikrotik WinBox interface for configuring a new interface. The left sidebar shows a tree view with categories like Wireless, Bridge, PPP, Switch, Mesh, IP, IPv6, MPLS, Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, MetaROUTER, Make Supout.rif, and Manual. The 'PPP' category is selected, and a sub-menu is open showing options: PPP Server, PPP Client, PPTP Server, PPTP Client, SSTP Server, SSTP Client, L2TP Server, L2TP Client, OVPN Server, OVPN Client, PPPoE Server, and PPPoE Client. The 'PPTP Client' option is highlighted. The main window is titled 'New Interface' and has tabs for 'General', 'Dial Out', 'Status', and 'Traffic'. The 'Dial Out' tab is active, showing the 'Connect To' field set to '0.0.0.0', 'User' and 'Password' fields, a 'Profile' dropdown set to 'default-encryption', and checkboxes for 'Dial On Demand' and 'Add Default Route'. Under the 'Allow' section, checkboxes for 'pap', 'mschap1', 'chap', and 'mschap2' are all checked. At the bottom, there are status indicators for 'enabled', 'running', 'slave', and 'Status:'. Red arrows highlight the navigation path from the sidebar to the 'Dial Out' tab.



PPTP Client

- Parameter-parameter yang bisa kita tentukan pada saat pembuatan interface pptp client meliputi
 - Connect To : Alamat IP / domain dari server VPN
 - User : username dari VPN
 - Password : password dari VPN
 - Dial On Demand : VPN akan aktif otomatis apabila ada trafik yang akan melalui interface ini
 - Add Default route : Menambahkan default gateway melalui interface ini
 - Profile : Penggunaan pengaturan lebih detil pada sebuah interface

[LAB-1] PPTP Client



[LAB-1] PPTP Client

- Buat VPN client untuk pptp1 ke router 10.10.10.100, dan pptp2 ke 10.100.100.1
 - Untuk username pptp1 = pptp1-X (X = nomer meja)
 - Untuk username pptp2 = pptp2-X (X = nomer meja)
 - Password kedua vpn = test
- Setting router untuk koneksi internet via pptp-1 dan untuk koneksi network lokal teman sebelah via pptp-2
- Matikan default gateway ke 10.10.10.100
- Aktifkan nat masquerade untuk pptp1
- Make Backup :)

[LAB-1] PPTP Client

The screenshot displays the Mikrotik WinBox interface. The 'Route List' window is open, showing a table of routes. A red box highlights the '+' icon in the toolbar, and a red arrow points from it to the 'Route <10.100.100.1>' configuration dialog. In this dialog, the 'General' tab is active, and a red box highlights the 'Dst. Address' field (set to 10.100.100.1) and the 'Gateway' field (set to 10.10.10.100 reachable wlan1). Other fields include 'Check Gateway', 'Type: unicast', 'Distance: 1', 'Scope: 30', 'Target Scope: 10', 'Routing Mark', and 'Pref. Source'. Buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', and 'Remove' are visible on the right.

| Routes | Nexthops | Rules | VRF |
|--------|-------------------|------------------------------|-----|
| AS | ▶ 0.0.0.0/0 | 10.10.10.100 reachable wlan1 | |
| Dy | ▶ 10.10.10.0/24 | | |
| AS | ▶ 10.100.100.1 | | |
| Dy | ▶ 192.168.30.0... | | |

- Untuk multi VPN client dalam 1 router, disarankan untuk membuat routing statik terlebih dahulu ke server apabila IP server tidak terhubung 1 network

[LAB-1] PPTP Client

The image shows two side-by-side configuration windows for PPTP clients in Mikrotik WinBox. The left window is for 'Interface <pptp-out1>' and the right window is for 'Interface <pptp-out2>'. Both windows have tabs for 'General', 'Dial Out', 'Status', and 'Traffic'. The 'Dial Out' tab is active in both.

Interface <pptp-out1> Configuration:

- Connect To: 10.10.10.100
- User: pptp1-X
- Password: test
- Profile: default-encryption
- Dial On Demand
- Add Default Route
- Allow:
 - pap
 - mschap1
 - chap
 - mschap2

Interface <pptp-out2> Configuration:

- Connect To: 10.100.100.1
- User: pptp2-X
- Password: test
- Profile: default-encryption
- Dial On Demand
- Add Default Route
- Allow:
 - pap
 - mschap1
 - chap
 - mschap2

Buttons on the right side of the right window: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Torch.

Bottom status bars: The left window shows 'enabled', 'running', and 'slave'. The right window shows 'enabled', 'running', 'slave', and 'Status: connected'.

[LAB-1] PPTP Client

The screenshot shows the Mikrotik WinBox interface. The 'Route List' window is open, displaying a table of routes. A red box highlights the '+' icon in the toolbar, which is used to add a new route. A red arrow points from this icon to the 'Route <192.168.31.0/24>' configuration dialog. In this dialog, the 'General' tab is active, and a red box highlights the 'Dst. Address' field (set to '192.168.31.0/24') and the 'Gateway' dropdown menu (set to 'pptp-out2'). Other fields in the dialog include 'Check Gateway', 'Type' (unicast), 'Distance' (1), 'Scope' (30), 'Target Scope' (10), 'Routing Mark', and 'Pref. Source'. The dialog also features buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', and 'Remove'.

| Routes | Nexthops | Rules | VRF | |
|--------------|-----------------|----------|--------------|--------------|
| + | - | ✓ | ✗ | |
| Find | all | | | |
| Dst. Address | Gateway | Distance | Routing Mark | Pref. Source |
| X | 10.10.10.100 | 1 | | |
| DAS | 0.0.0.0/0 | | | |
| DAC | 10.10.10.10 | | | |
| DAC | 10.10.20.10 | | | |
| DAC | 10.10.30.10 | | | |
| AS | 10.100.10.10 | | | |
| DAC | 192.168.31.0/24 | | | |
| AS | 192.168.31.0/24 | | | |

Khusus untuk link point to point, kita bisa menggunakan interface sebagai gatewaynya



PPP Interface

- Untuk pembuatan PPTP server, bisa kita atur didalam menu PPP Interface
- PPP interface ini akan berisi interface-interface VPN baik server ataupun client yang terhubung ke server kita
- Interface PPTP server bisa dicreate dengan menggunakan 2 metode :
 - Dynamic Interface : Interface ini akan muncul secara otomatis apabila client melakukan login belum ada static interface yang dibuat
 - Static Interface : Interface kita buat secara manual berdasarkan username client kita
- Static Interface bisa kita gunakan apabila kita membutuhkan service berdasarkan parameter interface, misalnya parameter in-interface / out-interface pada firewall, bisa juga kita gunakan untuk memonitor trafik untuk keseluruhan session per client

PPTP Server

admin@192.168.30.1 (30-mejadepan) - WinBox v5.21 on RB433UAH (mipsbe)

Safe Mode

Quick Set
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal

PPP

Interface PPPoE Servers Secrets Profiles Active Connections

PPP Scanner PPTP Server SSTP Server L2TP Server

| | Name | Type | L2 MTU | Tx | Rx | Tx Pac... | Rx Pac... | Tx |
|---|------------|-------------|--------|---------|-------|-----------|-----------|----|
| R | ppptp-out1 | PPTP Client | | 358 bps | 0 bps | 2 | 0 | |
| R | ppptp-out2 | PPTP Client | | 0 bps | 0 bps | 0 | 0 | |

PPTP Server

Enabled

Max MTU: 1460

Max MRU: 1460

MRRU: [dropdown]

Keepalive Timeout: 30

Default Profile: default-encryption

Authentication

pap chap

mschap1 mschap2

OK
Cancel
Apply

2 items out of 7



PPTP Server

Parameter dalam penentuan PPTP server

- Enabled = Server aktif / tidak
- MTU (Maximum Transmission Unit) = Besar paket yang bisa dikirimkan setelah dikurangi header (untuk PPTP 40 byte)
- MRU (Maximum Receive Unit) = Besar paket yang bisa diterima setelah dikurangi header
- MRRU (Multilink Maximum Received Reconstructed Unit) = Besar paket yang bisa diterima untuk multilink PPP (detail pada materi BCP)
- Keepalive Timeout : interval pengecekan server terhadap client. Jika tidak ada respons dari client akan diputus koneksinya
- Default Profile : penggunaan default group untuk client VPN
- Authentication : metode pertukaran informasi username dan passwordnya



PPP Profile

- PPP profile merupakan sebuah fungsi untuk mengelompokkan / melakukan grouping pada user VPN kita nantinya sehingga masing-masing group bisa memiliki parameter yang berbeda antar groupnya
- Parameter yang sering digunakan meliputi :
 - Local & Remote Address
 - Incoming & Outgoing filter
 - Encryption, Compression, Rate Limit
 - Share user / Only one?
 - Session & Idle Timeout
- Profile ini juga bisa digunakan untuk user-user yang terautentikasi menggunakan RADIUS
- Jika didalam profile menggunakan parameter default, berarti akan mengikuti profile yang sesuai pada setting Server atau pada Radius Server

PPP Profile

PPP

Interface PPPoE Servers Secrets Profiles Act

| Name | Local Address | Remote Address |
|------------------|---------------|----------------|
| * default | | |
| * default-enc... | | |

2 items

New PPP Profile

General Protocols Limits

Name: profile1

Local Address: []

Remote Address: []

Bridge: []

Incoming Filter: []

Outgoing Filter: []

Address List: []

DNS Server: []

WINS Server: []

Change TCP MSS

default no yes

OK Cancel Apply Comment Copy Remove

PPP Profile

New PPP Profile

General Protocols **Limits**

– Use MPLS —
 default no yes required

– Use Compression —
 default no yes

– Use VJ Compression —
 default no yes

– Use Encryption —
 default no yes required

New PPP Profile

General Protocols **Limits**

Session Timeout: ▼

Idle Timeout: ▼

Rate Limit (rx/tx): ▼

– Only One —
 default no yes

OK
Cancel
Apply
Comment
Copy
Remove

PPP Profile

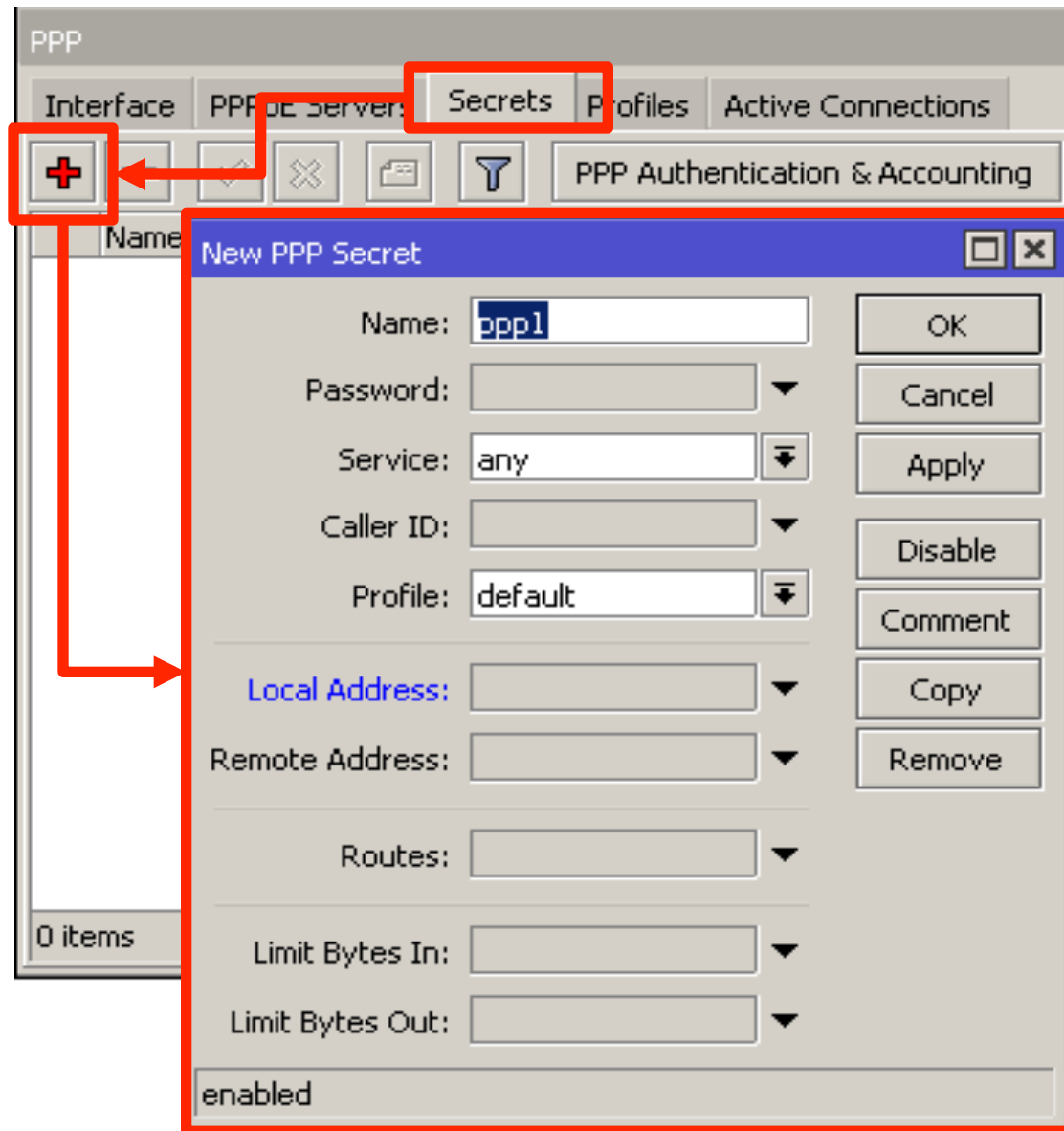
- Local Address = IP yang akan terpasang disisi router
- Remote Address = IP yang akan terpasang disisi client
 - Kedua IP ini bisa menggunakan IP Pool jika clientnya banyak
- Use Encryption = Apakah akan menggunakan Enkripsi MPPE (jika required berarti server dan client harus sama-sama diset)
- Use Compression = Apakah akan dilakukan compresi paket datanya
- Only One = Hanya 1 perangkat per username
- Session timeout = maximal waktu dalam sekali session / login
- Idle timeout = Koneksi akan diputus jika tidak ada trafik dalam waktu yang ditentukan
- Rate limit = limitasi / queue otomatis per client
 - Format : **rx-rate[/tx-rate] [rx-burst-rate[/tx-burst-rate] [rx-burst-threshold[/tx-burst-threshold] [rx-burst-time[/tx-burst-time] [priority] [rx-rate-min[/tx-rate-min]]]]]**



PPP Secret

- Merupakan database lokal penyimpanan informasi username dan password dari client
- PPP secret ini hanya bisa digunakan untuk service VPN yang masih berada dalam 1 mesin
- Jika local address dan remote address pada PPP secret diisikan maka parameter pada setting PPP profile akan diabaikan
- Didalam PPP secret ini kita juga bisa mengaktifkan accounting dan authentication menggunakan RADIUS server
- Apabila informasi username di local secret tidak ada, maka router akan melakukan pengecekan di RADIUS server

PPP Secret



PPP Secret

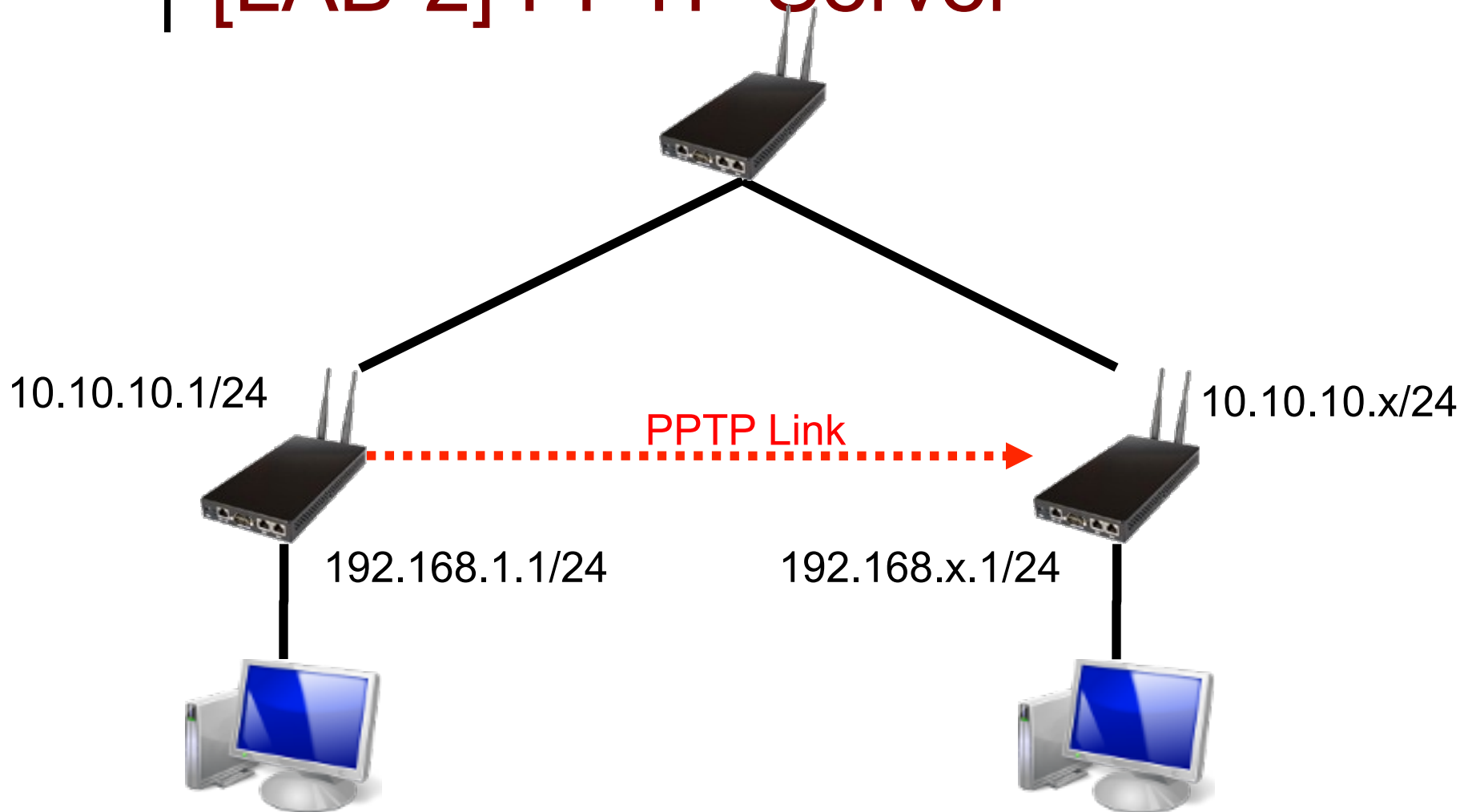
- Name : Informasi Username
- Password : Informasi Password
 - Kedua parameter diatas **case – sensitive !!**
- Service : Jika diset **BUKAN ANY** , berarti hanya untuk 1 service yang dipilih
- Caller id : Pembatasan IP / MAC dari user tertentu yang boleh login
- Profile : penggunaan group dari /ppp profile
- Routes : Akan dipasangkan routing ke network local client
 - **Format : *dst-address gateway metric***
- Limit Byte In : Maximum quota upload client
- Limit Byte Out : Maximum quota download client

PPP Active Connection

| | Name | Service | Caller ID | Encoding | Address | Uptime |
|---|----------|---------|-------------|-------------------|-------------|----------|
| L | pptp1-30 | pptp | 10.10.10.30 | MPPE128 stateless | 10.10.20.30 | 00:01:47 |
| L | pptp2-30 | pptp | 10.10.10.30 | | 10.10.30.30 | 00:00:39 |

- Merupakan tabel informasi session client VPN yang sedang terhubung pada router kita secara realtime
- Kita bisa memutus sebuah session dengan menekan tombol remove (-)
- Flag L : client terautentikasi dari database local secret
- Flag R : client terautentikasi dari database RADIUS

[LAB-2] PPTP Server



[LAB-2] PPTP Server

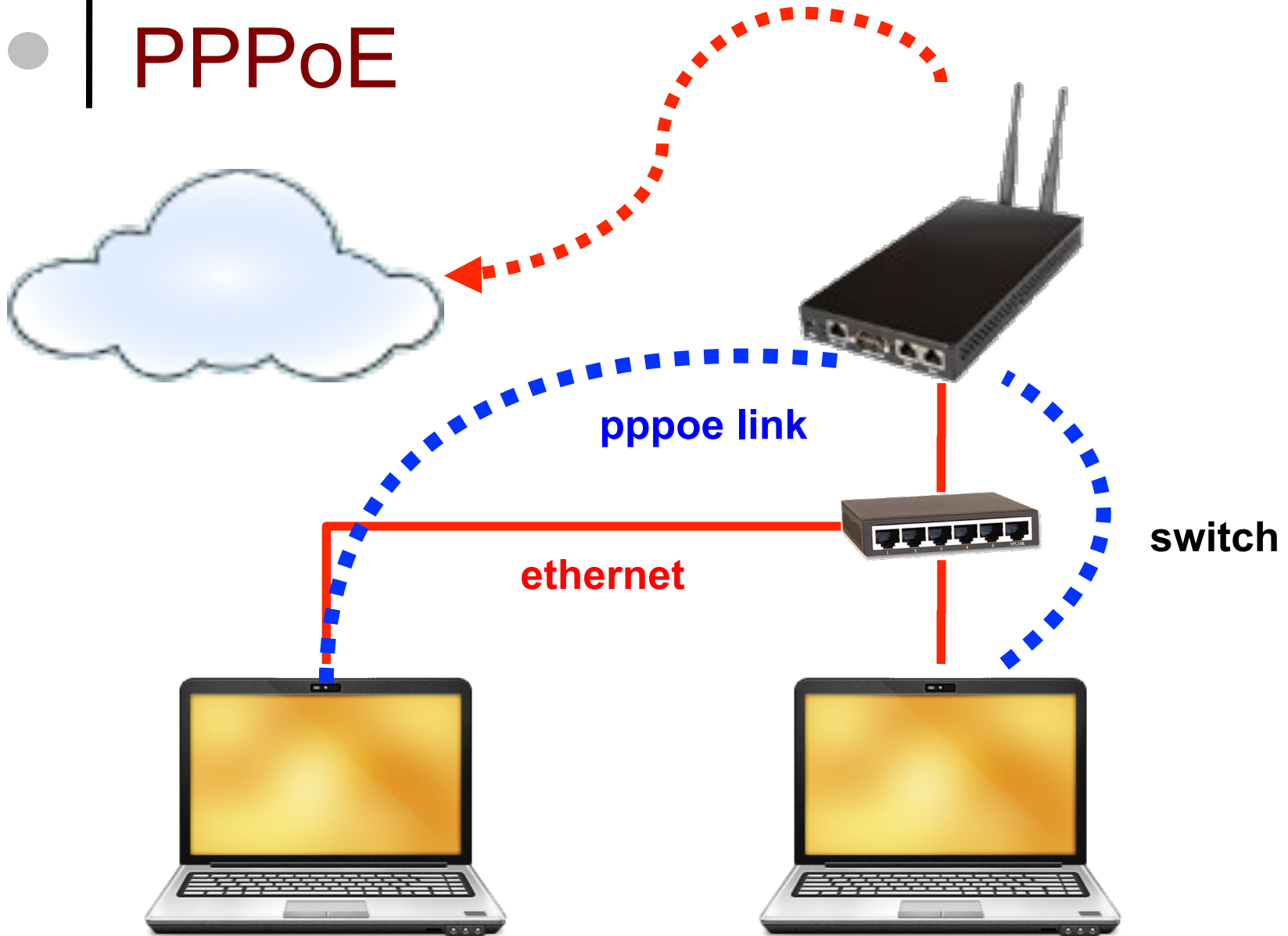
- Disable semua VPN dari LAB-1
- Aktifkan PPTP server di salah satu router, dan router lainnya berfungsi sebagai PPTP client
- Gunakan parameter rate-limit, routes, byte-in dan byte-out disisi server.
- Aktifkan dial on demand disisi client
- Cek ping dan traceroute ke masing-masing network lokal
- Make Backup



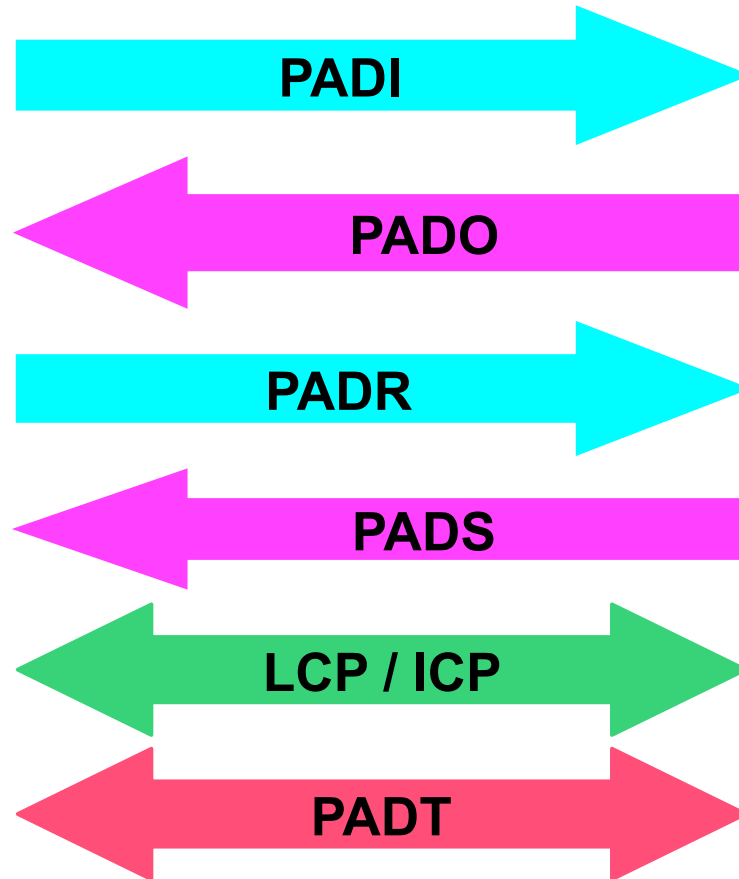
PPPoE

- PPPoE atau Point to Point Protocol over Ethernet merupakan sebuah protocol jaringan pengembangan dari PPP dimana komunikasi datanya dipertukarkan melalui frame ethernet
- PPPoE ini sering digunakan oleh provider untuk memberikan layanan internet broadband via ethernet, modem DSL, wireless bahkan tunnel (EOIP)
- PPPoE ini juga bisa digunakan untuk fitur security pada jaringan ethernet non-managed, untuk pemberian IP hanya bagi client yang sudah melakukan autentikasi, meskipun di interface router secara fisik tidak terpasang IP
- Didalam sebuah interface router bahkan disebuah network, bisa jadi terdapat banyak PPPoE server

PPPoE



PPPoE Discovery

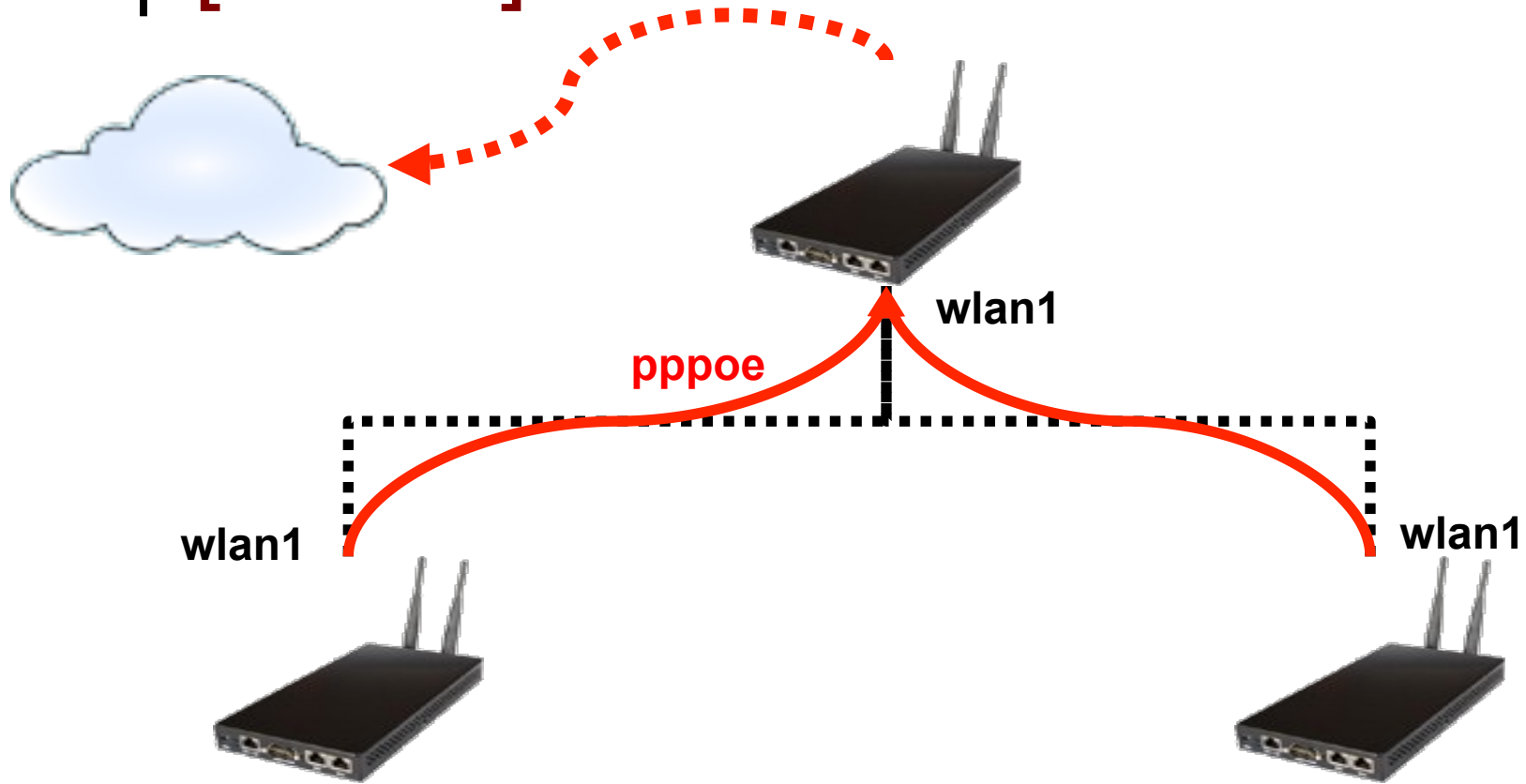




PPPoE Discovery

- Client akan mengirimkan paket Initiation (PADI) ke Ethernet broadcast (dst : FF:FF:FF:FF:FF:FF) yang berisi informasi MAC dari Client dan informasi service-name jika ditentukan
- Ketika server yang memiliki service-name menerima paket PADI, akan mengirimkan paket Offer (PADO) ke client bersangkutan yang memberitahu client ketersediaan service PPPoE
- Client akan mengirimkan paket Request (PADR) ke server yang menandakan client menerima offer untuk melakukan koneksi PPPoE ke server
- Server akan mengirimkan paket Session (PADS) ke client yang menandakan session PPP terbentuk antara router <> client
- LCP / ICP menandakan proses pertukaran informasi username, password dan sebagainya. Jika sudah cocok, maka koneksi PPPoE seutuhnya terbentuk
- PADT (Termination) bisa dikirimkan dari kedua belah pihak yang menandakan pemutusan koneksi

[LAB-3] PPPoE Client



[LAB-3] PPPoE Client

- Buat interface pppoe client di interface wlan1
- PPPoE Client parameter :
 - Username = pppoe-x
 - Password = test
 - Interface = wlan1
 - Add default route = yes
 - Service-name = mikrotik
- Cek IP yang didapatkan
- Tambahkan masquerade untuk out-interface pppoe-x
- Traceroute dari perangkat laptop

[LAB-3] PPPoE Client

- Di router Mikrotik, kita bisa melakukan scanning pppoe server yang tersedia didalam network kita, menggunakan tombol PPPoE scan pada menu PPP-Interface

The screenshot displays the Mikrotik WinBox interface for the PPPoE Scan function. At the top, there are tabs for 'OVPN Server', 'PPPoE Scan', and a 'Find' button. Below the tabs, there is a table with two columns: 'Tx Drops' and 'Rx Drops', both showing a value of 0. The main area of the window is titled 'PPPoE Scan' and features a dropdown menu for 'Interface' currently set to 'wlan1'. To the right of the dropdown are four buttons: 'Start', 'Stop', 'Close', and 'New Window'. At the bottom of the window, there is a table with the following data:

| Service | MAC Address | AC Name |
|-------------------|-------------------|---------|
| mikrotik-training | 02:0C:42:61:B8:1E | ro-tso |

[LAB-3] PPPoE Client

The screenshot displays the Mikrotik WinBox interface for configuring a PPPoE Client. The left sidebar shows the navigation menu with 'PPP' and 'PPPoE Client' highlighted. The main window shows the 'PPP' configuration page with the 'Interface' tab selected. The 'Interface <pppoe-out1>' configuration window is open, showing the following settings:

- Name: pppoe-out1
- Type: PPPoE Client
- L2 MTU: 1480
- Max MTU: 1480
- Max MRU: 1480
- MRRU: (empty)
- Service: mikrotik
- AC Name: (empty)
- User: pppoe-30
- Password: ****
- Profile: default-encryption
- Dial On Demand
- Add Default Route
- Use Peer DNS

The configuration is applied to the interface wlan1. The status bar at the bottom shows the interface is disabled and running.

PPPoE Server

The screenshot displays the Mikrotik WinBox interface for configuring a PPPoE server. On the left sidebar, the 'PPP' menu is highlighted. The main window shows the 'PPP' configuration page with the 'PPPoE Servers' tab selected. A 'New PPPoE Service' dialog box is open, showing the following configuration:

- Service Name: service1
- Interface: ether2
- Max MTU: 1480
- Max MRU: 1480
- MRRU: (empty)
- Keypalive Timeout: 10
- Default Profile: default
- One Session Per Host
- Max Sessions: (empty)
- Authentication options:
 - pap
 - chap
 - mschap1
 - mschap2

The dialog box is set to 'enabled' at the bottom. Red arrows indicate the navigation path: from the 'PPP' menu to the 'New' button, then to the 'PPPoE Servers' tab, and finally to the 'New PPPoE Service' dialog.



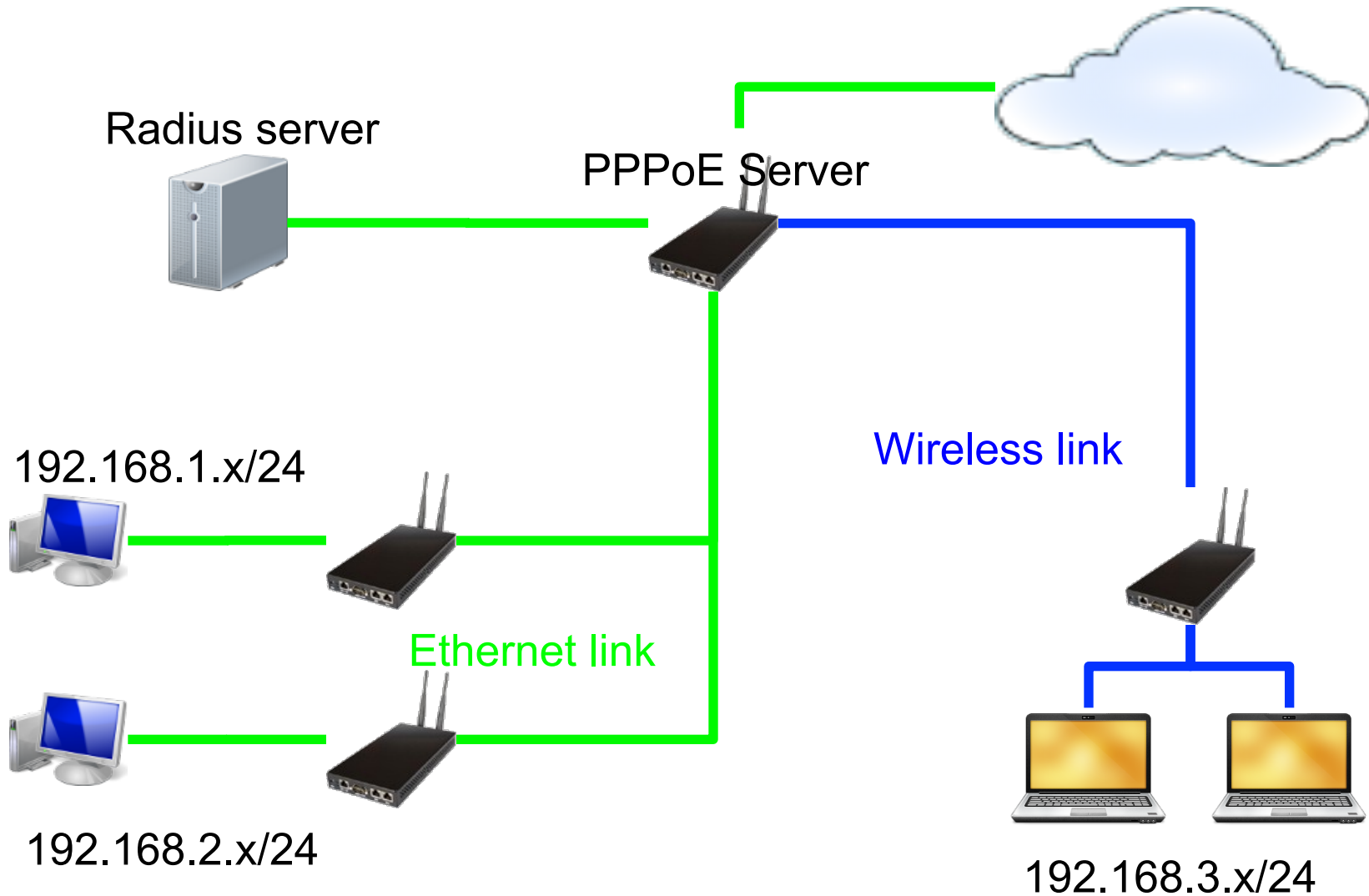
PPPoE Server

- Service Name : Nama dari service PPPoE server
- Interface : Interface untuk mendengarkan request PPPOE dari client
- MTU MRU : Besar paket untuk dikirimkan / diterima setelah dikurangi header (8 bytes)
- Keepalive Timeout : Interval pengecekan yang dilakukan router terhadap client
- Default profile : Penggunaan group untuk client
- One Session per host : Hanya 1 MAC address dalam sebuah session / login
- Maximal Session : Berapa banyak user active dalam 1 server
- Authentication : Metode pengiriman informasi username dan password

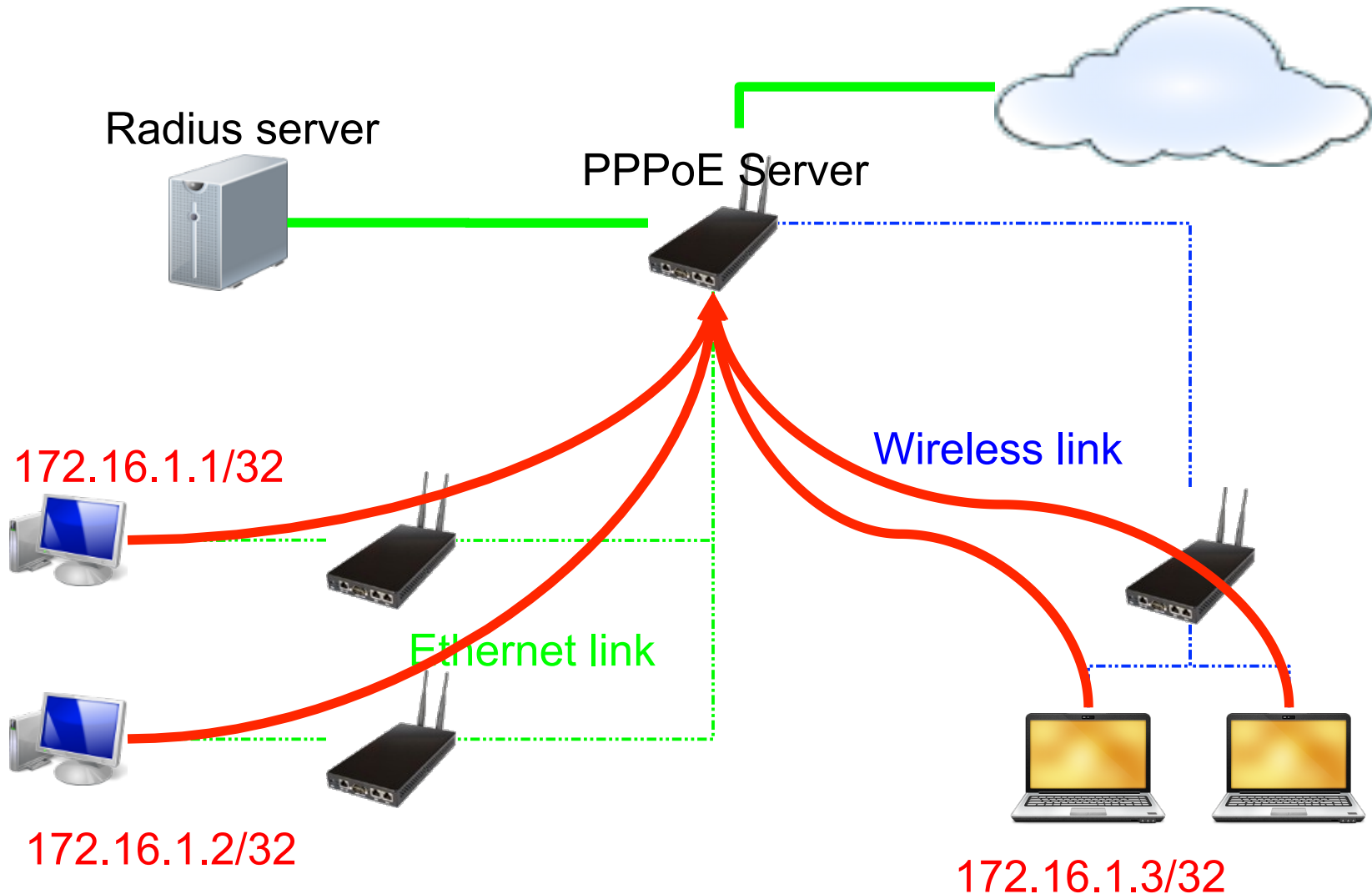
[LAB-4] PPPoE Server

- Aktifkan PPPoE server di interface Ether2 dengan service-name meja-x
- Tambahkan secret untuk koneksi PPPoE dari laptop
- Set laptop menggunakan IP DHCP dan buatlah koneksi PPPoE dari laptop
- Cek koneksi PPPoE anda menggunakan traceroute
- Make Backup

PPPoE Large Network



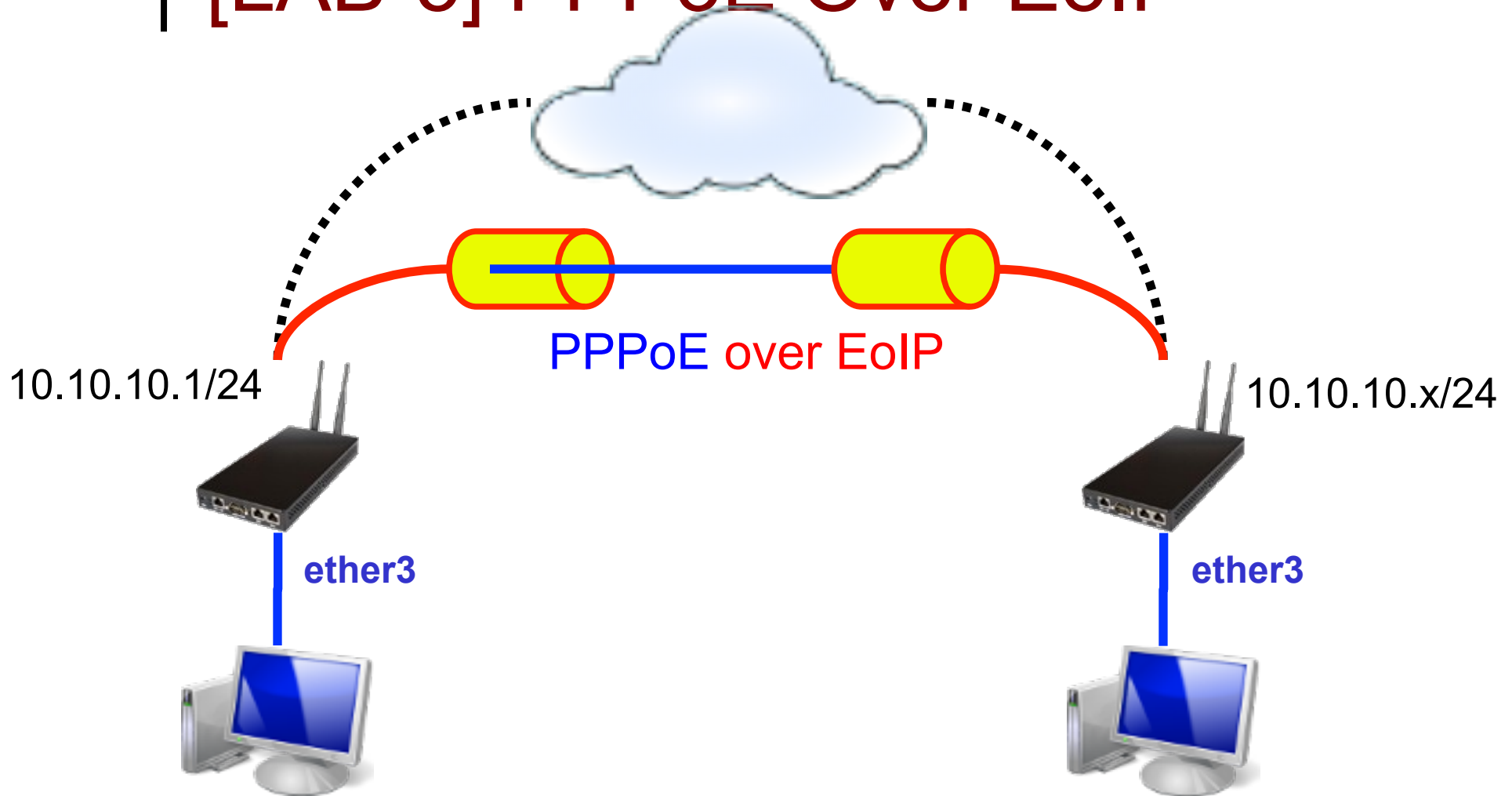
PPPoE Large Network



PPPoE Large Network

- Paket initiate (PADI) yang berasal dari client hanya bisa terbaca dalam sebuah broadcast network.
- Apabila jaringan kita sudah bertambah besar bisa jadi antara client dengan PPPoE server terdapat perangkat router lainnya (misalnya wireless router)
- Untuk jaringan skala besar kita bisa menggunakan beberapa metode
 - 1. Di masing-masing router melakukan bridging antara interface client dengan interface yang mengarah ke PPPoE server → Resiko broadcast !!
 - 2. Di masing-masing router membuat tunnel ke PPPoE server dan kemudian di bridge antara interface client dengan interface tunnel tersebut.

[LAB-5] PPPoE Over EoIP



[LAB-5] PPPoE Over EoIP

- Buat EoIP di kedua router
- Buat interface bridge dengan port ether3 dan EoIP
- Aktifkan PPPoE server di interface bridge dengan service-name meja-x
- Tambahkan secret untuk koneksi PPPoE dari laptop sebelah
- Lakukan dial dari masing-masing laptop ke PPPoE server yang sudah dibuat, test dengan merubah-rubah service-name
- Cek MTU yang bisa dilewatkan untuk PPPoE over EoIP



BCP & MLPPP



Certified Mikrotik Training - Advanced Class (MTCUME)

Organized by: Citraweb Nusa Infomedia

(Mikrotik Certified Training Partner)



Outline

- BCP Concept
- BCP Implementation
- PPTP + BCP LAB
- MLPPP Concept
 - MLPPP Single Link
 - MLPPP Multi Link
- MLPPP Implementation LAB

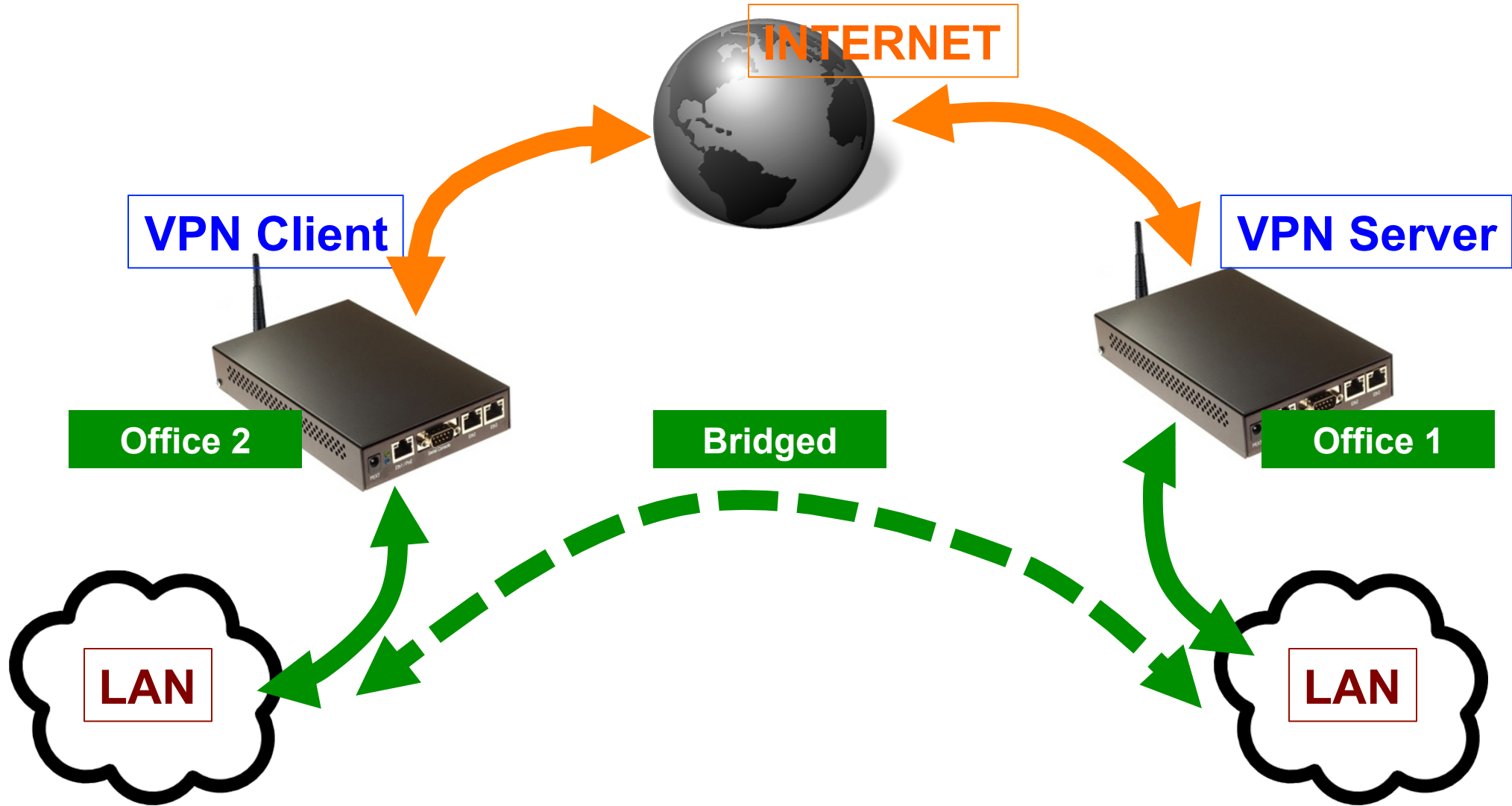
BCP (Bridge Control Protocol)

- BCP adalah sebuah mekanisme bridging yang bisa diimplementasikan di protocol PPP (PPTP, L2TP dan PPPoE).
- Dengan mengimplementasikan BCP ini maka memungkinkan untuk melakukan pengiriman frame ethernet ke dalam koneksi PPP.
- BCP Tidak berhubungan dengan ip address yang digenerate dari ppp
- Dengan kata lain, proses routing dan bridging pada link PPP ini berjalan sendiri-sendiri secara independen pada waktu bersamaan.
- Implementasi BCP ini bisa menjadi alternatif ketika kita menggunakan EoIP + VPN.

BCP Requirement

- Supaya BCP ini bisa dilakukan maka pada PPP server dan PPP Client harus sama-sama support BCP.
- BCP bisa dilakukan di link PPP sesama Mikrotik dan juga link PPP vendor lain asal perangkat vendor lain tersebut juga sudah support protocol standart BCP.

BCP Example



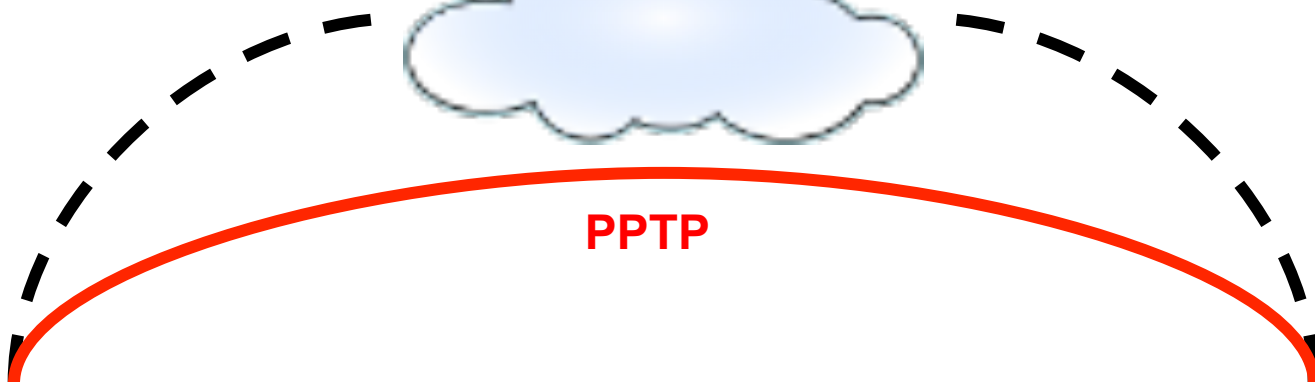


BCP Example

- Dari contoh gambar diatas, ada suatu kondisi dimana dibutuhkan menghubungkan jaringan local dari kedua site (yang terpisah secara geografis) menjadi satu segmen network yang sama.
- Tidak hanya menjadi satu segmen network tetapi link interkoneksinya juga dibutuhkan enkripsi supaya aman.
- Karena ada kebutuhan security maka kita menggunakan VPN (PPTP).

[LAB-1]

BCP Lab



Bridged

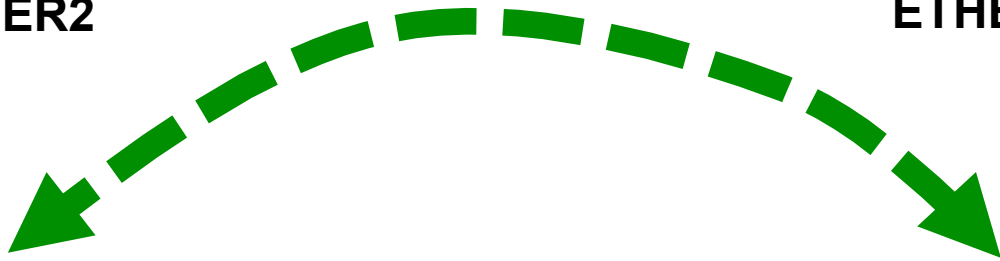
ETHER2

ETHER2



172.16.1.X/24

172.16.1.2/24



[LAB-1] BCP Lab

- Buat interface bridge dan isikan MAC ADDRESS dari interface bridge sesuai mac-address dari ether2
- Aktifkan RSTP Mode !!
- Tambahkan interface ether2 ke dalam Bridge port
- Atur di profile PPP untuk menggunakan BCP Bridging
- Aktifkan PPTP Client dan Server
- Cek di menu Bridge port jika PPTP sudah terbentuk
- Set Laptop menggunakan IP 1 segment dan pasangkan di interface ether2
- Lakukan Test Ping antar laptop

[LAB-1] Create Bridge

R1 dan R2

The screenshot displays the Mikrotik WinBox interface for creating a bridge. On the left sidebar, the 'Bridge' menu item is highlighted with a red box. An arrow points from this menu to a '+' icon in the 'Bridge' window, which is also highlighted with a red box. Below this, the configuration for 'Interface <bridge1>' is shown. The 'Name' is 'bridge1', 'Type' is 'Bridge', 'MTU' is '1500', 'L2 MTU' is '65535', and 'MAC Address' is '00:0C:42:95:14:6E'. The 'Admin. MAC Address' field is highlighted with a red box. An arrow points from this field to the 'MAC Address' field of the 'Interface <ether2>' configuration window on the right, which is also highlighted with a red box. Below the bridge configuration, the 'Protocol Mode' is set to 'rstp', which is also highlighted with a red box.

| Name | Type | L2 MTU | Tx | Rx | Tx Pac... | Rx Pac... | Tx D |
|---------|--------|--------|-------|-------|-----------|-----------|------|
| bridge1 | Bridge | 65535 | 0 bps | 0 bps | 0 | 0 | |

Interface <bridge1> Configuration:

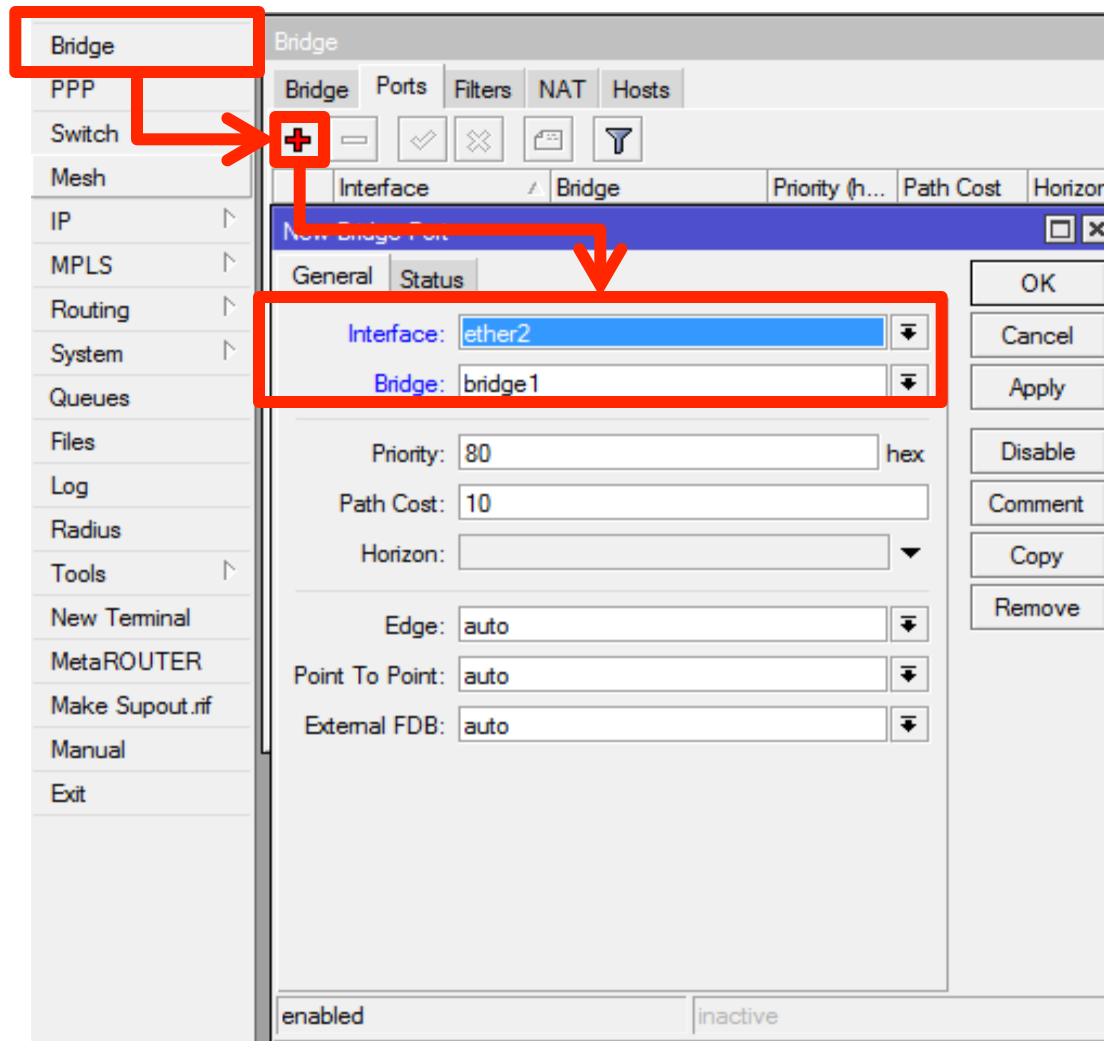
- Name: bridge1
- Type: Bridge
- MTU: 1500
- L2 MTU: 65535
- MAC Address: 00:0C:42:95:14:6E
- Admin. MAC Address: 00:0C:42:95:14:6E
- Protocol Mode: none stp rstp

Interface <ether2> Configuration:

- Name: ether2
- Type: Ethernet
- MTU: 1500
- L2 MTU: 1522
- Max L2 MTU: 1522
- MAC Address: 00:0C:42:95:14:6E
- ARP: enabled

[LAB-1] Bridge Port Config

R1 dan R2



[LAB-1] PPP Profile Config

R1 dan R2

The screenshot displays the Mikrotik WinBox interface for configuring a PPP profile. On the left sidebar, the 'Bridge' option is highlighted. The main window shows the 'PPP' configuration page with the 'Profiles' tab selected. A table lists existing profiles, and a '+' icon is used to add a new one. A dialog box titled 'PPP Profile <pptp-bridge>' is open, showing the configuration for a new profile. The 'Name' field is set to 'pptp-bridge', and the 'Bridge' dropdown is set to 'bridge1'. The 'Local Address' and 'Remote Address' fields are currently empty.

| Name | Local Address | Remote Address | Bridge |
|-------------|---------------|----------------|---------|
| pptp-bridge | | | bridge1 |

PPP Profile <pptp-bridge>

General Protocols Limits

Name: pptp-bridge

Local Address: []

Remote Address: []

Bridge: bridge1

OK Cancel Apply Comment Copy

[LAB-1] Server Config

The image shows the configuration process for a PPTP server in Mikrotik WinBox. The main window is titled 'PPP' and has several tabs: 'Interface', 'PPPoE Servers', 'Secrets', 'Profiles', and 'Active Connections'. A red box highlights the 'Interface' tab, and another red box highlights the 'PPTP Server' button. Below this, the 'PPTP Server' dialog is open, showing the following settings:

- Enabled
- Max MTU: 1460
- Max MRU: 1460
- MRRU: [empty]
- Keepalive Timeout: 30
- Default Profile: default-encryption
- Authentication:
 - pap
 - chap
 - mschap1
 - mschap2

To the right, the 'PPP Secret <user31>' dialog is open, showing the following settings:

- Name: user31
- Password: [masked]
- Service: any
- Caller ID: [empty]
- Profile: pptp-bridge
- Local Address: [empty]
- Remote Address: [empty]
- Routes: [empty]
- Limit Bytes In: [empty]
- Limit Bytes Out: [empty]
- Comment: [empty]

Red arrows indicate the flow of configuration from the main window to the PPTP Server dialog and then to the PPP Secret dialog.

Server Side

[LAB-1] Client Config

Client Side

The screenshot displays the Mikrotik WinBox configuration interface for a PPP Client. The main window is titled "Interface <pptp-out1>" and is currently on the "Dial Out" tab. The configuration includes:

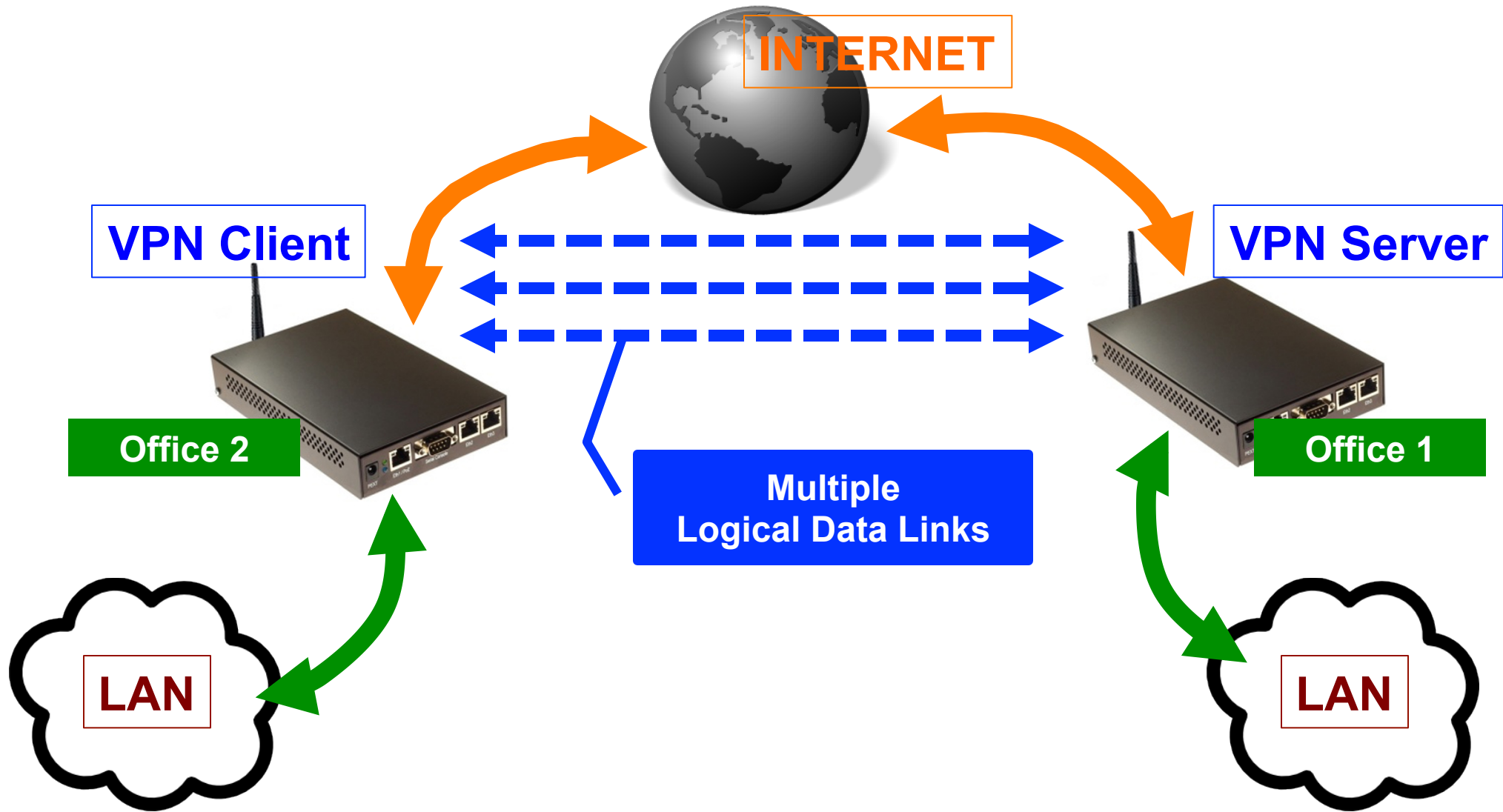
- Connect To:** 10.10.10.30
- User:** user31
- Password:** ****
- Profile:** pptp-bridge
- Allow:** pap, mschap1, chap, mschap2
- Options:** Dial On Demand, Add Default Route

The status bar at the bottom indicates the interface is "enabled", "running", and "slave", with a "Status: connected".

MLPPP

- Multi-Link Point to Point Protocol (MLPPP, Multi-Link PPP, MultiPPP or MLPPP) adalah sebuah protocol yang memungkinkan untuk melakukan pemisahan, penggabungan, dan pengurutan data di beberapa Logical Data Link di koneksi PPP tersebut.
- Ketika kondisinya sudah ada link PPP dan kita ingin menambah besar kapasitas link (MTU) maka kita bisa menggunakan teknik MLPPP ini tanpa harus mengganti atau menambah perangkat.
- Ketika ada paket besar yang dikirimkan maka akan dipecah secara merata ke beberapa Logical Data Link

MLPPP Example



● ● ● | MLPPP Example

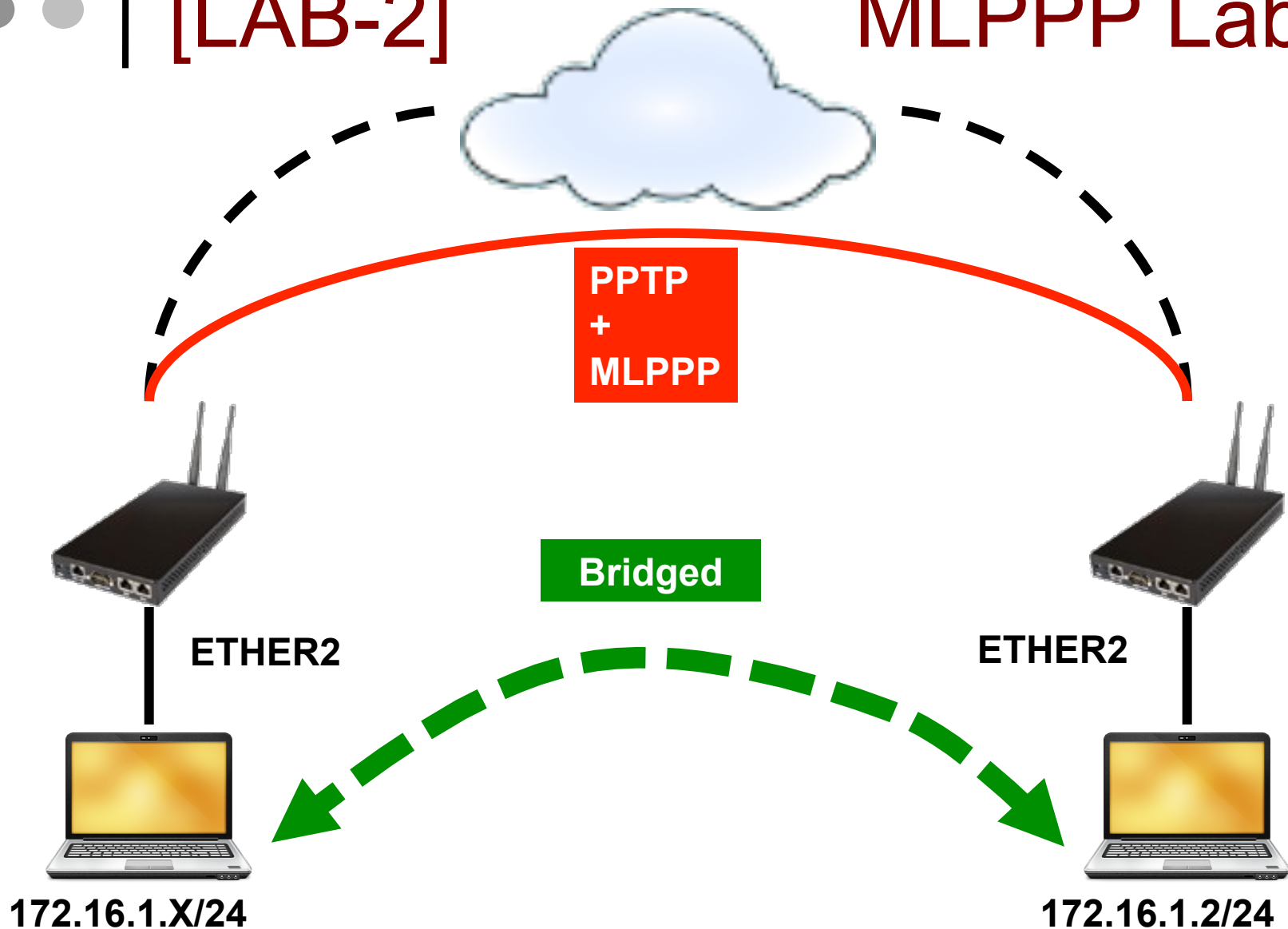
- Biasanya ukuran paket yang dikirim melalui link PPP berkurang (terjadi fragmentasi) karena overhead disebabkan PPP Header.
- MP (Multilink Protocol) dapat digunakan untuk mengirim dan menerima Ethernet full frame melalui link Tunggal (MLPPP over single link) ataupun Multiple (MLPPP over multiple link).
- Yang dibutuhkan oleh Protokol Multilink adalah menggunakan Opsi tambahan LCP yaitu Multilink Maximum Received Reconstructed Unit (MRRU)

● ● ● | MLPPP over Single Link

- Untuk mengaktifkan multi-link PPP over single link Anda harus menentukan MRRU.
- Jika kedua perangkat mendukung fitur ini maka tidak ada kebutuhan MSS adjustment (dalam mangle firewall).
- Studi menunjukkan bahwa penyesuaian MRRU lebih efisien di CPU dibandingkan dengan jika menggunakan 2 mangle change MSS per klien.
- MRRU memungkinkan untuk membagi paket ke beberapa logical link sehingga meningkatkan MTU dan MRU (sampai max 65.535 byte)

[LAB-2]

MLPPP Lab



● ● ● | [LAB-2] MLPPP Over Single Link

- Atur ulang parameter MRRU pada Server dan Client
- Lakukan Test Ping antar laptop packet size 1500 no-fragmented (bisa / tidak)

[LAB-2] Configure MRRU - Server

The image displays three overlapping windows from the Mikrotik WinBox interface:

- Main Window:** Shows the 'PPP' configuration menu with the 'PPTP Server' tab selected. A red box highlights the 'PPTP Server' tab, and a red arrow points to it from the 'Interface' tab.
- PPTP Server Window:** Shows the configuration for a PPTP server. The 'Enabled' checkbox is checked. The 'Max MTU' is 1460, 'Max MRU' is 1460, and 'MRRU' is 1600 (highlighted with a red box). The 'Keepalive Timeout' is 30, and the 'Default Profile' is 'default-encryption'. Authentication options include 'pap', 'chap', 'mschap1' (checked), and 'mschap2' (checked). Buttons for 'OK', 'Cancel', and 'Apply' are visible.
- PPP Secret <user31> Window:** Shows the configuration for a user secret. The 'Name' is 'user31', 'Password' is masked with '****', 'Service' is 'any', and 'Profile' is 'pptp-bridge' (highlighted with a red box). Other fields include 'Caller ID', 'Local Address', 'Remote Address', 'Routes', 'Limit Bytes In', and 'Limit Bytes Out'. Buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', and 'Remove' are visible.

Server Side

[LAB-2] Configure MRRU - Client

The screenshot displays the Mikrotik WinBox interface for configuring a PPP client. The left sidebar shows the 'PPP' menu expanded, with 'PPTP Client' selected. The main window shows the configuration for 'Interface <pptp-out1>'. The 'General' tab is active, showing the following settings:

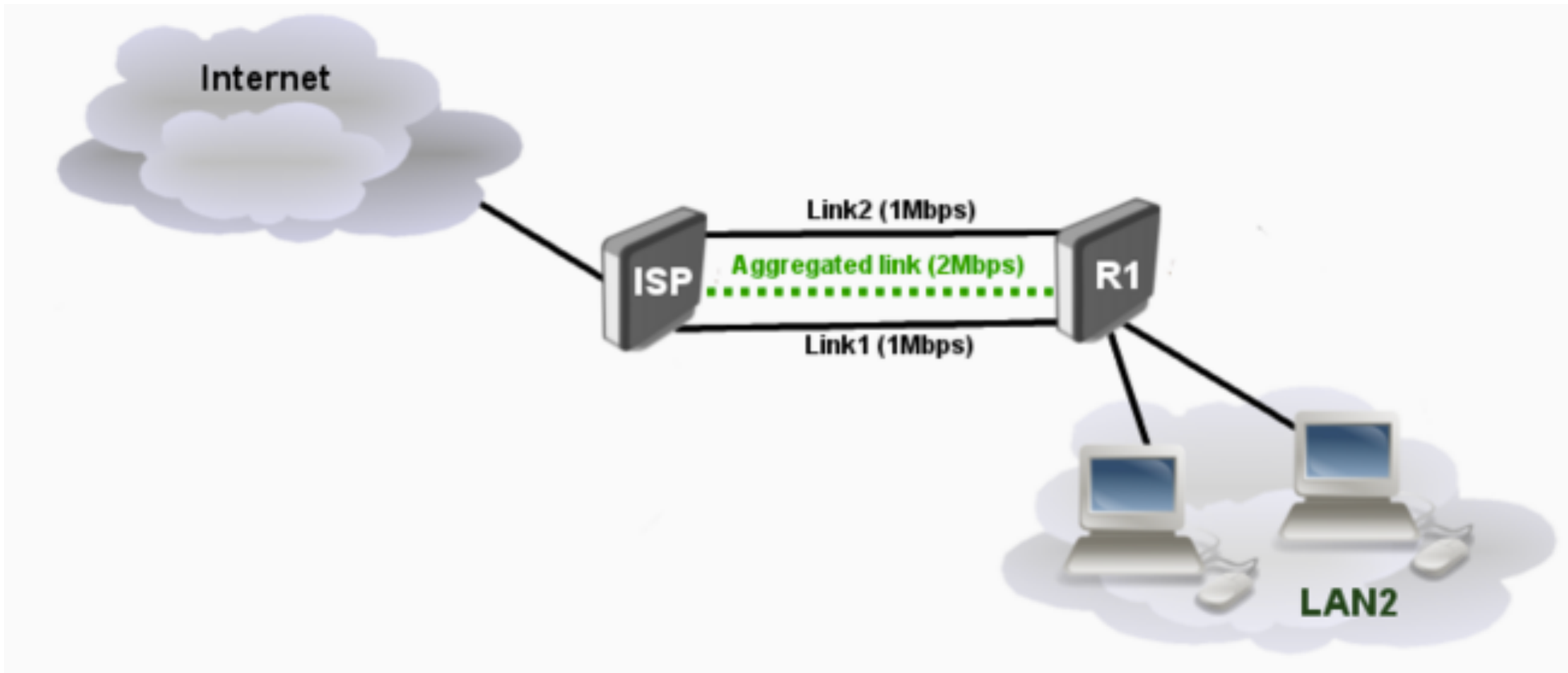
- Name: pptp-out1
- Type: PPTP Client
- L2 MTU: 460
- Max MTU: 460
- Max MRU: 460
- MRRU: 1600

The 'Connect To' field is set to 10.10.10.30. The 'User' field is set to user31, and the 'Profile' is set to pptp-bridge. The 'Allow' section has checkboxes for pap, mschap1, chap, and mschap2, all of which are checked. The 'Client Side' label is visible in the bottom right corner of the configuration window.

MLPPP over Multiple Link

- MLPPP over Multiple Link memungkinkan untuk membuat agregasi link PPP tunggal diatas beberapa koneksi fisik.
- Semua link PPP harus berasal dari server dan client yang sama (server harus sudah support MLPPP) dan semua link PPP harus memiliki username dan password yang sama.
- Untuk konfigurasi MLPPP over Multiple Link hanya perlu membuat klien PPP dan menentukan beberapa interface fisik.
- Mikrotik RouterOS memiliki dukungan MLPPP client mulai dari versi 3.10. Tetapi sampai saat ini belum ada server yang sudah support MLPPP over Multiple Link.

MLPPP over Multiple Link





L2TP & IPSec



Certified Mikrotik Training - Advanced Class (MTCUME)

Organized by: Citraweb Nusa Infomedia

(Mikrotik Certified Training Partner)



Outline

- L2TP vs PPTP
- L2TP Configuration (similar like PPTP)
 - Client
 - Server
- IPSec
- L2TP + IPSec
- Configuration Example

L2TP vs PPTP – PPTP Spec

- Point-to-Point Tunneling Protocol (PPTP), developed by Microsoft in conjunction with other technology companies.
- PPTP Bertugas membuatkan sebuah network tunnel dan menggunakan MPPE (Microsoft Point to Point Encryption) sebagai enkripsinya.
 - Low Overhead, lighter than other VPN
 - Port/rotocol: 1723 TCP and protocol GRE
 - User Authentication Protocol: EAP-TLS or MS-CHAP v2
 - Encryption method: MPPE (Microsoft Point-to-Point Encryption)
 - Encryption Strength: MPPE 40-128 bit

L2TP vs PPTP – L2TP Spec

- The Layer 2 Tunneling Protocol (L2TP) was developed in cooperation between Cisco and Microsoft to combine features of PPTP with those of Cisco's proprietary Layer 2 Forwarding (L2F) protocol.
- L2TP supports pada jaringan non-TCP/IP clients dan protocols (Contoh: Frame Relay, ATM and SONET).
- L2TP tidak memiliki mekanisme enkripsi, biasanya menggunakan protocol enkripsi lain yang lewat didalam tunnelnya.

L2TP vs PPTP – L2TP Spec (2)

- Port: 1701 UDP
- User Authentication Protocol: EAP-TLS or MS-CHAP v2
 - In addition to providing computer-level authentication, IPSec provides end-to-end encryption for data that passes between the sending and receiving nodes.
- Encryption: IPSec
- Encryption Strength: Advanced Encryption Standard (AES) 256, AES 192, AES 128, and 3DES encryption algorithms

L2TP vs PPTP – Conclusion (1)

- + PPTP mudah diimplementasikan
- + PPTP menggunakan TCP, sehingga reliable dan mampu retransmit packet yang rusak / hilang.
- + PPTP sudah disupport berbagai macam OS
- – PPTP tidak terlalu aman karena menggunakan MPPE(up to 128 bit)
- – data encryption baru dilakukan setelah PPP connection selesai diproses.
- – PPTP connections hanya membutuhkan Autentikasi di user-level dan hanya menggunakan PPP authentication protocol

L2TP vs PPTP – Conclusion (2)

- + L2TP/IPSec encryption dilakukan sebelum proses PPP connection.
- + L2TP/IPSec menggunakan AES(up to 256bit) or DES (up to three 56-bit keys)
- + L2TP/IPSec menggunakan mekanisme authentication yang lebih kuat yaitu menggunakan computer-level authentication memanfaatkan SSL certificates ditambah user-level authentication yaitu PPP Protocol authentication.
- + L2TP menggunakan UDP sehingga pengiriman pakatnya lebih cepat. Sayangnya tidak reliable karena tidak ada mekanisme pengiriman ulang paket yang hilang/rusak.
- + L2TP lebih “firewall friendly” dibandingkan PPTP — suatu Keuntungan besar jika menggunakan protocol Extranet ini, karena kebanyakan Firewall tidak mensupport GRE.
- – L2TP/IPSec membutuhkan SSL Certificate yang tidak terlalu familiar bagi pengguna Awam.

L2TP Configuration - Client

The image shows two side-by-side screenshots of the Mikrotik WinBox 'New Interface' configuration window. The left window shows the 'General' tab with the following fields: Name: 2tp-out1, Type: L2TP Client, L2 MTU: (empty), Max MTU: 1460, Max MRU: 1460, and MRRU: (empty). The right window shows the 'Dial Out' tab with the following fields: Server Address: 10.10.10.100, User: userx, Password: test, and Profile: default-encryption. Below the Profile field are two checkboxes: 'Dial On Demand' and 'Add Default Route', both unchecked. At the bottom, there is a section labeled 'Allow' with four checked checkboxes: pap, mschap1, chap, and mschap2. A red box highlights the 'Profile' dropdown menu, and a red line connects it to the text 'Encryption Option - MPPE 128Bit'.

Encryption Option – MPPE 128Bit

Akan menyesuaikan Server

L2TP Configuration - Server

The image shows two configuration windows from Mikrotik WinBox. The left window is titled 'L2TP Server' and has the following settings:

- Status: Enabled
- Max MTU: 1460
- Max MRU: 1460
- MRRU: [empty]
- Default Profile: default-encryption (highlighted with a red box)
- Authentication: pap, mschap1, chap, mschap2

The right window is titled 'New PPP Secret' and has the following settings:

- Name: User-L2TP-1
- Password: test
- Service: l2tp
- Caller ID: [empty]
- Profile: default-encryption (highlighted with a red box)
- Local Address: 172.16.1.1
- Remote Address: 172.16.1.2

A red line connects the 'default-encryption' selection in both windows. A red text label 'Encryption Option - MPPE 128Bit' is positioned above the line, indicating the encryption method associated with this profile.



L2TP Security

- L2TP secara default bisa menggunakan MPPE 128Bit sama seperti yang digunakan pada PPTP.
- Karena MPPE dirasa kurang aman maka L2TP dikembangkan untuk bisa digabungkan dengan protocol security yang lain yaitu **IPSec**.



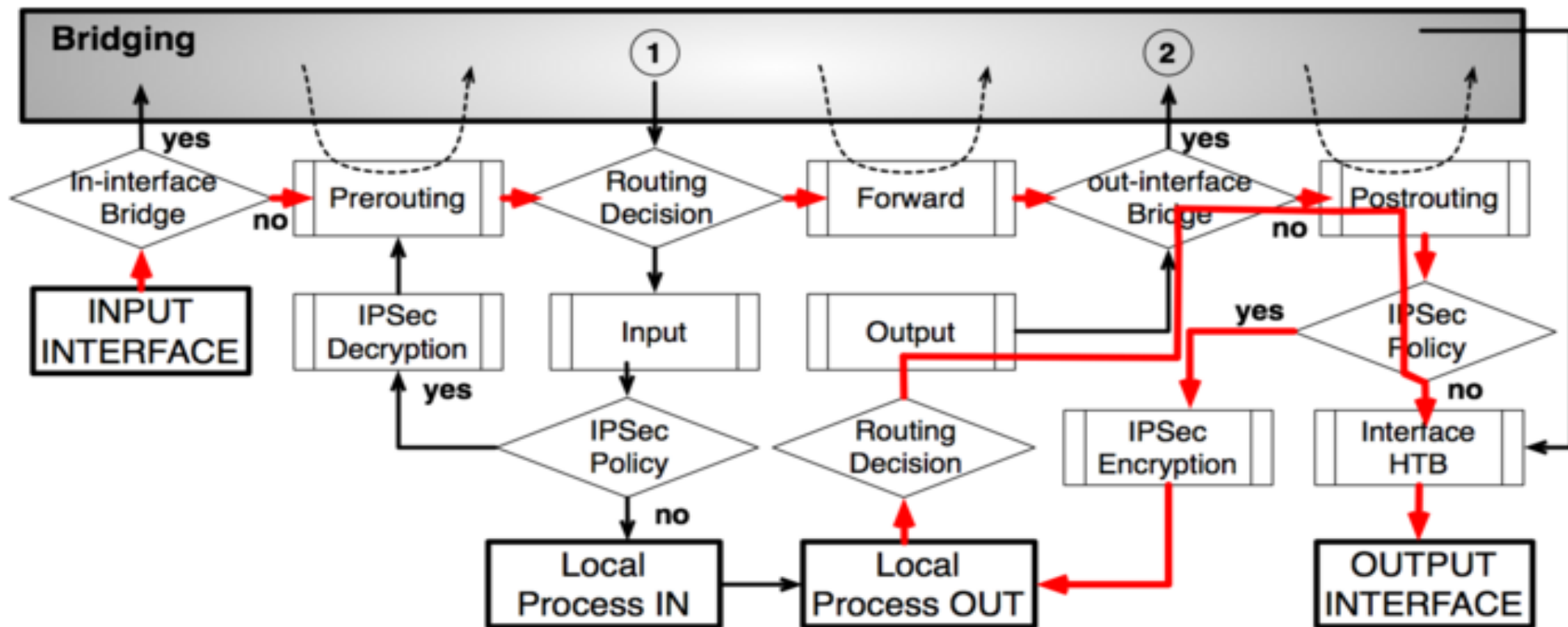
IPsec

- Protocol IPSec (IP Security) mampu mengimplementasikan security (Enkripsi) di komunikasi jaringan TCP/IP (IPv4/IPv6).
- Setiap traffic akan dilakukan dua fase :
 - **Encryption**
 - **Decryption**
- Pada traffic yang menggunakan IPSec, kedua sisi akan memiliki peran atau posisi yang berbeda :
 - **Initiator** – Sebagai sisi yang menentukan encryption policy (metode autentikasi dan enkripsi yang ada di tawarkan - **Proposal**).
 - **Responder** – Perangkat yang menjadi posisi ini akan menyesuaikan metode autentikasi dan enkripsi supaya komunikasi yang terenkripsi dapat dijalankan.
- Selama Perangkat Responder tidak dapat menyamakan metode enkripsi dan autentikasi yang ditawarkan oleh router Initiator maka komunikasi akan di drop.

IPSec Encryption

- Setelah paket terkena proses src-nat tetapi sebelum masuk kedalam interface-queue, paket data akan di hadapkan pada pilihan akan dienkripsi atau tidak berdasarkan database policy dari IPsec yaitu berdasarkan SPD (Security Policy Database).
- SPD memiliki dua bagian :
 - **Packet Matching** – daftar dari src/dst address, protocol dan port (TCP dan UDP) dari traffic yang akan dienkripsi.
 - **Action** – Jika rule dengan type data mengalami kecocokan maka :
 - **Accept** – paket akan diteruskan tanpa ada proses enkripsi
 - **Drop** – paket akan di drop
 - **Encrypt** – paket data akan dilakukan proses Enkripsi
- Database policy (SPD) bisa berupa kombinasi dari implementasi security yaitu dari beberapa metode enkripsi seperti key, algoritma.

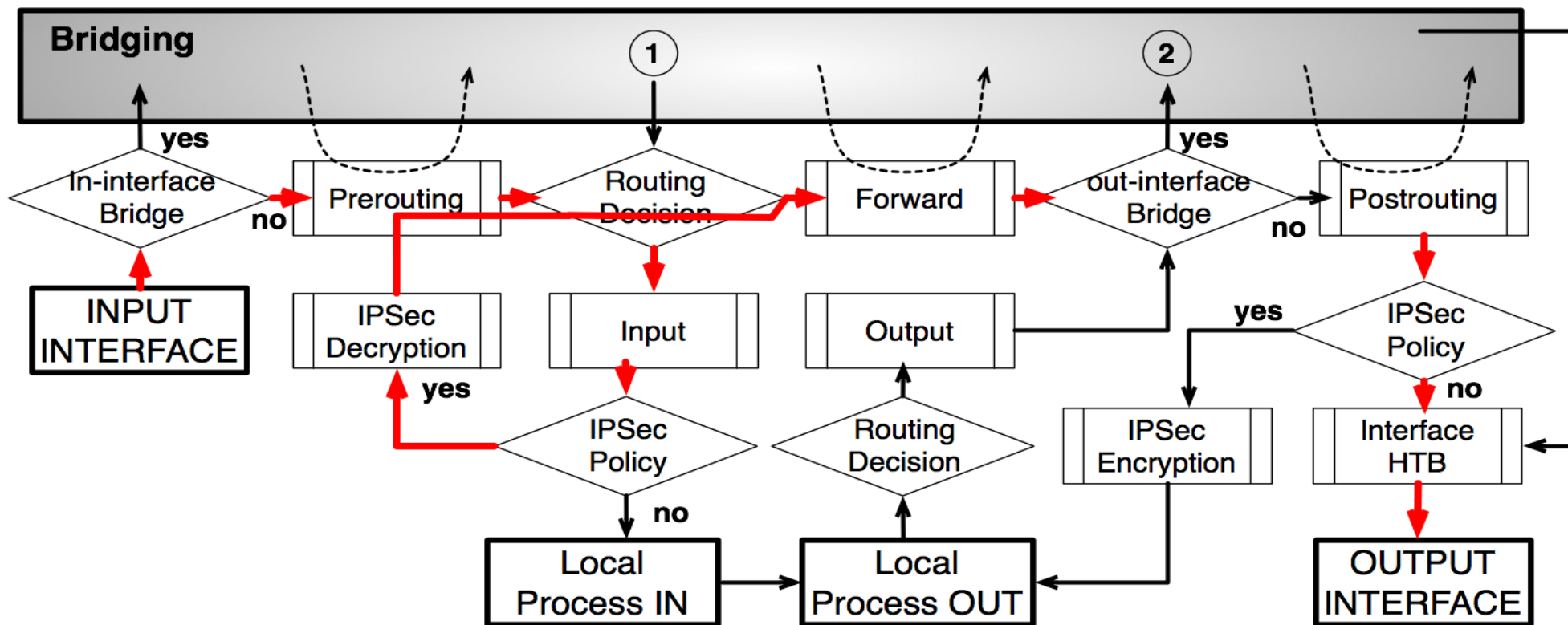
IPSec – Flow (encryption)



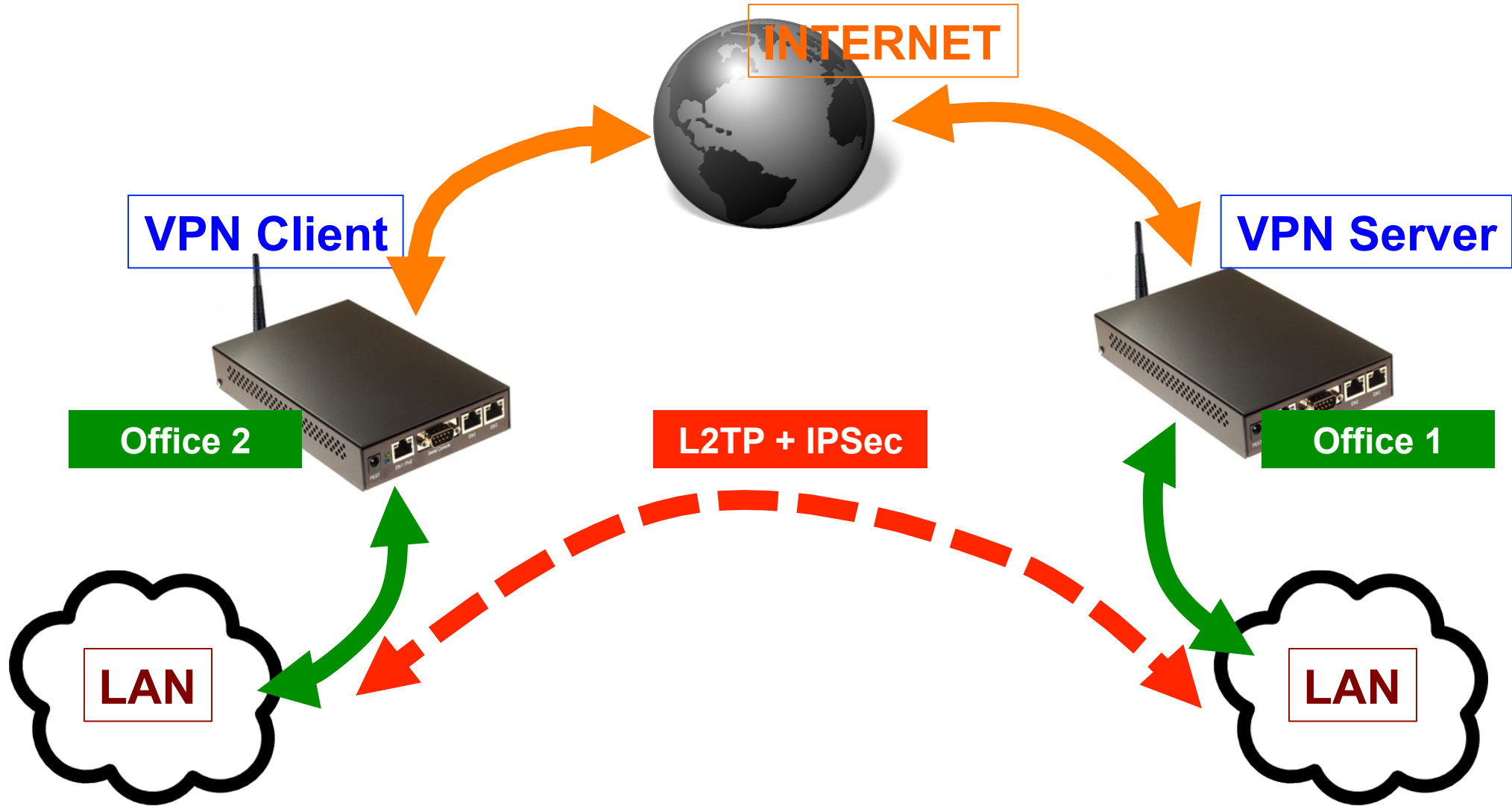
IPSec Decryption

- Jika paket yang terkena enkripsi diterima oleh router host (setelah **dst-nat** dan **filter Input**), maka router akan mencocokkan metode enkripsi dari paket untuk melakukan proses Dekripsi.
- Jika metode tidak ditemukan maka paket akan di drop tetapi jika ditemukan maka paket akan didekripsi.
- Jika proses dekripsi berjalan lancar paket akan kembali dimasukkan melewati **dst-nat** dan **routing** table untuk kembali didistribusikan ketujuan yang asli.
- Sedikit catatan dimana paket berada sebelum chain **forward** dan **input** paket akan dihadapkan lagi ke SPD dan dicocokkkan kembali jika masih memerlukan enkripsi maka paket akan di drop. Proses ini disebut Incoming Policy Check.

IPSec – Flow (decryption)



L2TP + IPSec Example



Server : Create L2TP Server & Secret

L2TP Server

Enabled

Max MTU: 1460

Max MRU: 1460

MRRU: ▼

Default Profile: default ▼

— Authentication —

pap

chap

mschap1

mschap2

PPP Secret <L2TP-IPSec-1>

Name: L2TP-IPSec-1

Password: test ▲

Service: any ▼

Caller ID: ▼

Profile: default ▼

Local Address: 172.16.1.1 ▲

Remote Address: 172.16.1.2 ▲

Remote IPv6 Prefix: ▼

Server : Add Interface – L2TP Server

Interface <L2TP-IPSec-in-1 >

| General | Status | Traffic |
|---------|----------------------------------------------|---------|
| Name: | <input type="text" value="L2TP-IPSec-in-1"/> | |
| Type: | <input type="text" value="L2TP Server"/> | |
| L2 MTU: | <input type="text"/> | |
| User: | <input type="text" value="L2TP-IPSec-1"/> | |

Server : Create IPsec Policy

IPsec Policy <192.168.130.0/24:0->192.168.30.0/24:0>

| General | Action |
|---------------|------------------|
| Src. Address: | 192.168.130.0/24 |
| Src. Port: | |
| Dst. Address: | 192.168.30.0/24 |
| Dst. Port: | |
| Protocol: | 255 (all) |

| General | Action |
|--------------------------------------------|------------|
| Action: | encrypt |
| Level: | require |
| IPsec Protocols: | esp |
| <input checked="" type="checkbox"/> Tunnel | |
| SA Src. Address: | 172.16.1.1 |
| SA Dst. Address: | 172.16.1.2 |
| Proposal: | default |
| Priority: | 0 |

Server : Create IPsec Peer

IPsec Peer <172.16.1.2>

Address: 172.16.1.2

Port: 500

Auth. Method: pre shared key

Secret: testing

Exchange Mode: main

Send Initial Contact

NAT Traversal

My ID User FQDN:

Proposal Check: obey

Hash Algorithm: sha

Encryption Algorithm: 3des

DH Group: modp1024

Generate Policy

Lifetime: 1d 00:00:00

Lifeytes:

DPD Interval: disable DPD

DPD Maximum Failures: 1

Client : Create L2TP-Client

Interface <l2tp-out1 >

General Dial Out Status Traffic

Server Address: 10.10.10.100

User: L2TP-IPSec-1

Password: test ▲

Profile: default ▼

Dial On Demand

Add Default Route

— Allow —

pap chap

mschap1 mschap2

Client : Create IPsec Policy

IPsec Policy <192.168.30.0/24:0->192.168.130.0/24:0>

General

Action

Src. Address: 192.168.30.0/24

Src. Port:

Dst. Address: 192.168.130.0/24

Dst. Port:

Protocol: 255 (all)

General

Action

Action: encrypt

Level: require

IPsec Protocols: esp

Tunnel

SA Src. Address: 172.16.1.2

SA Dst. Address: 172.16.1.1

Proposal: default

Priority: 0

Client : Create IPsec Peer

IPsec Peer <172.16.1.1>

Address: 172.16.1.1

Port: 500

Auth. Method: pre shared key

Secret: testing

Exchange Mode: main

Send Initial Contact

NAT Traversal

My ID User FQDN:

Proposal Check: obey

Hash Algorithm: sha

Encryption Algorithm: 3des

DH Group: modp1024

Generate Policy

Lifetime: 1d 00:00:00

Lifeytes:

DPD Interval: disable DPD

DPD Maximum Failures: 1

IPsec

Policies Peers Remote Peers Proposals I

Kill Connections

| Local Address | Remote Address |
|---------------|----------------|
| 172.16.1.2 | 172.16.1.1 |

IPsec Remote Peer <172.16.1.1>

Local Address: 172.16.1.2

Remote Address: 172.16.1.1

Side: responder

Established: 00:00:47

PH2 Active: 0

PH2 Total: 0

established

CLIENT

IPsec

Policies Peers Remote Peers Proposals I

Kill Connections

| Local Address | Remote Address |
|---------------|----------------|
| 172.16.1.1 | 172.16.1.2 |

IPsec Remote Peer <172.16.1.2>

Local Address: 172.16.1.1

Remote Address: 172.16.1.2

Side: initiator

Established: 00:02:01

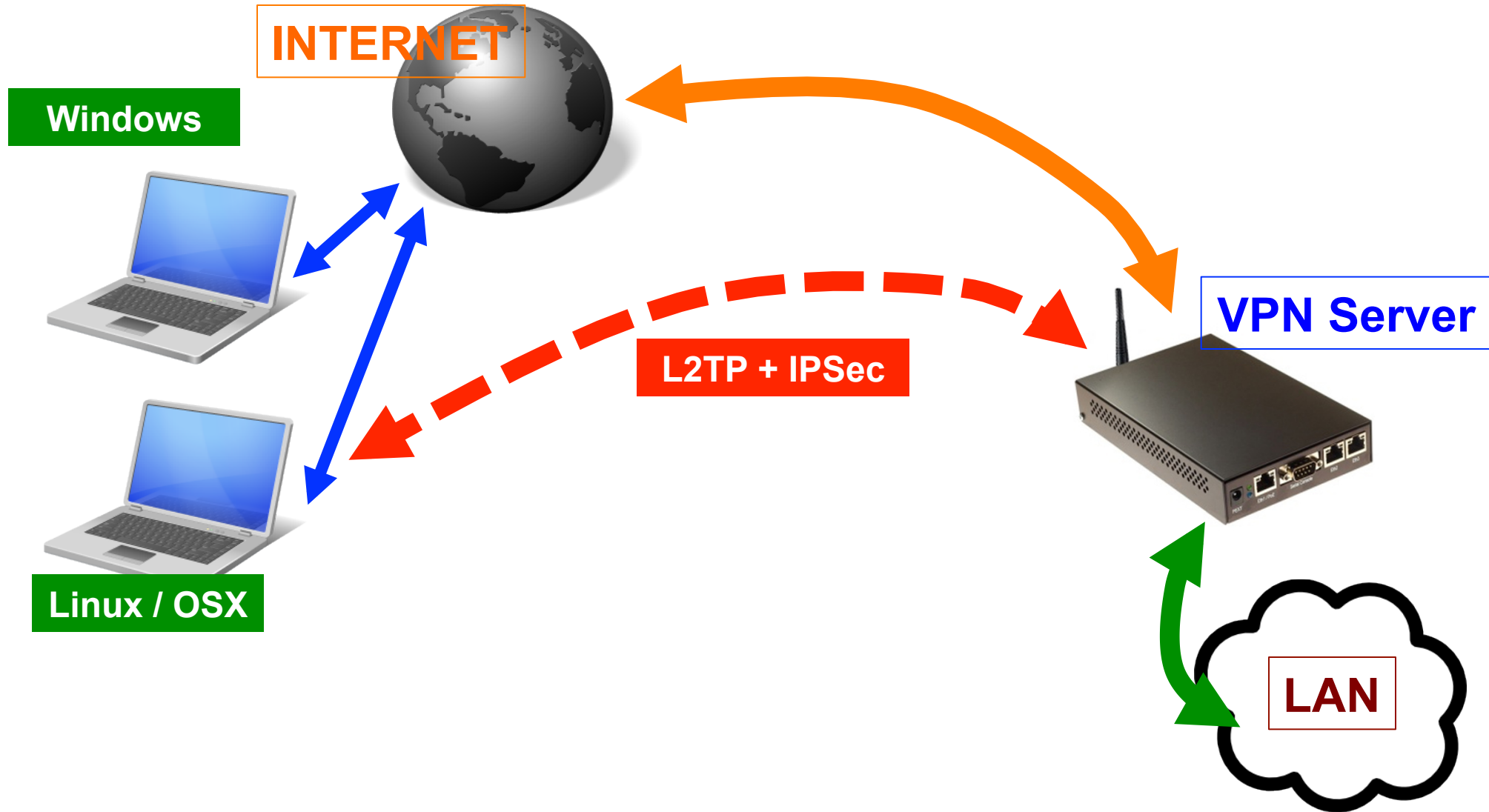
PH2 Active: 0

PH2 Total: 0

established

SERVER

L2TP/IPSec vs Windows/OSX



Server : Create New Secret

PPP Secret <L2TP-IPSec-2>

| | |
|-----------------|-------------------------------------------|
| Name: | <input type="text" value="L2TP-IPSec-2"/> |
| Password: | <input type="text" value="test"/> ▲ |
| Service: | <input type="text" value="any"/> ▼ |
| Caller ID: | <input type="text" value=""/> ▼ |
| Profile: | <input type="text" value="default"/> ▼ |
| Local Address: | <input type="text" value="172.21.1.1"/> ▲ |
| Remote Address: | <input type="text" value="172.21.1.2"/> ▲ |

Server : Create New Peer

IPsec Peer <0.0.0.0/0>

Address: 0.0.0.0/0

Port: 500

Auth. Method: pre shared key

Secret: testing-1

Lifetime: 1d 00:00:00

Lifeytes:

DPD Interval: 120 s

DPD Maximum Failures: 5

Exchange Mode: main l2tp

Send Initial Contact

NAT Traversal

My ID User FQDN:

Proposal Check: obey

Hash Algorithm: sha

Encryption Algorithm: 3des

DH Group: modp1024

Generate Policy

Windows : Create L2TP Client

Change your networking settings



Set up a new connection or network
Set up a wireless, broadband, dial-up,



Connect to a workplace
Set up a dial-up or VPN connection to your workplace.

→ Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.

Determine Server Address

Your network administrator can give you this address.

Internet address:

192.168.130.161

Destination name:

VPN Connection

Type your user name and password

User name:

L2TP-IPSec-2

Password:

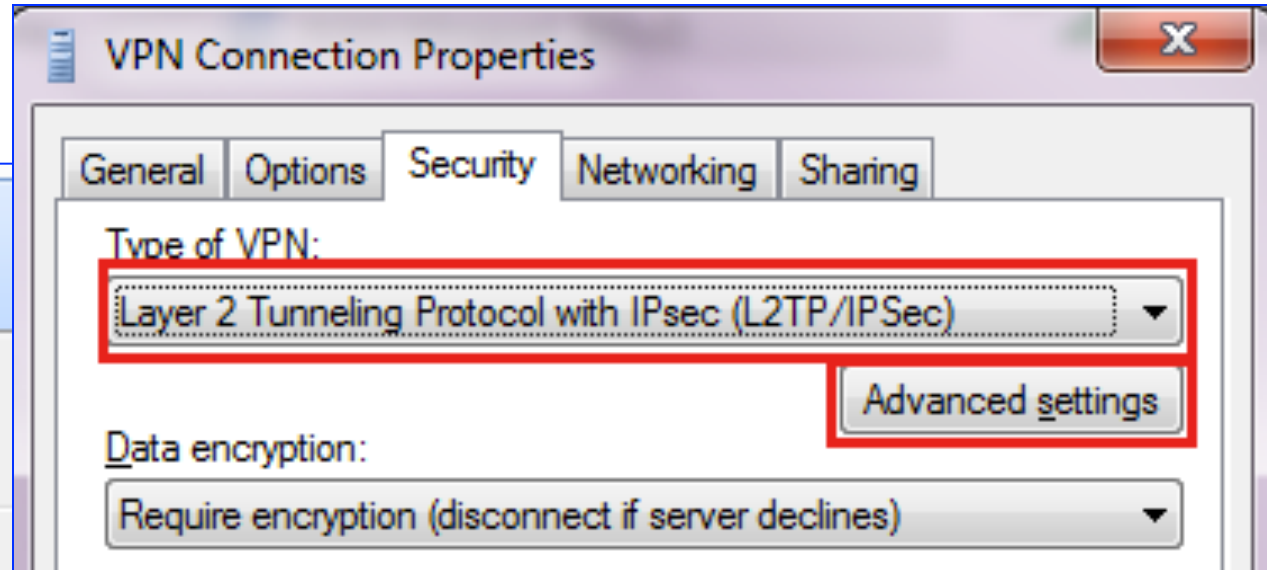
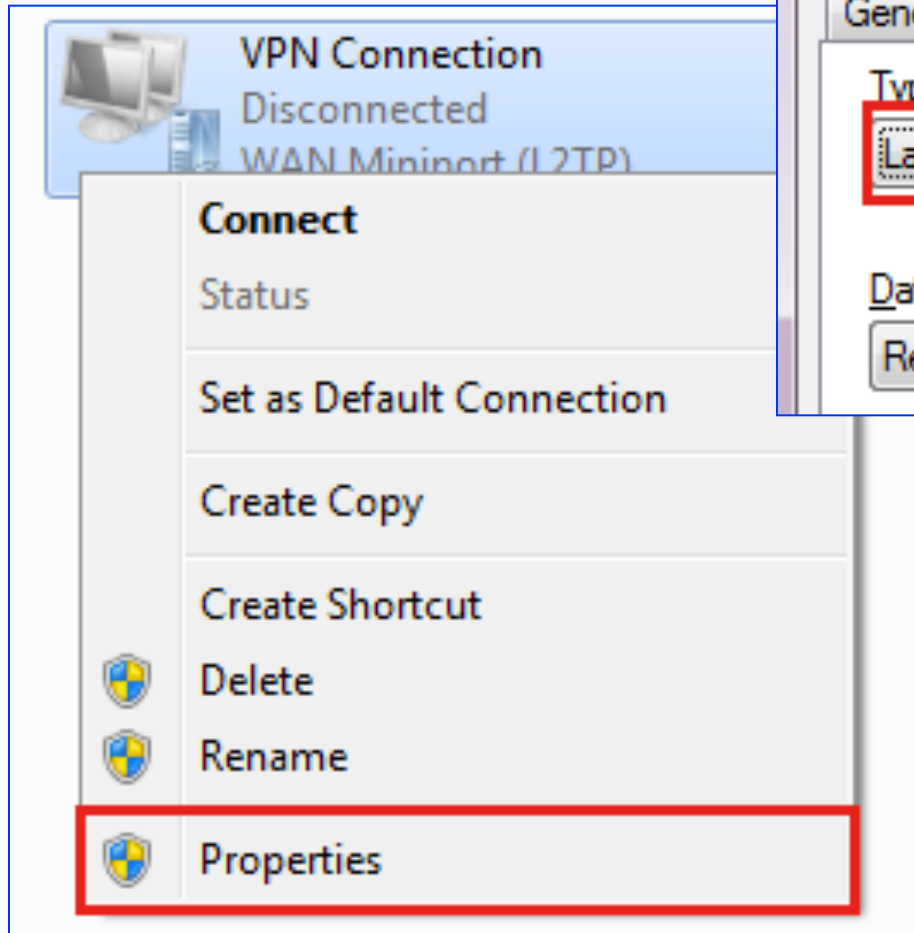
••••

Show characters

Remember this password

Domain (optional):

Configure VPN Client – L2TP



Configure Pre Shared Key

Advanced Properties

L2TP

Use preshared key for authentication

Key:

Use certificate for authentication

Verify the Name and Usage a

IPsec Peer <0.0.0.0/0>

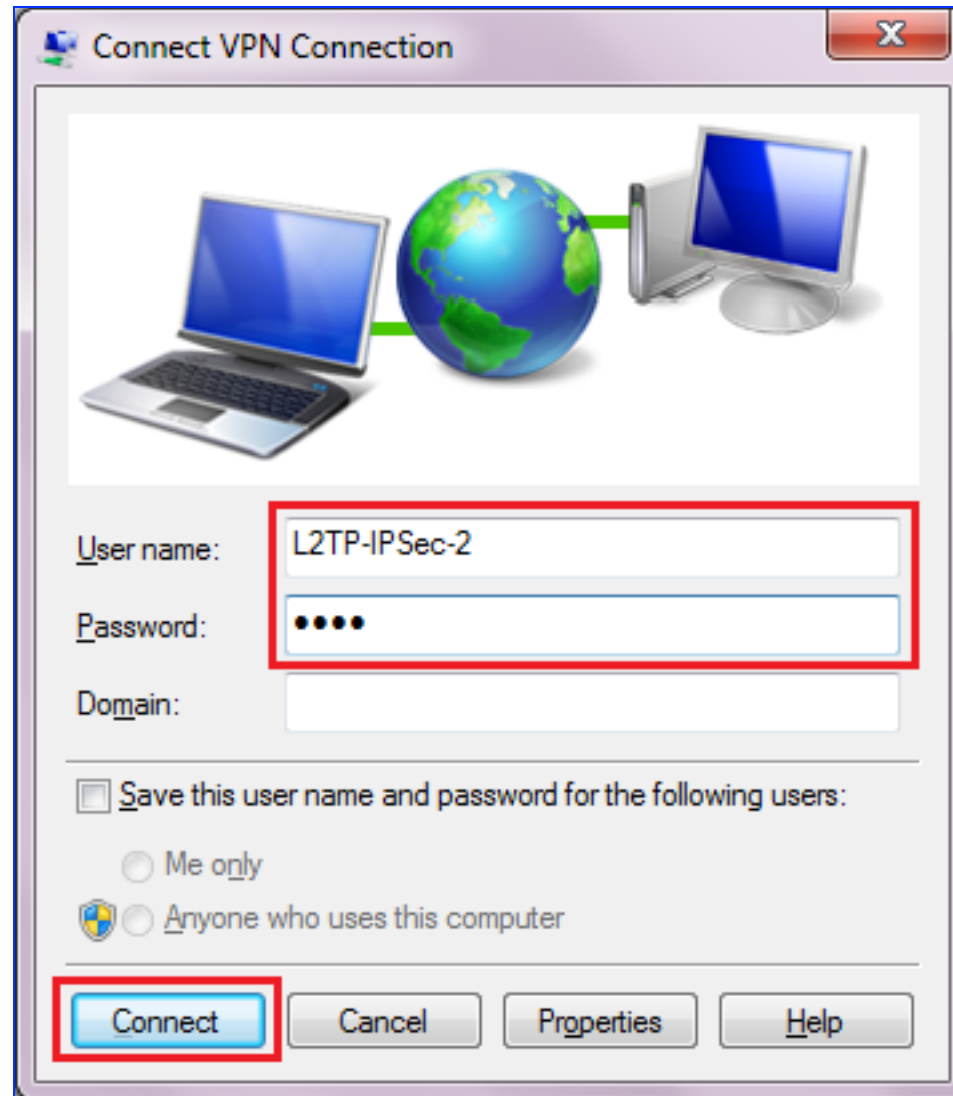
Address:

Port:

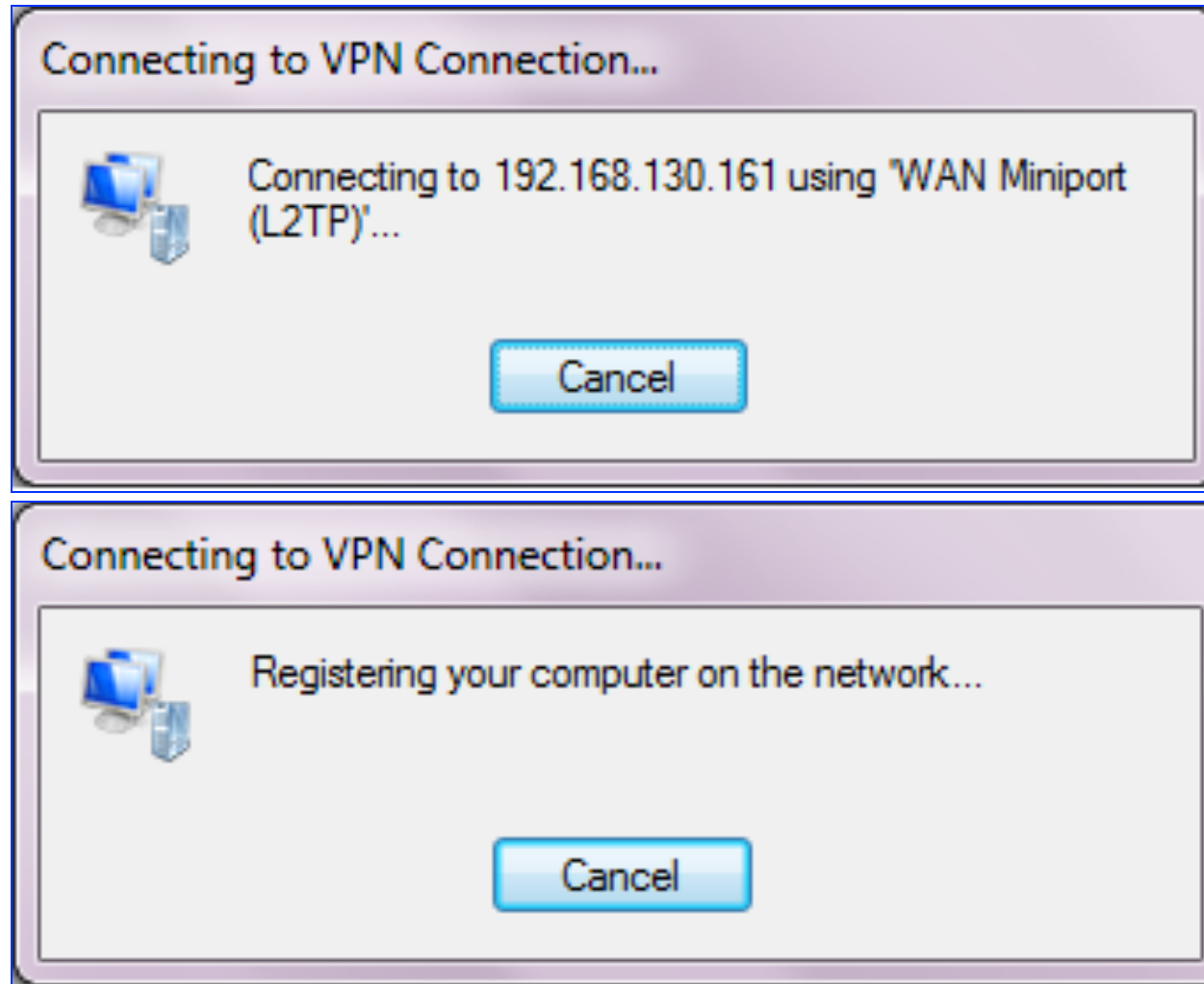
Auth. Method:

Secret:

Dial L2TP



Connecting Progress



IPsec Dynamic Encryption

IPsec Policy <192.168.130.169:0->192.168.130.161:0>

| General | Action |
|---------------|-----------------|
| Src. Address: | 192.168.130.169 |
| Src. Port: | |
| Dst. Address: | 192.168.130.161 |
| Dst. Port: | |
| Protocol: | 17 (udp) |
| dynamic | |

IPsec Policy <192.168.130.169:0->192.168.130.161:0>

| General | Action |
|---------------------------------|-----------------|
| Action: | encrypt |
| Level: | require |
| IPsec Protocols: | esp |
| <input type="checkbox"/> Tunnel | |
| SA Src. Address: | 192.168.130.169 |
| SA Dst. Address: | 192.168.130.161 |
| Proposal: | default |
| Priority: | 2 |
| dynamic | |



HOTSPOT



Certified Mikrotik Training - Advanced Class (MTCUME)

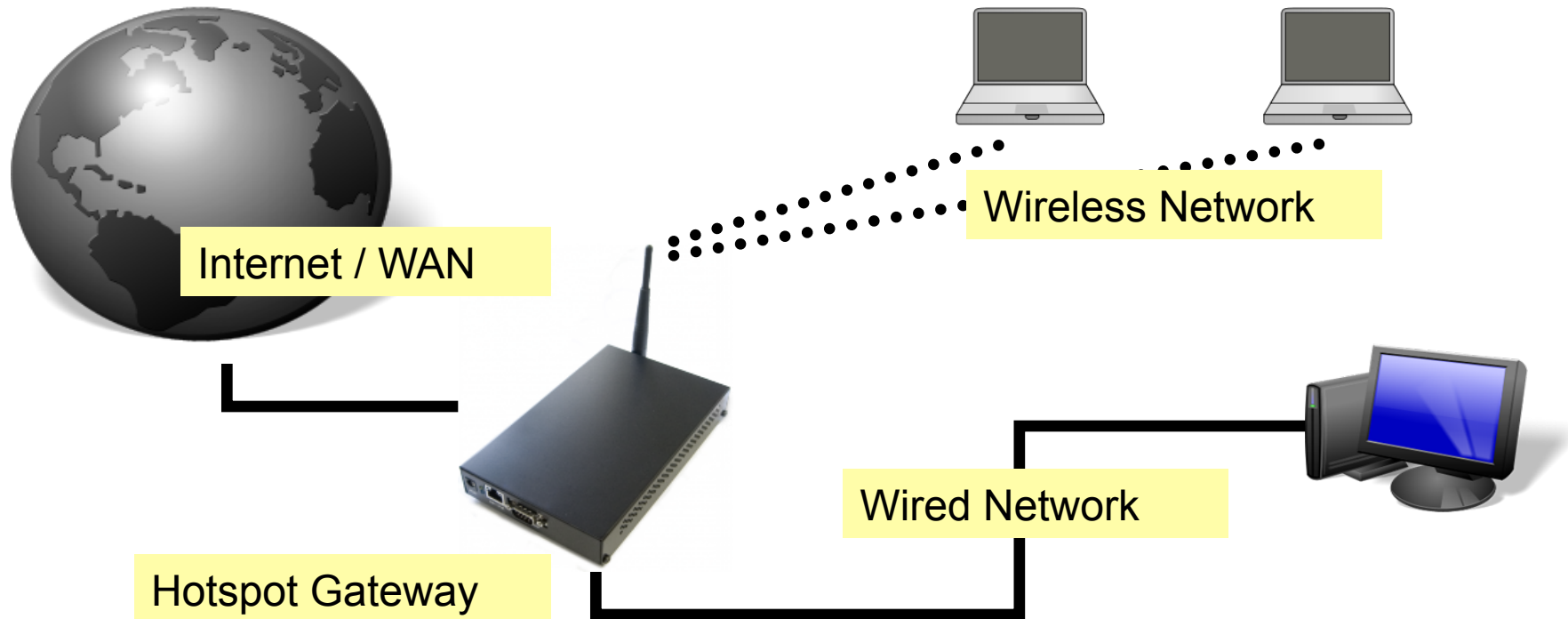
Organized by: **Citraweb Nusa Infomedia**
(Mikrotik Certified Training Partner)



HotSpot

- Hotspot System digunakan untuk memberikan layanan akses jaringan (Internet/Intranet) di Public Area dengan media kabel maupun wireless.
- Hotspot menggunakan Autentikasi untuk menjaga Jaringan tetap dapat dijaga walaupun bersifat public.
- Proses Autentikasi menggunakan protocol HTTP/HTTPS yang bisa dilakukan oleh semua web-browser.
- Hotspot System ini merupakan gabungan atau kombinasi dari beberapa fungsi dan fitur RouterOS menjadi sebuah system yang sering disebut 'Plug-n-Play' Access.

HotSpot Network - Example



- Hotspot System bisa digunakan pada berbagai interface jaringan, seperti Wireless, Kabel bahkan di virtual interface seperti VAP, VLAN, tunnel dan sebagainya.
- Jaringan Hotspot bersifat **Bridge Network**

How does it work ?

- User mencoba membuka halaman web.
- Authentication Check dilakukan oleh router pada Hotspot System.
- Jika belum ter-autentikasi, router akan mengalihkan ke halaman login.
- User memasukkan informasi login.

Please log on to use the mikrotik hotspot service



A screenshot of a web-based login interface for Mikrotik Hotspot. The interface is enclosed in a thin grey border. At the top, the text 'Please log on to use the mikrotik hotspot service' is displayed in a light grey font. Below this, there are two input fields: the first is labeled 'login' and contains the text 'anyuser'; the second is labeled 'password' and contains a series of asterisks. Below the password field is an 'OK' button. At the bottom of the form area, the 'MikroTik' logo is displayed in a stylized red font.

Powered by mikrotik routers © 2005 mikrotik

How does it work ?

- Jika informasi login sudah tepat, router akan :
 - Mengautentikasi client di hotspot system.
 - Membuka halaman web yang diminta sebelumnya.
 - Membuka popup halaman status.
- User dapat menggunakan akses jaringan.

Welcome anyuser!

| | |
|-----------------|---------------------|
| IP address: | 10.1.100.1 |
| bytes up/down: | 23.1 KiB / 43.5 KiB |
| connected: | 40s |
| status refresh: | 1m |

log off



HotSpot features

- Autentikasi User
- Perhitungan
 - Waktu akses
 - Data dikirim atau diterima
- Limitasi Data
 - Berdasarkan data rate (kecepatan akses)
 - Berdasarkan jumlah data
- Limitasi Akses User berdasarkan waktu
- Support RADIUS
- Bypass!

HotSpot setup wizard

- RouterOS sudah menyediakan Wizard untuk melakukan setup Hotspot System.
- Wizard ini berupa menu interaktif yang terdiri dari beberapa pertanyaan mengenai parameter setting hotspot.
- Wizard bisa dipanggil atau dieksekusi menggunakan perintah “*/ip hotspot setup*”
- Jika anda mengalami kegagalan dalam konfigurasi hotspot direkomendasikan reset kembali router dan konfigurasi ulang dari awal.

HotSpot Setup Wizard

- Pada Langkah awal Tentukan interface mana yang akan digunakan untuk menjalankan Hotspot System:
hotspot interface: (ex: ether1,wlan1,bridge1,vlan1)
- Tentukan Alamat IP untuk Interface Hotspot :
Local address of hotspot network: (ex: 10.5.50.1/24)
- Opsi Hotspot Network akan NAT atau Routing :
masquerade hotspot network: yes
- Tentukan IP-Pool untuk jaringan Hotspot :
address pool of hotspot network: 10.5.50.2-10.5.50.254
- Menggunakan SSL-certificate jika ingin menggunakan Login-By HTTPS :
select certificate: none

HotSpot Setup Wizard

- Jika diperlukan SMTP server khusus untuk Server hotspot bisa ditentukan, sehingga Server bisa mengirimkan email (misal email notifikasi). Konfigurasi SMTP server :

Ip address of smtp server: 0.0.0.0

- Konfigurasi DNS server yang akan digunakan oleh user Hotspot :

dns servers: 10.100.100.1

- Konfigurasi DNS-name dari router Hotspot, Hal ini digunakan jika Router memiliki DNS-Name yang valid (FQDN), Jika tidak ada biarkan kosong.

dns name: hotspot.websiteku.com

- Langkah terakhir dari wizard adalah pembuatan sebuah user hotspot :

name of local hotspot user: admin

password for the user: 12345

HotSpot Setup Wizard (Step 1)

The screenshot displays the Mikrotik WinBox interface for configuring a Hotspot. The main window title is "admin@192.168.30.1 (mejadepan) - WinBox v5.21 on RB433UAH (mipsbe)". The status bar shows "Safe Mode", "Uptime: 00:39:39", "Memory: 107.3 MiB", "CPU: 2%", "Date: Oct/25/2012", and "Time: 10:34:30".

In the left sidebar, the "Hotspot" menu item is highlighted with a red box. In the top toolbar, the "Hotspot Setup" button is also highlighted with a red box. A red arrow points from the "Hotspot Setup" button to the "Hotspot Setup" dialog box.

The "Hotspot Setup" dialog box is titled "Hotspot Setup" and contains the following elements:

- A label "Select interface to run HotSpot on" above a dropdown menu.
- The dropdown menu is currently set to "ether3".
- Buttons for "Back", "Next", and "Cancel" at the bottom.

HotSpot Setup Wizard (Step 2-5)

Hotspot Setup

Set HotSpot address for interface

Local Address of Network:

Masquerade Network

Back Next Cancel

Hotspot Setup

Set pool for HotSpot addresses

Address Pool of Network:

Back Next Cancel

Hotspot Setup

Select SMTP server

IP Address of SMTP Server:

Back Next Cancel

Hotspot Setup

Select hotspot SSL certificate

Select Certificate:

Back Next Cancel

HotSpot setup wizard (step 5-8)

Hotspot Setup

Setup DNS configuration

DNS Servers:

Back Next Cancel

Hotspot Setup

DNS name of local hotspot server

DNS Name:

Back Next Cancel

Hotspot Setup

Setup has completed successfully

OK

Hotspot Setup

Create local HotSpot user

Name of Local HotSpot User:

Password for the User:

Back Next Cancel

HotSpot Server

The screenshot displays the Mikrotik WinBox interface for configuring a Hotspot Server. The main window shows a table with the following data:

| Name | Interface | Address Pool | Profile | Adresse... |
|----------|-----------|--------------|---------|------------|
| hotspot1 | ether3 | hs-pool-5 | hsprof1 | 2 |

A dialog box titled "Hotspot Server <hotspot1>" is open, showing the configuration for the selected server. The fields are as follows:

- Name: hotspot1
- Interface: ether3
- Address Pool: hs-pool-5
- Profile: hsprof1
- Idle Timeout: 00:05:00
- Keypalive Timeout: (empty)
- Addresses Per MAC: 2
- IP of DNS Name: 10.5.50.1
- Proxy Status: running

Buttons on the right side of the dialog include: OK, Cancel, Apply, Disable, Copy, Remove, and Reset HTML. At the bottom, there are checkboxes for "enabled" and "HTTPS".

HotSpot Server

- Didalam sebuah router bisa dibangun banyak hotspot server, dengan catatan dalam 1 interface hanya bisa untuk 1 hotspot server
- Di menu ini kita bisa mengaktifkan One to One Nat / universal client
- Kita bisa mengatur untuk timeout user yang belum melakukan login sehingga IP bisa dialokasikan ke user yang lain
- Selain itu kita juga bisa membatasi jumlah MAC sama yang melakukan request akses. Hal ini berguna untuk mencegah DHCP starvation

HotSpot Server Profiles

The screenshot displays the Mikrotik WinBox interface for configuring Hotspot Server Profiles. The main window is titled 'Hotspot' and has several tabs: Servers, Server Profiles, Users, User Profiles, Active, Hosts, IP Bindings, Service Ports, Walled Garden, and a search field labeled 'Find'. The 'Server Profiles' tab is active, showing a list of profiles. Two profiles are listed: 'default' and 'hsprof1'. The 'hsprof1' profile is selected and highlighted in blue. A dialog box titled 'Hotspot Server Profile <hsprof1>' is open, showing the configuration for this profile. The dialog has three tabs: 'General', 'Login', and 'RADIUS'. The 'General' tab is selected, and the following fields are visible:

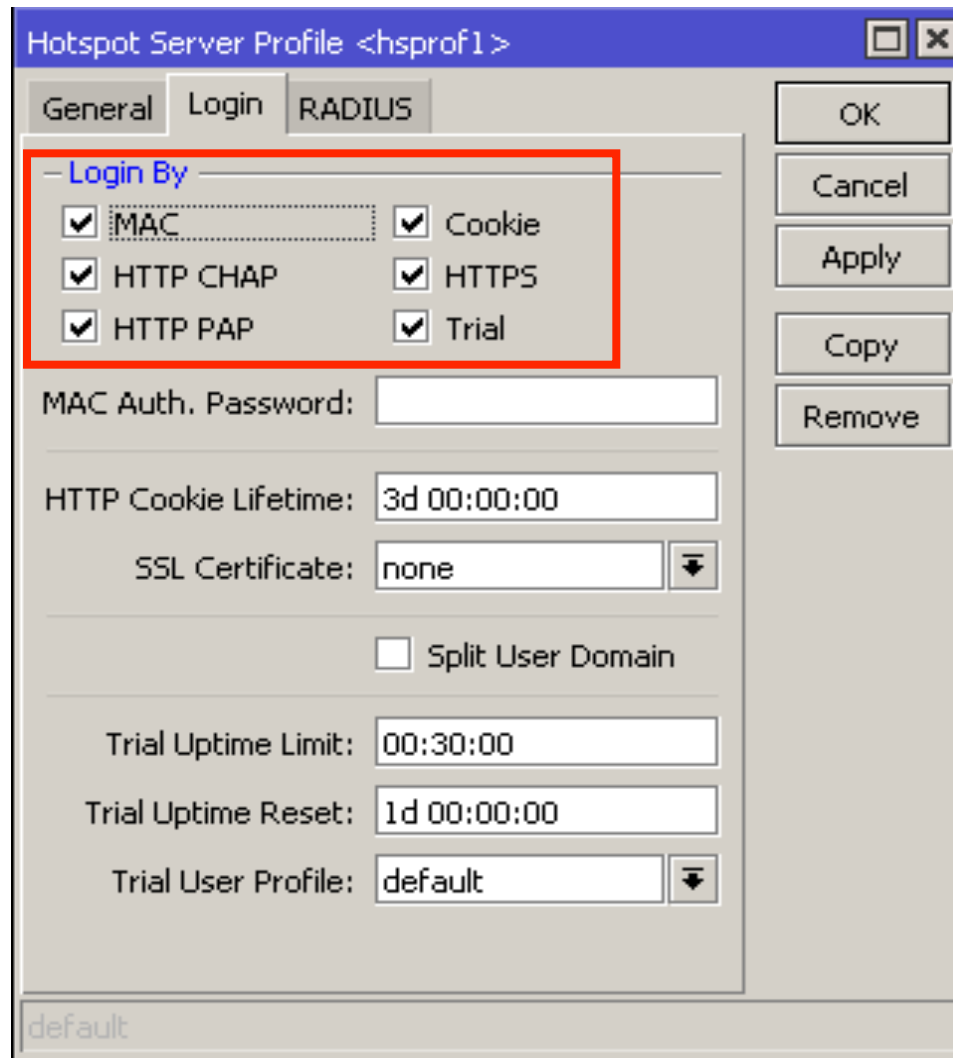
- Name:
- Hotspot Address:
- DNS Name:
- HTML Directory:
- Rate Limit (rx/tx):
- HTTP Proxy:
- HTTP Proxy Port:
- SMTP Server:

On the right side of the dialog, there are buttons for 'OK', 'Cancel', 'Apply', 'Copy', and 'Remove'. At the bottom of the dialog, the word 'default' is visible. The status bar at the bottom of the main window indicates '2 items (1 selected)'.

HotSpot Server profiles

- Hotspot Server Profile digunakan untuk menyimpan konfigurasi-konfigurasi umum dari beberapa hotspot server.
- Profile ini digunakan untuk grouping beberapa hotspot server dalam satu router.
- Parameter yang bisa kita gunakan untuk memodifikasi hotspot server kita antara lain :
 - Pengaturan proxy transparent
 - Pengaturan halaman HTML
 - Metode Autentikasi
 - Pengaturan RADIUS

Authentication Method

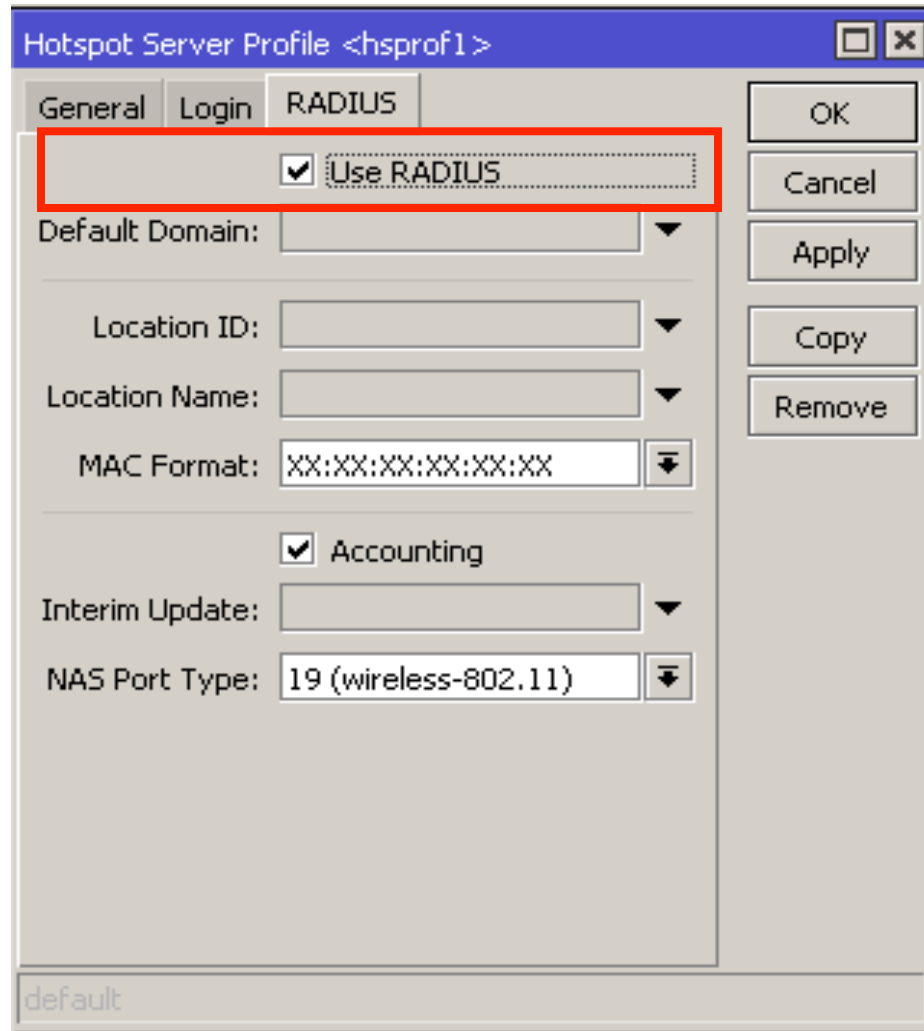


6 Metode autentikasi yang berbeda pada server profile.

Hotspot Authentication Methods

- **HTTP-PAP** - metode autentikasi yang paling sederhana, yaitu menampilkan halaman login dan mengirimkan info login berupa plain text.
- **HTTP-CHAP** - metode standard yang mengintegrasikan proses CHAP pada proses login.
- **HTTPS** – menggunakan Enkripsi Protocol SSL untuk Autentikasi.
- **HTTP Cookie** - setelah user berhasil login data cookie akan dikirimkan ke web-browser dan juga disimpan oleh router di 'Active HTTP cookie list' yang akan digunakan untuk autentikasi login selanjutnya.
- **MAC Address** - metode ini akan mengautentikasi user mulai dari user tersebut muncul di 'host-list', dan menggunakan MAC address dari client sebagai username dan password.
- **Trial** - User tidak memerlukan autentikasi pada periode waktu yang sudah ditentukan.

AAA Hotspot



Hotspot Server Profile <hsprof1>

General Login **RADIUS**

Use RADIUS

Default Domain:

Location ID:

Location Name:

MAC Format:

Accounting

Interim Update:

NAS Port Type:

OK
Cancel
Apply
Copy
Remove

default

- Hotspot dengan integrasi RADIUS server (usermanager)



HotSpot User Profiles

- Hotspot User Profile digunakan untuk menyimpan konfigurasi-konfigurasi umum dari User-User hotspot / Authorization. Profile ini digunakan untuk grouping beberapa User dalam sebuah aturan yang sama.
- Pada User Profile, mampu melakukan assign pool-ip tertentu ke group user untuk proses one to one nat.
- Parameter Time-out juga bisa diaktifkan untuk melogout otomatis user jika lupa log out.
- Limitasi data rate dan lama sesi juga bisa ditentukan di User-Profile
- Kita juga bisa memasang custom script yang akan dieksekusi setelah user login ataupun logout

User Profiles

Pool IP One to One NAT

Pembatasan jumlah maksimal multi login dengan 1 user

Limitasi bandwidth per user
format : rx-rate[/tx-rate] [rx-burst-rate[/tx-burst-rate] [rx-burst-threshold[/tx-burst-threshold] [rx-burst-time[/tx-burst-time]]]] [priority] [rx-rate-min[/tx-rate-min]]

Trafik http user akan dilewatkan proxy hotspot

New Hotspot User Profile

General Advertise Scripts

Name: lprof1

Address Pool: none

Session Timeout:

Idle Timeout: none

Keepalive Timeout: 00:02:00

Status Autorefresh: 00:01:00

Shared Users: 1

Rate Limit (rx/tx):

Address List:

Incoming Filter:

Outgoing Filter:

Incoming Packet Mark:

Outgoing Packet Mark:

Open Status Page: always

Transparent Proxy

OK Cancel Apply Copy Remove



User Profiles

Address List : IP user akan ditambahkan ke dalam firewall address-list sesuai list yang ditentukan

Incoming Filter : Nama chain baru untuk trafik yang berasal dari IP user (trafik upload)

Outgoing Filter : Nama chain baru untuk trafik yang menuju IP user (trafik download)

Incoming Packet Mark : Nama packet-mark untuk trafik yang berasal dari IP user (trafik upload)

Outgoing Packet Mark : Nama packet-mark untuk trafik yang menuju IP user (trafik download)

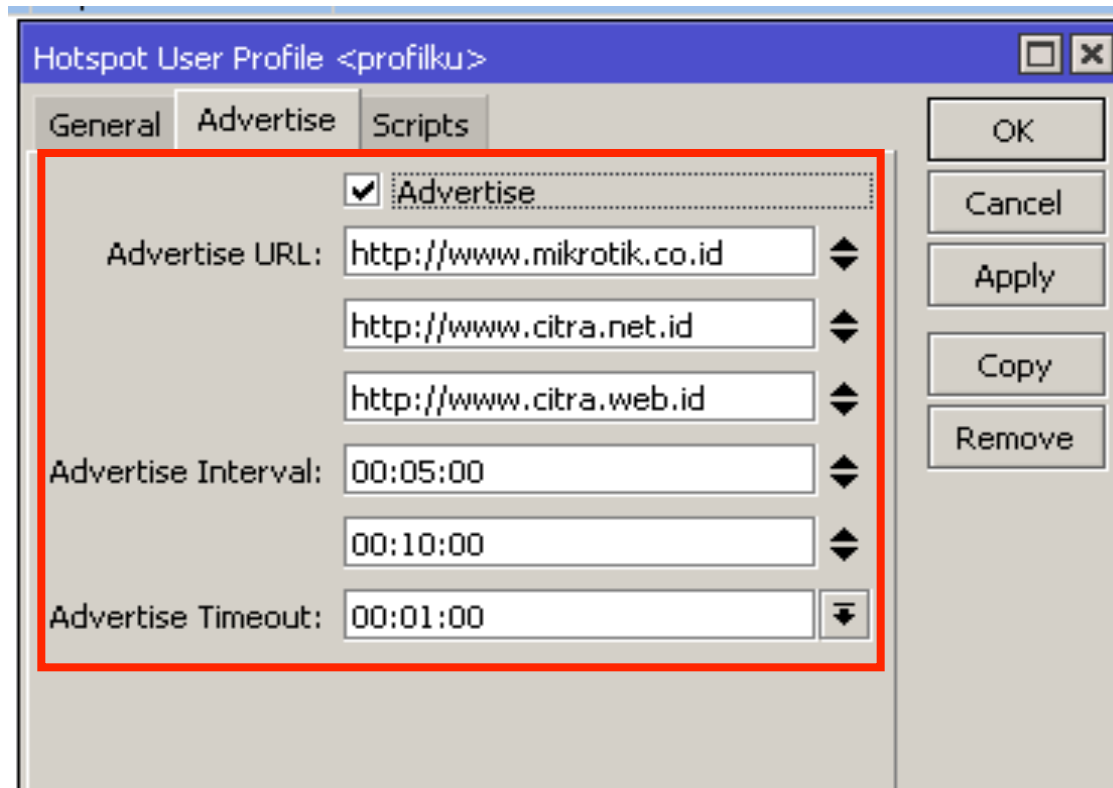
Kelima parameter ini bisa kita gunakan untuk melakukan filtering dan qos yang advanced

Advertisement

- Advertisement bisa kita gunakan untuk menampilkan popup halaman web (misal : iklan) di web-browser para user yang sudah terautentikasi.
- Halaman Advertisement dimunculkan berdasarkan periode waktu yang sudah ditentukan, dan akses akan dihentikan jika pop-up halaman advertisement diblock (pop-up blocker aktif), dan akan disambungkan kembali jika halaman Advertisement sudah dimunculkan.
- Advertisement hanya bisa dilakukan jika option transparent proxy pada user profile di set

Advertisement

- Jika sudah waktunya untuk memunculkan advertisement, server akan memanggil halaman status dan meriderect halaman status tersebut ke halaman web iklan yang sudah ditentukan.



[LAB-1] Hotspot Config

- Aktifkan Hotspot gateway pada interface ether3
- Buat profile yang berbeda-beda untuk user nantinya
 - Trial :
 - Advertisement
 - Share bandwidth upload / download : 128k/256k
 - Configure Uptime : 10 minute + Uptime reset : 1week
 - VIP
 - Dedicated bandwidth upload / download 512k/512k
 - Reguler
 - Block some protocol (ex : no PING)
 - Share bandwidth upload / download : 512k/512k
- Lakukan Backup !

[LAB-1] Profile

The image shows two overlapping windows from Mikrotik WinBox. The left window is the 'Hotspot' main interface, and the right window is the 'Hotspot User Profile <trial>' configuration dialog.

Hotspot Main Interface:

- Buttons: +, -, Filter
- Table:

| Name | Selected |
|-----------|----------|
| * default | |
| reguler | |
| trial | Selected |
| vip | |
- Footer: 4 items (1 selected)

Hotspot User Profile <trial> Configuration:

- General tab: Name: trial, Address Pool: none, Session Timeout: [empty], Idle Timeout: none, Keepalive Timeout: 00:02:00, Status Autorefresh: 00:01:00, Shared Users: 1, Rate Limit (rx/tx): [empty], Address List: [empty], Incoming Filter: [empty], Outgoing Filter: [empty], Incoming Packet Mark: packet-in-trial, Outgoing Packet Mark: packet-out-trial, Open Status Page: always, Transparent Proxy
- Advertise tab: Advertise, Advertise URL: http://www.mikrotik.co.id, http://www.citra.net.id, http://www.citra.web.id, Advertise Interval: 00:00:15, Advertise Timeout: 00:01:00

Red boxes highlight the '+' button in the main interface, the 'Incoming Packet Mark' and 'Outgoing Packet Mark' fields, and the 'Advertise' section in the configuration dialog. Red arrows point from the '+' button to the packet marking fields and from the 'Advertise' section to the 'Advertise URL' field.

[LAB-1] Profile (2)

Hotspot User Profile <vip>

General | Advertise | Scripts

Name: vip

Address Pool: none

Session Timeout: []

Idle Timeout: none

Keepalive Timeout: 00:02:00

Status Autorefresh: 00:01:00

Shared Users: 1

Rate Limit (rx/tx): 512k/512k

Address List: []

Incoming Filter: []

Outgoing Filter: []

Incoming Packet Mark: []

Outgoing Packet Mark: []

Open Status Page: always

Transparent Proxy

OK
Cancel
Apply
Copy
Remove

default

Hotspot User Profile <reguler>

General | Advertise | Scripts

Name: reguler

Address Pool: none

Session Timeout: []

Idle Timeout: none

Keepalive Timeout: 00:02:00

Status Autorefresh: 00:01:00

Shared Users: 1

Rate Limit (rx/tx): []

Address List: []

Incoming Filter: filter-in-reguler

Outgoing Filter: []

Incoming Packet Mark: packet-in-reguler

Outgoing Packet Mark: packet-out-reguler

Open Status Page: always

Transparent Proxy

OK
Cancel
Apply
Copy
Remove

default

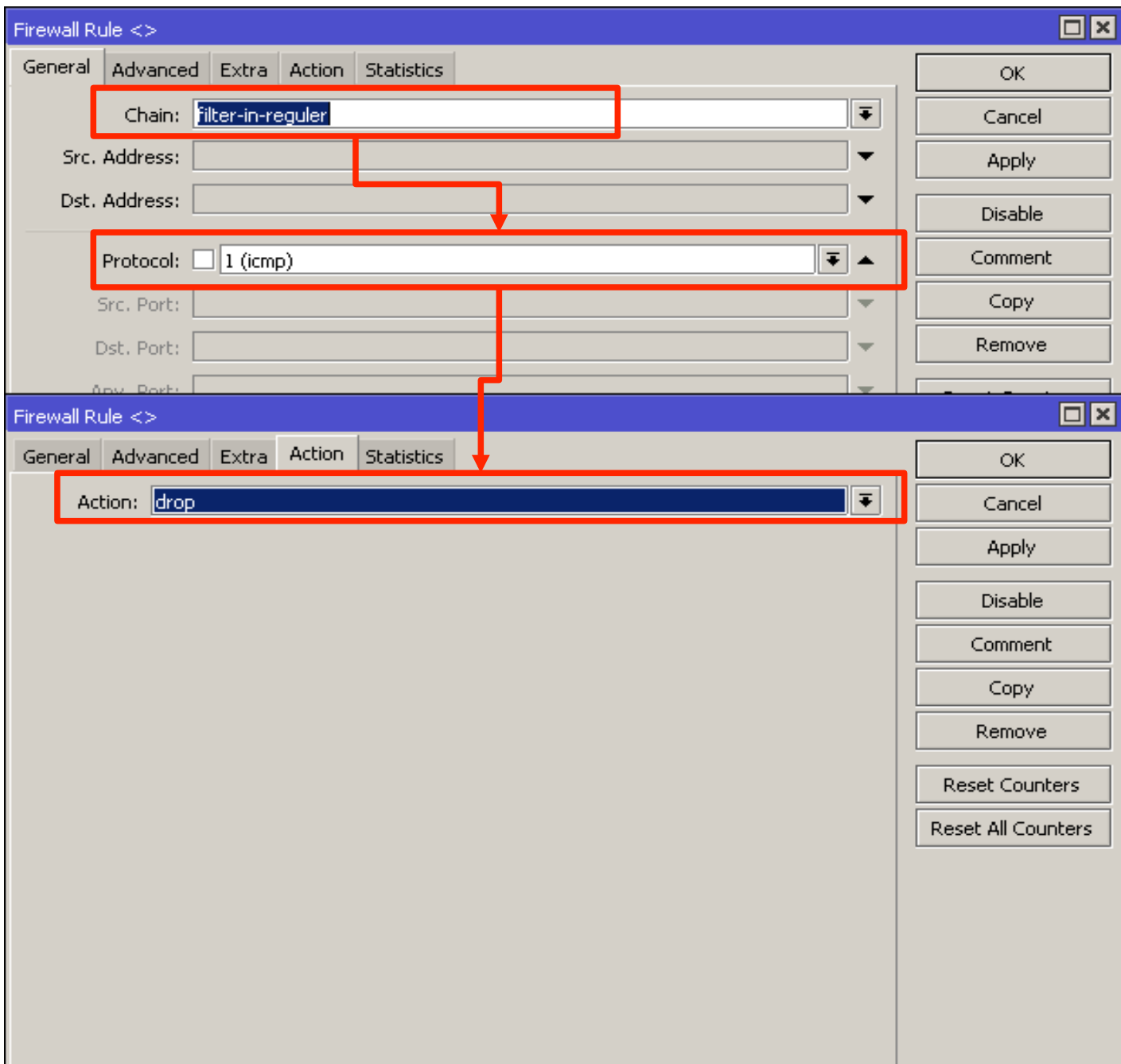
[LAB-1] Hotspot Config

The image shows the Mikrotik WinBox Firewall configuration interface. On the left, the 'Filter Rules' table lists existing rules. The main area shows two 'New Firewall Rule' dialog boxes. The top dialog is on the 'General' tab with 'Chain' set to 'forward'. The bottom dialog is on the 'Action' tab with 'Action' set to 'jump' and 'Jump Target' set to 'hotspot'. Red boxes and arrows highlight these specific settings.

| # | Action | Chain |
|------------------------------|--------|------------------------|
| 0 | D | jump Forward |
| 1 | D | jump Forward |
| 2 | D | jump input |
| 3 | D | drop input |
| 4 | DI | jump hs-input |
| 5 | D | acc... hs-input |
| 6 | D | acc... hs-input |
| 7 | D | ret... hs-unauth |
| 8 | D | jump hs-input |
| 9 | D | reject hs-unauth |
| 10 | D | ret... hs-unauth-to |
| 11 | D | reject hs-unauth |
| 12 | D | reject hs-unauth-to |
| ;;; place hotspot rules here | | |
| 13 | X | pas... unused-hs-chain |
| 14 | I | jump forward |
| 15 | | drop filter-in-regular |

New Firewall Rule (General Tab):
Chain: forward

New Firewall Rule (Action Tab):
Action: jump
Jump Target: hotspot



[LAB-1] Hotspot Config

The screenshot shows the Mikrotik WinBox Firewall configuration interface. The 'Filter Rules' tab is active, and a new rule is being configured. The rule is a Mangle Rule with the following settings:

- Chain:** prerouting
- In. Interface:** ether3
- Action:** jump
- Jump Target:** hotspot

Red arrows highlight the configuration steps: the '+' button to add a rule, the 'Chain' dropdown, the 'In. Interface' dropdown, and the 'Action' and 'Jump Target' dropdowns.

The image displays two overlapping windows from the Mikrotik WinBox interface, both titled "Mangle Rule <>".

The top window is in the "General" tab. It features several input fields: "Chain" is set to "postrouting", "Out. Interface" is set to "ether3", and "In. Interface" is empty. Other fields like "Src. Address", "Dst. Address", "Protocol", "Src. Port", "Dst. Port", "Any. Port", "P2P", and "Packet Mark" are also present but empty. A red box highlights the "Chain" field, and another red box highlights the "Out. Interface" field. A red arrow points from the "Chain" box down to the "Out. Interface" box.

The bottom window is in the "Action" tab. It features two input fields: "Action" is set to "jump" and "Jump Target" is set to "hotspot". A red box highlights both the "Action" and "Jump Target" fields. A red arrow points from the "Out. Interface" field in the top window down to the "Action" field in the bottom window.

Both windows have a vertical column of buttons on the right side, including "OK", "Cancel", "Apply", "Disable", "Comment", "Copy", "Remove", "Reset Counters", and "Reset All Counters".

Queue List

Simple Queues Interface Queues Queue Tree Queue Types

+ - ✓ ✕ [icon] [icon] Reset Counters 00 Reset All Counters Find

| Name | Parent |
|------------------|-----------|
| download-reguler | ether3 |
| download-trial | ether3 |
| upload-reguler | global-in |
| upload-trial | global-in |

4 items out of 7 0 B queue

Queue <upload-trial>

General Statistics

Name: upload-trial

Parent: global-in

Packet Marks: packet-in-trial

Queue Type: default

Priority: 8

Limit At: bits/s

Max Limit: 128k bits/s

Burst Limit: bits/s

Burst Threshold: bits/s

Burst Time: s

enabled

OK Cancel Apply Disable Comment Reset Counters Reset All Counters



Queue <download-trial>

General Statistics

Name: download-trial

Parent: ether3

Packet Marks: packet-out-trial

Queue Type: default

Priority: 8

Limit At: bits/s

Max Limit: 256k bits/s

Burst Limit: bits/s

Burst Threshold: bits/s

Burst Time: s

enabled

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

Queue <upload-reguler>

General Statistics

Name:

Parent: ▼

Packet Marks: ▼ ▲

Queue Type: ▼

Priority:

Limit At: ▼ bits/s

Max Limit: ▲ bits/s

Burst Limit: ▼ bits/s

Burst Threshold: ▼ bits/s

Burst Time: ▼ s

enabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

Queue <download-reguler>

General Statistics

Name:

Parent: ▼

Packet Marks: ▼ ▲

Queue Type: ▼

Priority:

Limit At: ▼ bits/s

Max Limit: ▲ bits/s

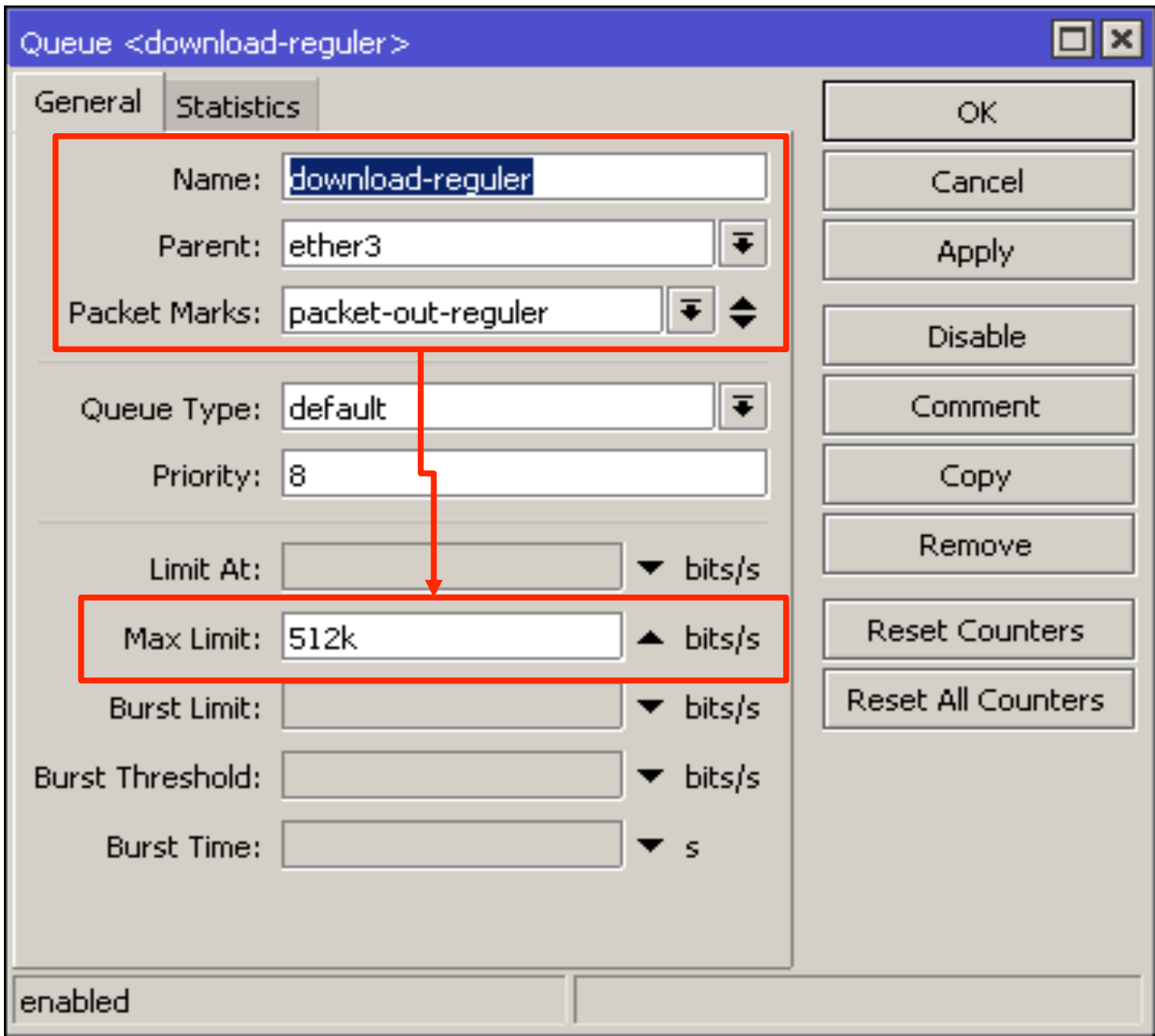
Burst Limit: ▼ bits/s

Burst Threshold: ▼ bits/s

Burst Time: ▼ s

enabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters





HotSpot User

- Halaman dimana parameter username, password dan profile dari user disimpan.
- Beberapa limitasi juga bisa ditentukan di halaman user seperti uptime-limit dan bytes-in/bytes-out. Jika limitasi sudah tercapai maka user tersebut akan expired dan tidak dapat digunakan lagi.
- IP yang spesifik juga bisa ditentukan di halaman ini sehingga user akan mendapat ip yang sama.
- User bisa dibatasi pada MAC-address tertentu.

HotSpot users

Quick Set

Interfaces

Wireless

Bridge

PPP

Switch

Mesh

IP

MPLS

Routing

System

Queues

Files

Log

Radius

Tools

New Terminal

MetaROUTER

Make Supout.rif

Manual

ARP

Accounting

Addresses

DHCP Client

DHCP Relay

DHCP Server

DNS

Firewall

Hotspot

IPsec

Neighbors

Packing

Pool

Routes

SMB

SNMP

Services

Hotspot

Server Profiles

Users

User Profiles

Active

Hosts

IP Bindings

Service Ports

Walled Gard

+ - ✓ ✗ 📁 🔍

00 Reset All Counters

| Server | Name | Address | MAC Addr... | Profile | Uptime |
|--------|-------|---------|-------------|---------|----------|
| all | admin | | | default | 00:00:00 |

1 item (1 selected)

New Hotspot User

General Limits Statistics

Server: all

Name: user1

Password: 12345

Address:

MAC Address:

Profile: default

Routes:

Email:

enabled

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset All Counters

User Limitation

- **Limit Uptime** batas waktu user dapat menggunakan akses ke Hotspot Network.
- **Limit-bytes-in, Limit-bytes-out** dan **Limit-bytes-total** batas quota transfer data yang bisa dilakukan oleh user.

The screenshot shows the 'New Hotspot User' dialog box with the 'Limits' tab selected. The dialog has three tabs: 'General', 'Limits', and 'Statistics'. The 'Limits' tab contains four input fields with up/down arrows to their right:

- Limit Uptime: 01:00:00
- Limit Bytes In: 1000000000
- Limit Bytes Out: 5000000000
- Limit Bytes Total: 4000000000

On the right side of the dialog, there is a vertical stack of buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, and Reset All Counters. At the bottom left of the dialog, the text 'enabled' is displayed.



[LAB-2] User Limitation

- Buat username masing-masing profile yang sudah kita buat
 - VIP
 - Lock hanya bisa dari laptop kita
 - Quota unlimited
 - Reguler
 - Limit uptime : 1h
 - Quota download : 10MB, upload : 5MB
- Test kedua username dan trial user anda
- Amati perubahan firewall filter, mangle dan counter queue dari lab1
- Backup for next lab :)

Hotspot

Server Profiles Users User Profiles Active Hosts IP Bindings Service Ports ...

+ - ✓ ✗ 📁 🔍 00 Reset All Counters Find

| Server | Name | Address | MAC Addr... | Profile | Uptime |
|----------|--------|---------|-------------|---------|----------|
| all | admin | | | default | 00:01:33 |
| all | regula | | | | |
| all | vip | | | | |
| hotspot1 | T-9C: | | | | |

Hotspot User <vip>

General Limits Statistics

Server: all

Name: vip

Password: 12345

Address:

MAC Address: 9C:8E:99:48:F6:20

Profile: vip

Routes:

Email:

OK Cancel Apply Disable Comment Copy Remove Reset All Counters

4 items (1 selected)

enabled

[LAB-2] User Limitation

The image displays two screenshots of the Mikrotik Hotspot User configuration interface, illustrating the process of setting user limitations.

Left Screenshot (General Tab):

- Server: all
- Name: reguler
- Password: 12345
- Profile: reguler
- Address: [Empty]
- MAC Address: [Empty]
- Routes: [Empty]
- Email: [Empty]
- Status: enabled

Right Screenshot (Limits Tab):

- Limit Uptime: 01:00:00
- Limit Bytes In: 5000000
- Limit Bytes Out: 10000000
- Limit Bytes Total: [Empty]
- Status: enabled

Red boxes highlight the 'all' server, 'reguler' name, 'reguler' profile, and the limit values. A red arrow points from the 'Profile' dropdown to the 'Limit Bytes Total' field.

Bypass! - IP bindings

- One-to-one NAT bisa dikonfigurasi secara static berdasarkan :
 - Original IP Host
 - Original MAC Address
- Bypass host terhadap Hotspot Authentication bisa dilakukan menggunakan IP-Bindings.
- Block Akses dari host tertentu (Berdasarkan Original MAC-address atau Original IP-Address) juga bisa dilakukan menggunakan IP-Bindings.

HotSpot IP bindings

The screenshot displays the Mikrotik Hotspot configuration window. The 'IP Bindings' tab is selected. A red box highlights the '+' button in the toolbar, with an arrow pointing to the 'New Hotspot IP Binding' dialog box. The dialog box contains the following fields:

- MAC Address: :BB:CC:DD:EE:FF
- Address: 0.0.0.0
- To Address: (empty)
- Server: all
- Type: regular (dropdown menu is open, showing options: regular, blocked, bypassed, regular)

Buttons on the right side of the dialog include: OK, Cancel, Apply, Disable, Comment, Copy, and Remove. The 'enabled' checkbox is checked at the bottom of the dialog. The main window shows a table with columns: #, MAC Address, Address, To Address, and Server. The status bar at the bottom indicates '0 items'.

Bypass - WalledGarden

- **WalledGarden** adalah sebuah system yang memungkinkan untuk user yang belum terautentikasi menggunakan (Bypass!) beberapa resource jaringan tertentu tetapi tetap memerlukan autentikasi jika ingin menggunakan resource yang lain.
- **IP-WalledGarden** hampir sama seperti WalledGarden tetapi mampu melakukan bypass terhadap resource yang lebih spesifik pada protocol dan port tertentu.
- Biasanya digunakan untuk melakukan bypass terhadap server local yang tidak memerlukan autentikasi.

HTTP-level WalledGarden

The screenshot shows the Mikrotik Hotspot configuration interface. The 'Walled Garden' tab is selected. A red box highlights the '+' icon in the toolbar, with an arrow pointing to the 'Walled Garden Entry' dialog box. The dialog box is titled 'Walled Garden Entry <*mikrotik.co.id>'. Inside the dialog, the 'Action' is set to 'allow' (radio button selected), and the 'Dst. Host' is set to '*mikrotik.co.id'. Other fields like 'Server', 'Src. Address', 'Dst. Address', 'Method', 'Dst. Port', and 'Path' are empty. The dialog also contains buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', and 'Remove'. The main interface shows a table with one entry: 'allow' under the 'Action' column. The status at the bottom is '1 item' and 'enabled'.

| Action | Server | Method | Dst. Host | Dst. Port |
|--------|--------|--------|-----------|-----------|
| allow | | | | |

IP-WalledGarden

Hotspot

Active Hosts IP Bindings Service Ports Walled Garden **Walled Garden IP List** Cookies ...

+ - ✓ ✗ [icon] [icon] Find

| Action | Server | Src. Address | Protocol | Dst. Port |
|--------|--------|--------------|----------|-----------|
| accept | | | | |

Walled Garden IP Entry <>

Action: accept drop reject

Server: [dropdown]

Src. Address: [dropdown]

Dst. Address: [dropdown]

Protocol: 6 (tcp) [dropdown]

Dst. Port: 20-21 [dropdown]

Dst. Host: [dropdown]

OK Cancel Apply Disable Comment Copy Remove

enabled

1 item

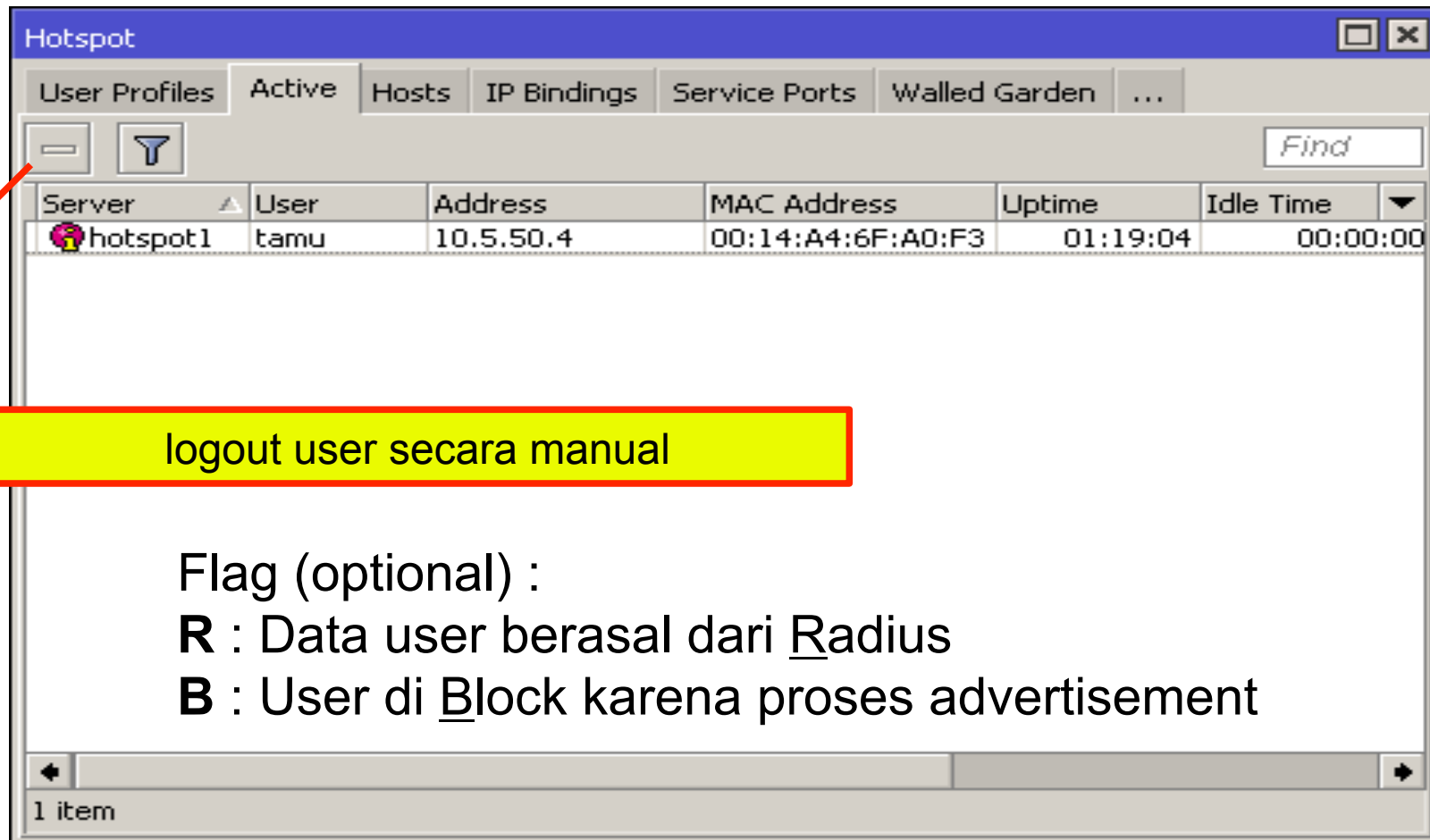


[LAB-3] Bypass Lab

- Lakukan bypass untuk akses ke website mikrotik
- Lakukan bypass untuk trafik winbox
- Lakukan bypass untuk trafik ping dari PC tertentu
- Lakukan bypass semua akses untuk PC tertentu
- Lakukan backup router anda :)

Hotspot - Active

- Tabel active digunakan untuk memonitoring client yang sedang aktif / terautentikasi di hotspot server kita secara realtime.



| Server | User | Address | MAC Address | Uptime | Idle Time |
|----------|------|-----------|-------------------|----------|-----------|
| hotspot1 | tamu | 10.5.50.4 | 00:14:A4:6F:A0:F3 | 01:19:04 | 00:00:00 |

logout user secara manual

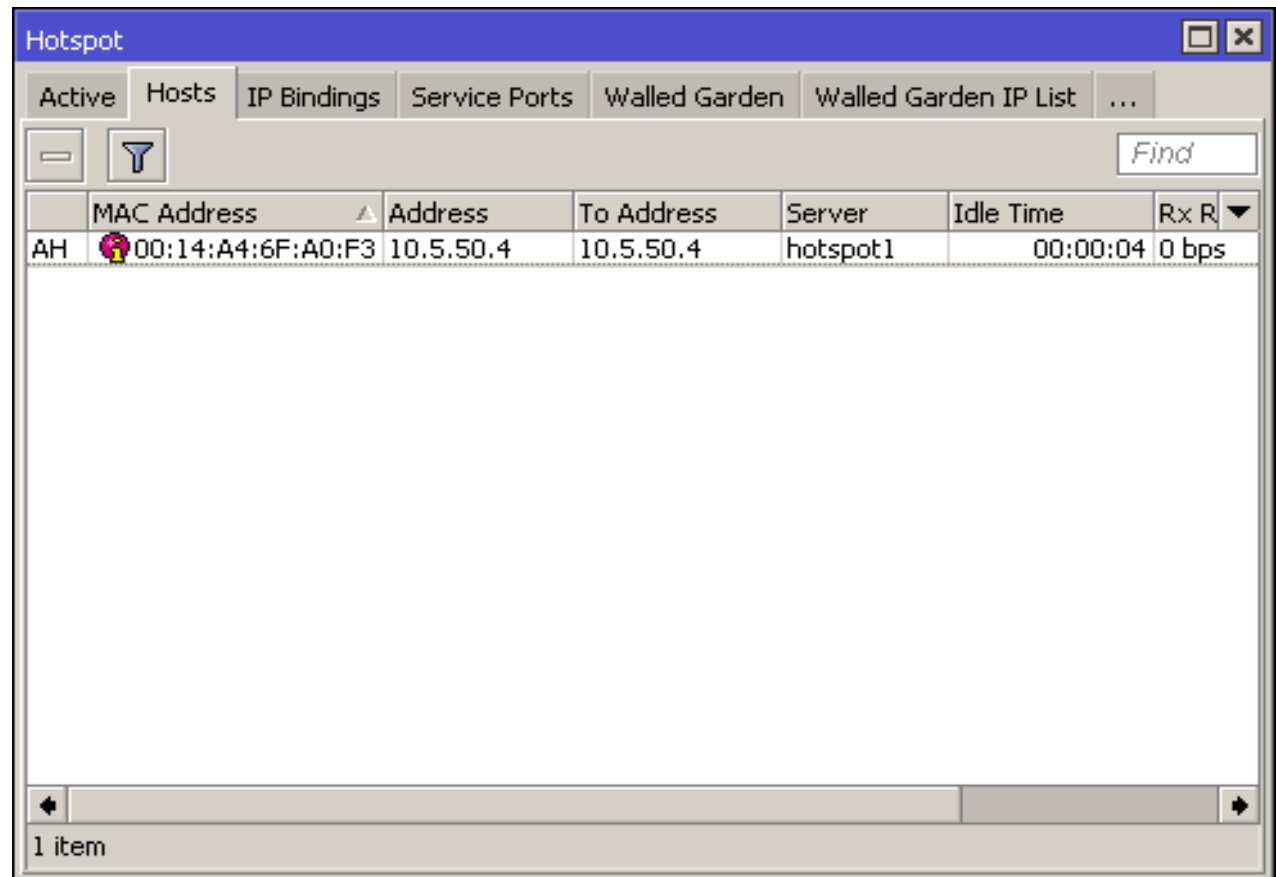
Flag (optional) :

- R** : Data user berasal dari Radius
- B** : User di Block karena proses advertisement

1 item

Hotspot - Host

- Tabel host digunakan untuk memonitoring semua perangkat yang terhubung dengan hotspot server baik yang sudah login ataupun belum



Hotspot

Active Hosts IP Bindings Service Ports Walled Garden Walled Garden IP List ...

Find

| | MAC Address ▲ | Address | To Address | Server | Idle Time | Rx R▼ |
|----|-------------------|-----------|------------|----------|-----------|-------|
| AH | 00:14:A4:6F:A0:F3 | 10.5.50.4 | 10.5.50.4 | hotspot1 | 00:00:04 | 0 bps |

1 item

Hotspot - Host

- Flag yang tersedia didalam tabel Host :
- **S** : User sudah ditentukan IP nya didalam IP binding
- **H** : User menggunakan IP DHCP
- **D** : User menggunakan IP statik
- **A** : User sudah melakukan login / Autentikasi
- **P** : User di byypass pada IP binding

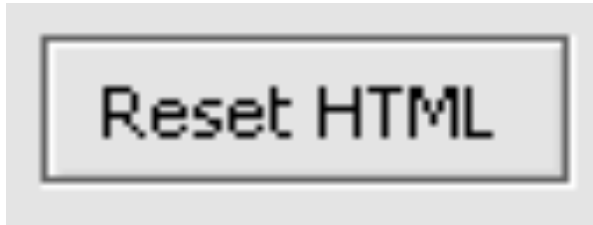
Hotspot Customization

- Antar muka / tampilan Hotspot server pada Mikrotik tersusun dari berbagai macam file html, yang memungkinkan untuk kita lakukan customisasi tampilan.
- Penyimpanan file HTML berada di internal storage router dan bisa diakses di menu “FILES”
- Jika di router ada banyak hotspot server, masing-masing hotspot server tersebut bisa kita atur menggunakan file / direktori hotspot yang berbeda-beda

Hotspot Customization

- Untuk upload / download file html tersebut kita bisa menggunakan FTP client (ex : filezilla) ataupun drag-n-drop langsung ke komputer (windows only !)
- Apabila terjadi kesalahan konfigurasi file html, kita bisa tekan tombol “Reset HTML” pada menu ip hotspot server

- ***/ip hotspot reset-html***



Reset HTML

RouterOS WinBox

Safe Mode CPU: 0% Hide Passwords

Quick Set
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Make Supout.rif
Manual
Exit

File List

Backup Restore Find

| File Name | Type | Size | Creation Time |
|---------------------------------------|------------|---------|----------------------|
| hotspot | directory | | Oct/25/2012 10:45:51 |
| hotspot/alogin.html | .html file | 1293 B | Oct/25/2012 10:45:51 |
| hotspot/error.html | .html file | 898 B | Oct/25/2012 10:45:51 |
| hotspot/login.html | .html file | 3362 B | Oct/25/2012 10:45:51 |
| hotspot/logout.html | .html file | 1813 B | Oct/25/2012 10:45:51 |
| hotspot/radvert.html | .html file | 1481 B | Oct/25/2012 10:45:51 |
| hotspot/redirect.html | .html file | 318 B | Oct/25/2012 10:45:51 |
| hotspot/rlogin.html | .html file | 850 B | Oct/25/2012 10:45:51 |
| hotspot/status.html | .html file | 3009 B | Oct/25/2012 10:45:51 |
| hotspot/md5.js | .js file | 7.0 KiB | Oct/25/2012 10:45:51 |
| hotspot/errors.txt | .txt file | 3615 B | Oct/25/2012 10:45:51 |
| hotspot/img | directory | | Oct/25/2012 10:45:51 |
| hotspot/img/logobottom.png | .png file | 3925 B | Oct/25/2012 10:45:51 |
| hotspot/lv | directory | | Oct/25/2012 10:45:51 |
| hotspot/lv/alogin.html | .html file | 1303 B | Oct/25/2012 10:45:51 |
| hotspot/lv/login.html | .html file | 3408 B | Oct/25/2012 10:45:51 |
| hotspot/lv/logout.html | .html file | 1843 B | Oct/25/2012 10:45:51 |
| hotspot/lv/radvert.html | .html file | 1475 B | Oct/25/2012 10:45:51 |
| hotspot/lv/status.html | .html file | 2760 B | Oct/25/2012 10:45:51 |
| hotspot/lv/errors.txt | .txt file | 3810 B | Oct/25/2012 10:45:51 |
| hotspot/xml | directory | | Oct/25/2012 10:45:51 |
| hotspot/xml/alogin.html | .html file | 821 B | Oct/25/2012 10:45:51 |
| hotspot/xml/error.html | .html file | 416 B | Oct/25/2012 10:45:51 |
| hotspot/xml/flogout.html | .html file | 361 B | Oct/25/2012 10:45:51 |
| hotspot/xml/login.html | .html file | 787 B | Oct/25/2012 10:45:51 |
| hotspot/xml/logout.html | .html file | 359 B | Oct/25/2012 10:45:51 |
| hotspot/xml/rlogin.html | .html file | 530 B | Oct/25/2012 10:45:51 |
| hotspot/xml/WISPAccessGatewayParam... | .xsd file | 4251 B | Oct/25/2012 10:45:51 |
| skins | directory | | Jan/01/1970 07:00:58 |
| usb1 | disk | | Nov/06/2012 15:38:16 |

30 items 41.9 MB of 520.1 MB used 91% free



HTML Customization

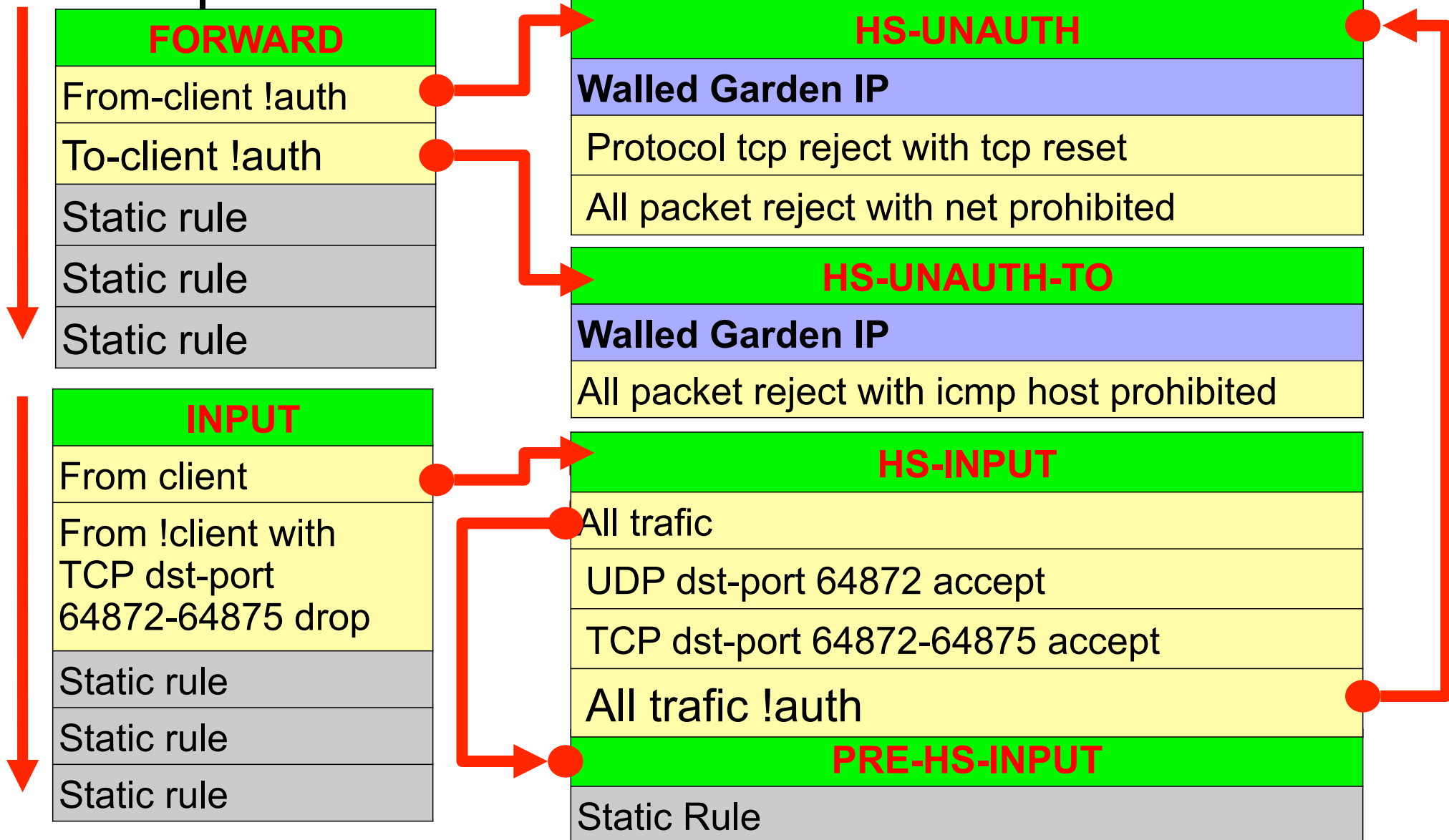
- Ada beberapa halaman html yang berinteraksi langsung dengan user antara lain :
 - Redirect.html : membelokkan user ke halaman lain
 - Login.html : halaman tempat user memasukkan username password
 - md5.js : file javascript untuk mengacak password (jika menggunakan metode autentikasi http-chap)
 - alogin.html : halaman yang ditampilkan setelah user melakukan login
 - status.html : halaman yang menampilkan informasi statistik penggunaan client saat itu juga
 - logout.html : halaman yang menampilkan informasi statistik penggunaan terakhir client setelah melakukan logout
 - error.html : halaman yang digunakan menampilkan pesan error jika terjadi sebuah kesalahan



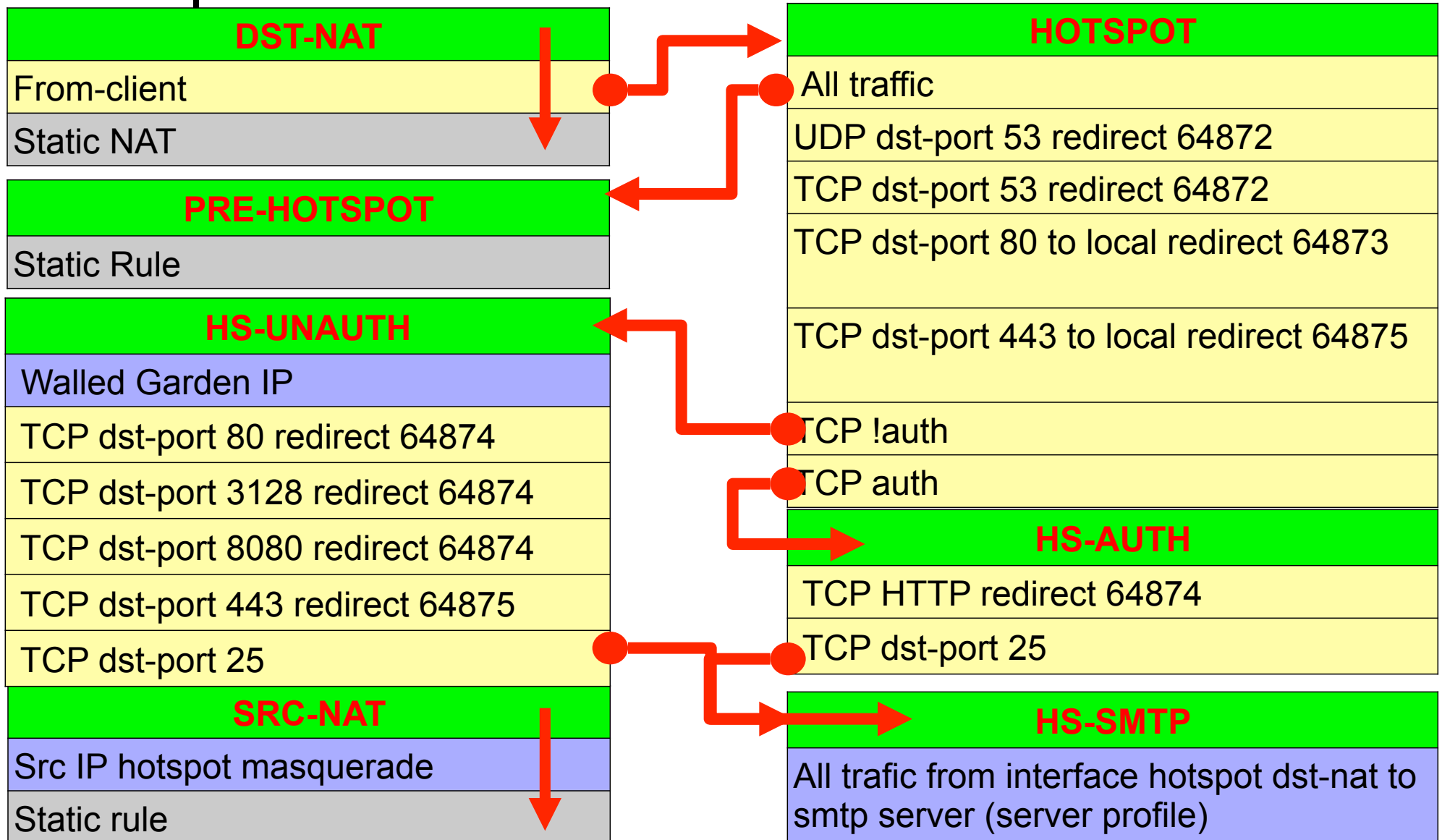
Hotspot Dynamic Rule

- Hotspot gateway pada Mikrotik bisa terbentuk dari kerjasama berbagai fungsi yang ada di router meliputi :
 - Firewall filter
 - Firewall nat
 - Firewall mangle
 - DHCP server + IP Pool
 - Proxy Server
 - DNS Server
 - Queue
- Dari semua rule tersebut akan dibuatkan secara otomatis pada saat kita melakukan SETUP hotspot

Filter Dynamic Rule



NAT Dynamic Rule





RADIUS



Certified Mikrotik Training - Advanced Class (MTCUME)

Organized by: Citraweb Nusa Infomedia

(Mikrotik Certified Training Partner)



Outline

- AAA
- RADIUS Protocol
- RADIUS & NAS
- Radius Communication
- Radius Packet
- Radius Component
- Radius Implementation
- Radius Client
- Radius Incoming

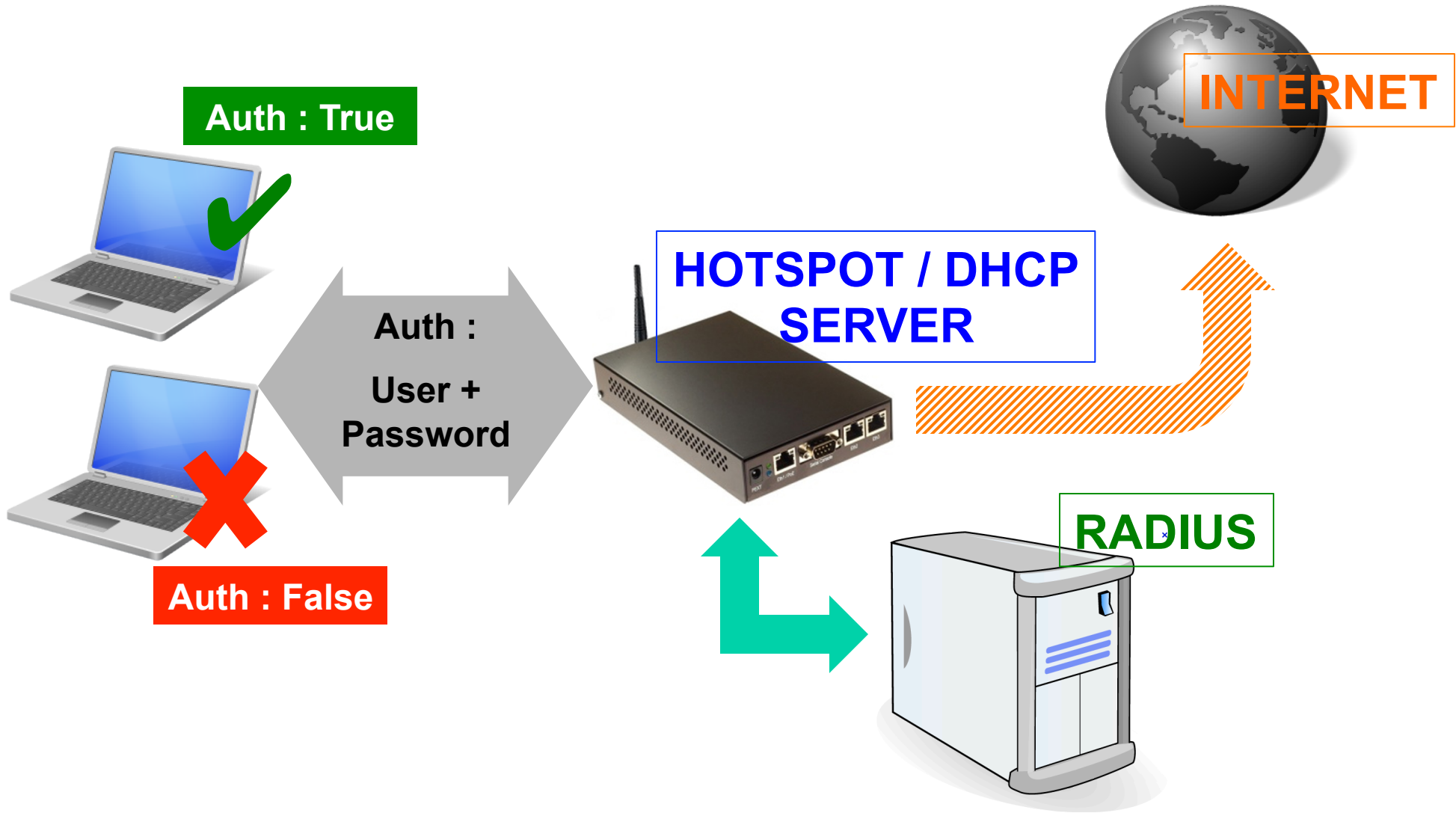
AAA – Security Implementation

- Adalah sebuah konsep security yang diimplementasikan ke dalam sebuah jaringan komputer.
- AAA ini terdiri dari 3 basis prosedur :
 - Authorization
 - Authentication
 - Accounting
- Konsep dan prosedur AAA diterapkan di Protocol RADIUS.

AAA - Authentication

- Adalah Prosedur AAA yang mengatur Verifikasi atau validitas dari user.
- Berbagai aspek dari user bisa digunakan untuk menentukan user tersebut adalah user yang valid.
 - ID's (KTP, NIK dll)
 - Username + Password
 - Physical Token
 - Biometric Measure (Fingerprint, Retina Scanner)

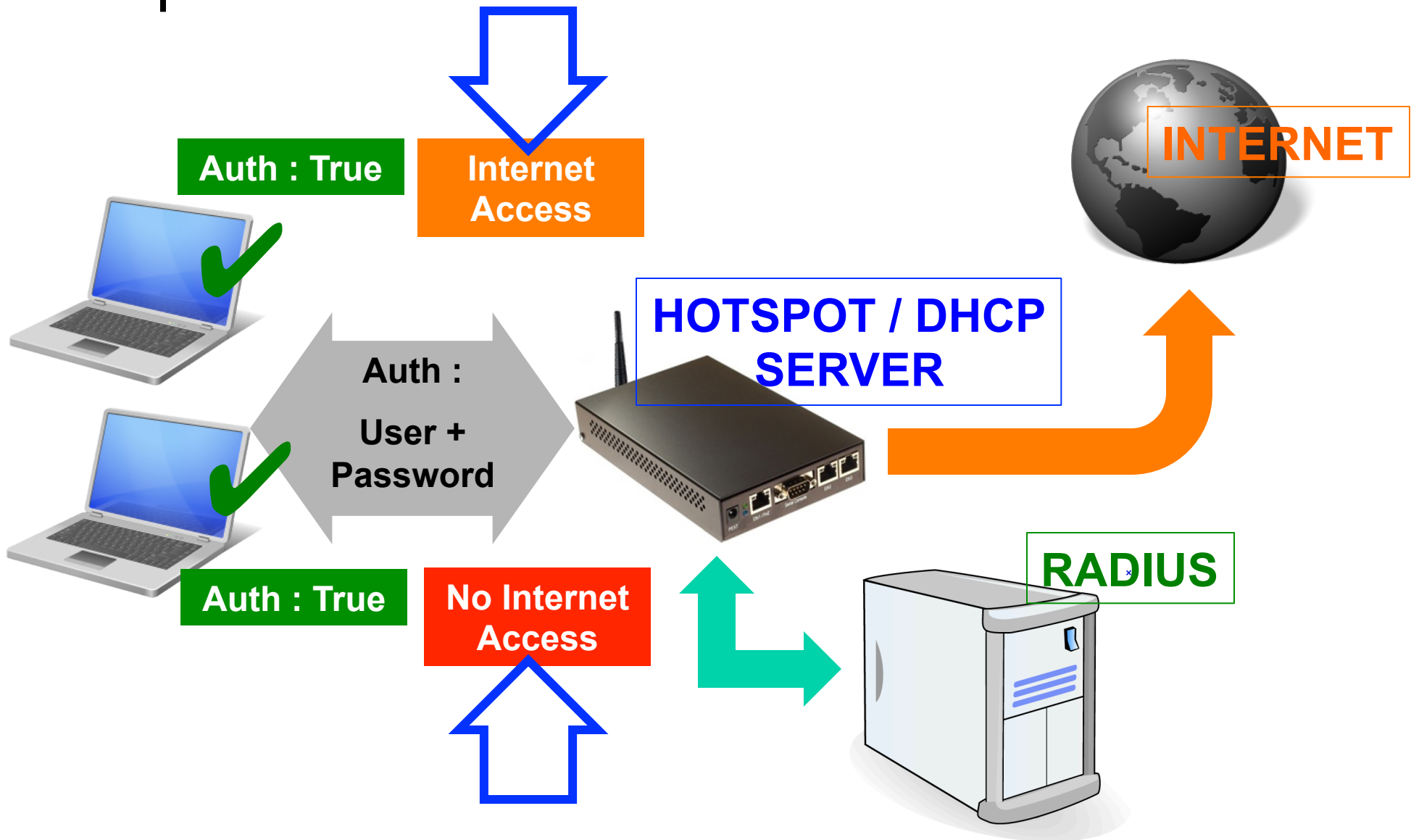
Authentication Challenge



AAA - Authorization

- Adalah Prosedur AAA yang mengatur apa saja yang user bisa lakukan ke dalam system tersebut, setelah berhasil dan melewati proses Authentication.
- Pada dasarnya adalah privilege user :
 - Internet Access Control
 - Data Access Control
 - Restrictions
 - Type Of Service

Authorization Decision

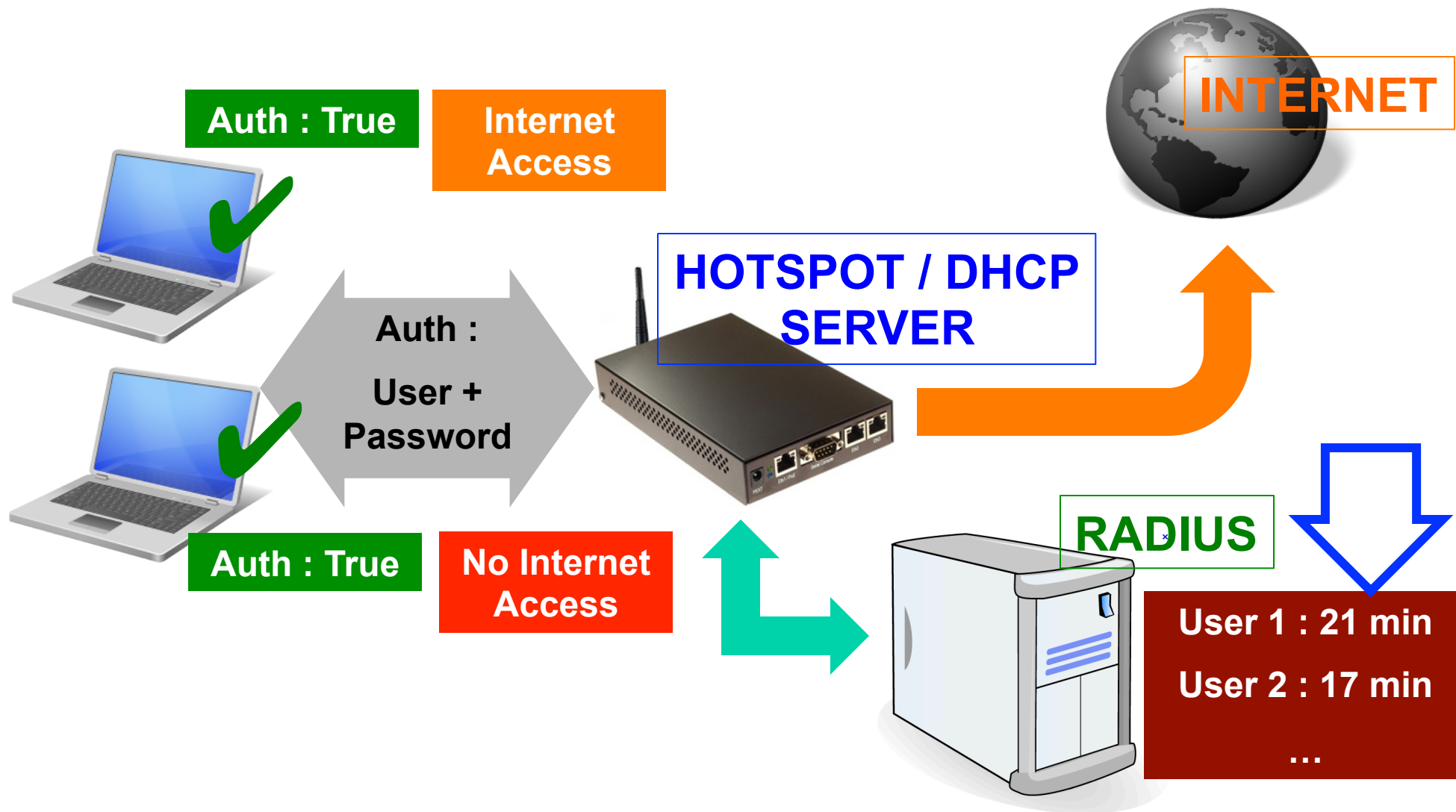




AAA - Accounting

- Adalah Prosedur AAA yang melakukan pencatatan terhadap apa saja yang dilakukan User.
- User Accounting :
 - Traffic
 - Time
 - Session
 - Log
- Biasanya digunakan untuk management atau billing.

Accounting Database





RADIUS Protocol

- Protocol Radius adalah sebuah protocol yang mengatur mekanisme pengimplementasian konsep AAA dari berbagai NAS (Network Access Server) ke dalam sebuah server yang terpusat.
- Memungkinkan untuk menggunakan hanya 1 database untuk menyimpan data Authentication (username, password), Athorization (profile, user restriction), dan Accounting (session, log) dari berbagai service yang diberikan oleh NAS.
- Data Radius diencapsulasi ke dalam UDP Datagram



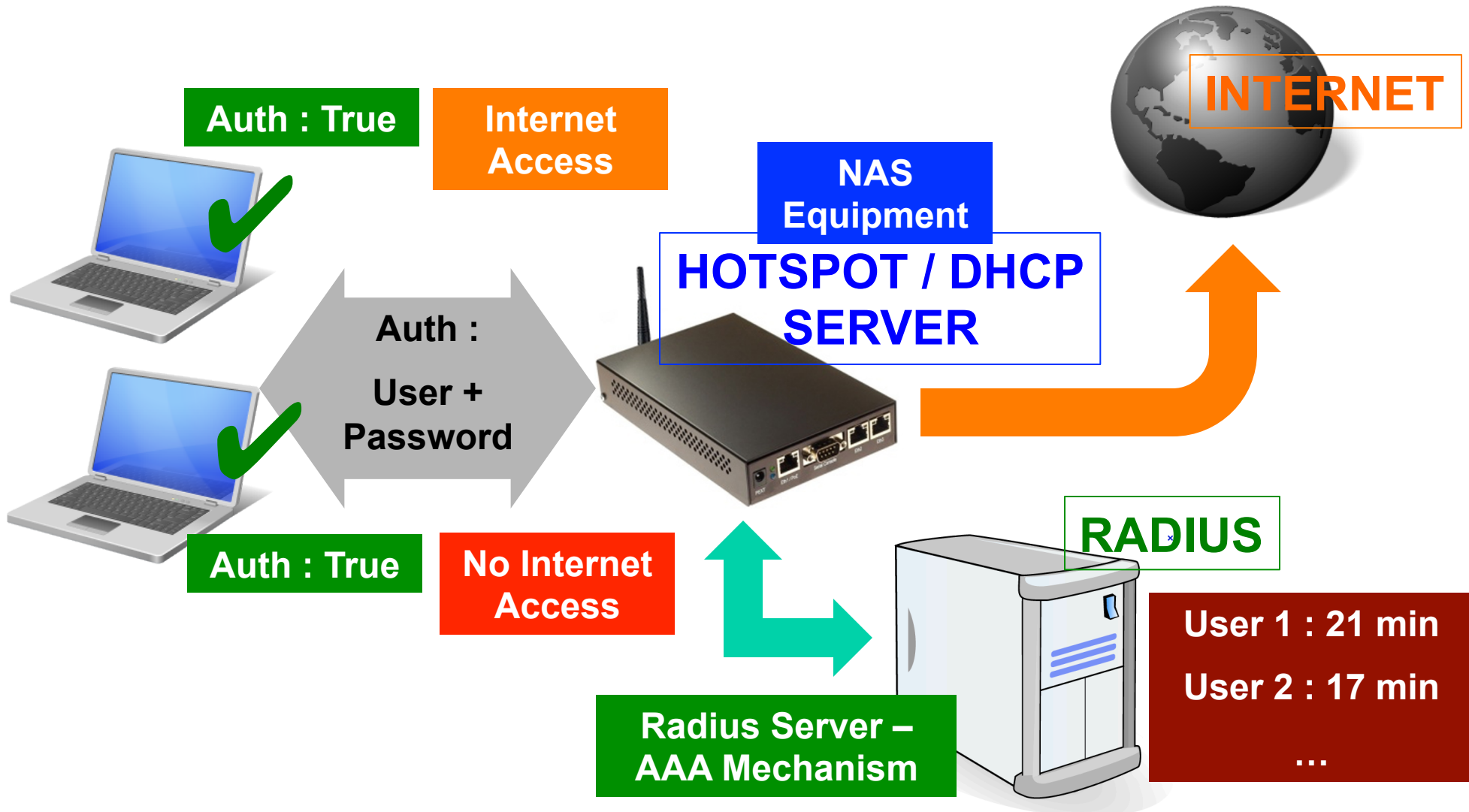
RADIUS Benefit

- Management user dan security menjadi lebih mudah karena sudah terpusat di sebuah server.
- Tidak memerlukan management user di NAS.
- Management yang sudah terpusat sehingga biaya bisa lebih di hemat.
- Radius bisa dikombinasikan dengan berbagai Access Method (Hotspot, PPTP, PPPoE, Wireless, DHCP dll)

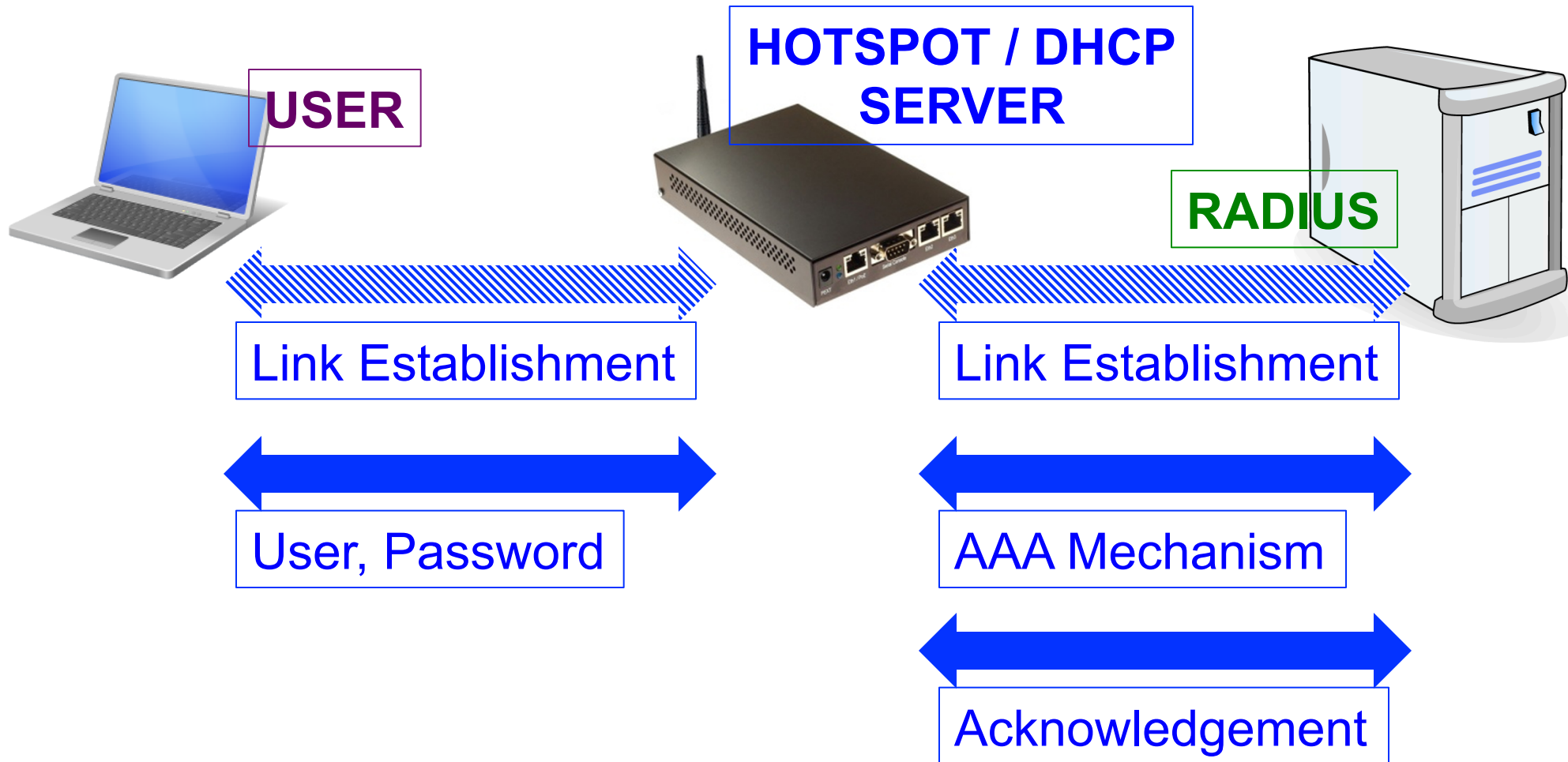
NAS – Network Access Server

- NAS adalah sebuah perangkat yang memiliki dua interkoneksi (terletak diantara jaringan yang terproteksi dan jaringan user yang tidak terproteksi).
- NAS ini adalah sebuah perangkat perantara di mana user harus terkoneksi dengan perangkat NAS tersebut secara langsung dan harus melewati proses / mekanisme AAA supaya bisa menggunakan resource jaringan yang dibutuhkan oleh user.

RADIUS & NAS



RADIUS - Communication

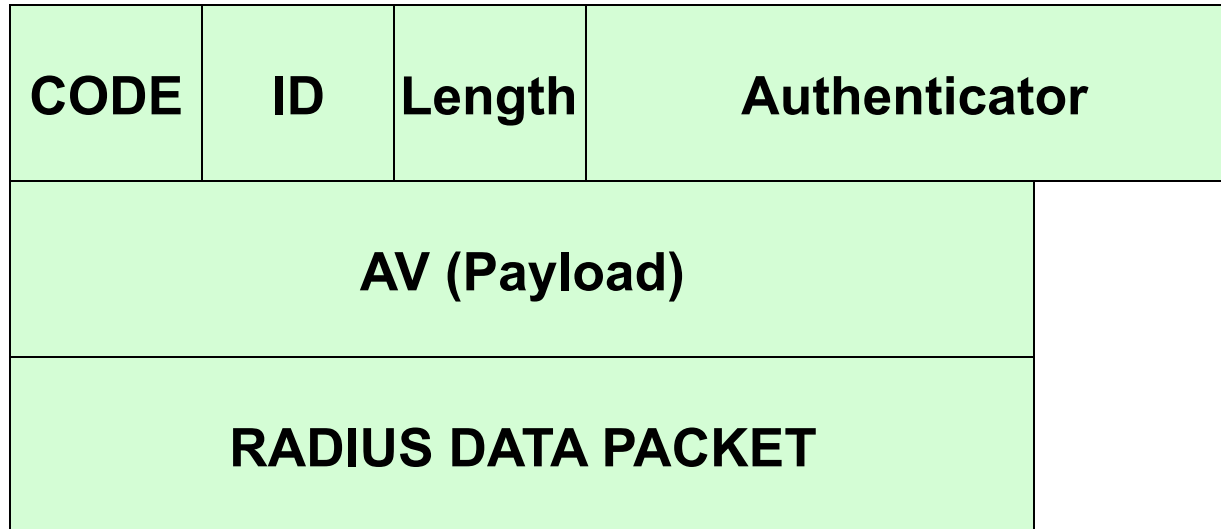




RADIUS Packet

- ACCESS-REQUEST (1)
- ACCESS-RESPONSE (2)
- ACCESS-REJECT (3)
- ACCESS-CHALLENGE (11)
- ACCOUNTING-REQUEST (4)
- ACCOUNTING-RESPONSE (5)
- STATUS-SERVER (12)
- STATUS-CLIENT (13)

RADIUS Packet - Detail



- Code : as above
- ID (Identifier) : Untuk penghubungan otomatis antara request dan reply.
- Length : Valid Range 20 – 4096
- Authenticator : untuk menyembunyikan password (MD5), Request menggunakan random Number / Response menggunakan Authenticator

RADIUS Packet – Detail Example

RADIUS Request - Access

| | | | |
|---------------------------------------------------------------|------------------|----------------------------------|--------------------------------------------|
| CODE (1) | ID (q) | Length (Header + Payload) | Authenticator (Request) (Random) |
| Attributes : User, NAS-IP, (MD5)Password, CHAP PWD | | | |

RADIUS Response – Access Accept

| | | | |
|---------------------------------------------------------------------------|------------------|----------------------------------|----------------------------------------------------------------------------------------------------|
| CODE (2) | ID (q) | Length (Header + Payload) | Authenticator (Response) = MD5 (Code + ID + req.Authenticator + Attribute and Secret) |
| Attributes : (All optional) Services Authorized (varies) | | | |

RADIUS Packet – Detail Example

RADIUS Response – Access Reject

| | | | |
|--------------------------------|-------------------------------|--------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| CODE (3) | ID(q per transmission) | Length (Header + Payload) | Authenticator (Response) = MD5 (Code + ID + req.Authenticator + Attribute and Secret) |
| Attributes : (optional) | | | |



RADIUS - Component

- Client / Server Model
 - NAS (Client) \leftrightarrow Radius Server
- UDP Based
- Hop by Hop Security (Secret)
- Stateless
- Uses MD5 for Password Hiding
- A-V Pairs (Attribute Value for various Vendor)
 - MIKROTIK, CISCO, Windows Server, Samba etc



RADIUS – Implementation (Server)

- Livingston
- GNU
- FreeRADIUS
- Cistron
- Radiator
- Alepo
- Juniper: Steel Belt.
- Mikrotik User Manager



Radius Client

- Mikrotik RouterOS sudah support sebagai Radius Client. Konfigurasinya ada di menu “Radius”.
- Service RouterOS yang bisa disupport dengan Radius adalah :
 - RouterOS Login
 - Hotspot
 - PPP (PPTP, L2TP, PPPoE, OVPN dll)
 - DHCP Leases
 - Wireless Access List



Interraces
Wireless
Bridge
PPP
Switch
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Make Supout.rif

Radius

New Radius Server

General | Status

– Service –

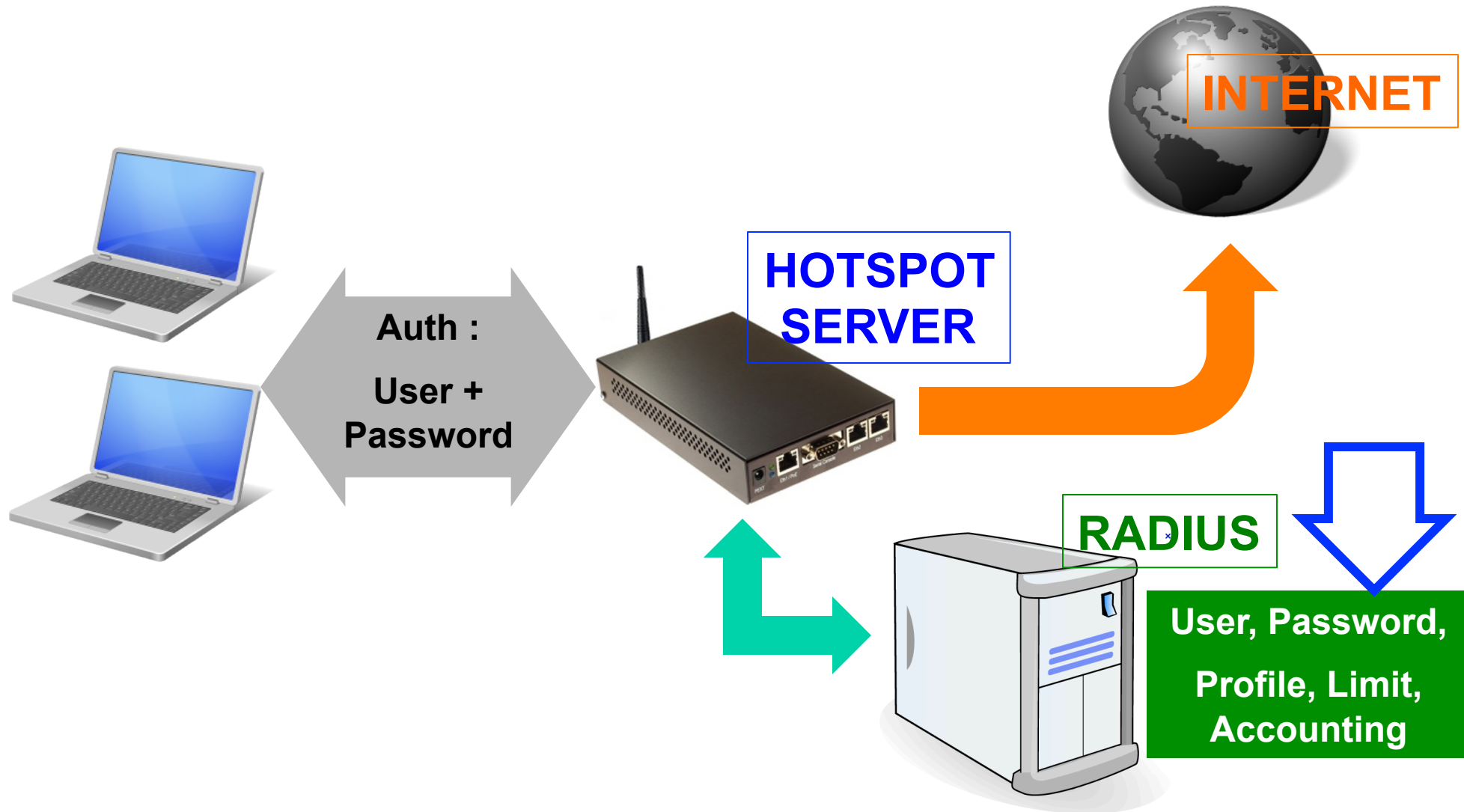
ppp login
 hotspot wireless
 dhcp

Called ID:
Domain:
Address:
Secret:

Authentication Port:
Accounting Port:
Timeout: ms

Accounting Backup
Realm:
Src. Address:

RADIUS Client - Hotspot



Radius Client – Hotspot Config

Hotspot Server Profile <hsprof1 >

General Login **RADIUS**

Use RADIUS

Default Domain:

Location ID:

Location Name:

MAC Format:

Accounting

Interim Update:

NAS Port Type:

Radius Server <192.168.130.1 >

General Status

Service

ppp login

hotspot wireless

dhcp

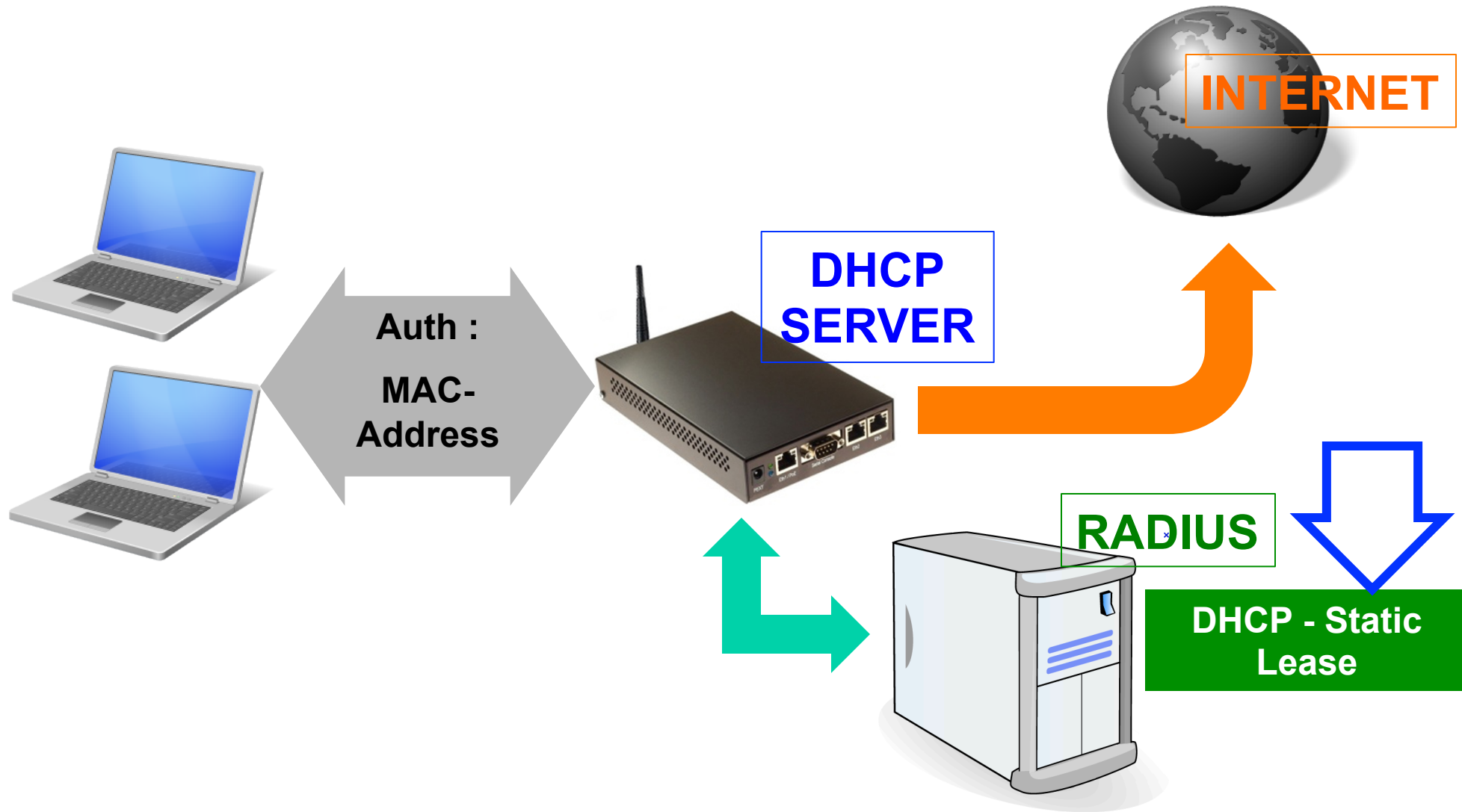
Called ID:

Domain:

Address:

Secret:

RADIUS Client – DHCP Server



Radius Client – DHCP Server

DHCP Server <dhcp1>

Name:

Interface: ▾

Relay: ▾

Lease Time:

Bootp Lease Time: ▾

Address Pool: ▾

Src. Address: ▾

Delay Threshold: ▾

Authoritative: ▾

Bootp Support: ▾

Add ARP For Leases

Always Broadcast

Use RADIUS

Radius Server <192.168.130.1>

General | Status

– Service –

ppp login

hotspot wireless

dhcp

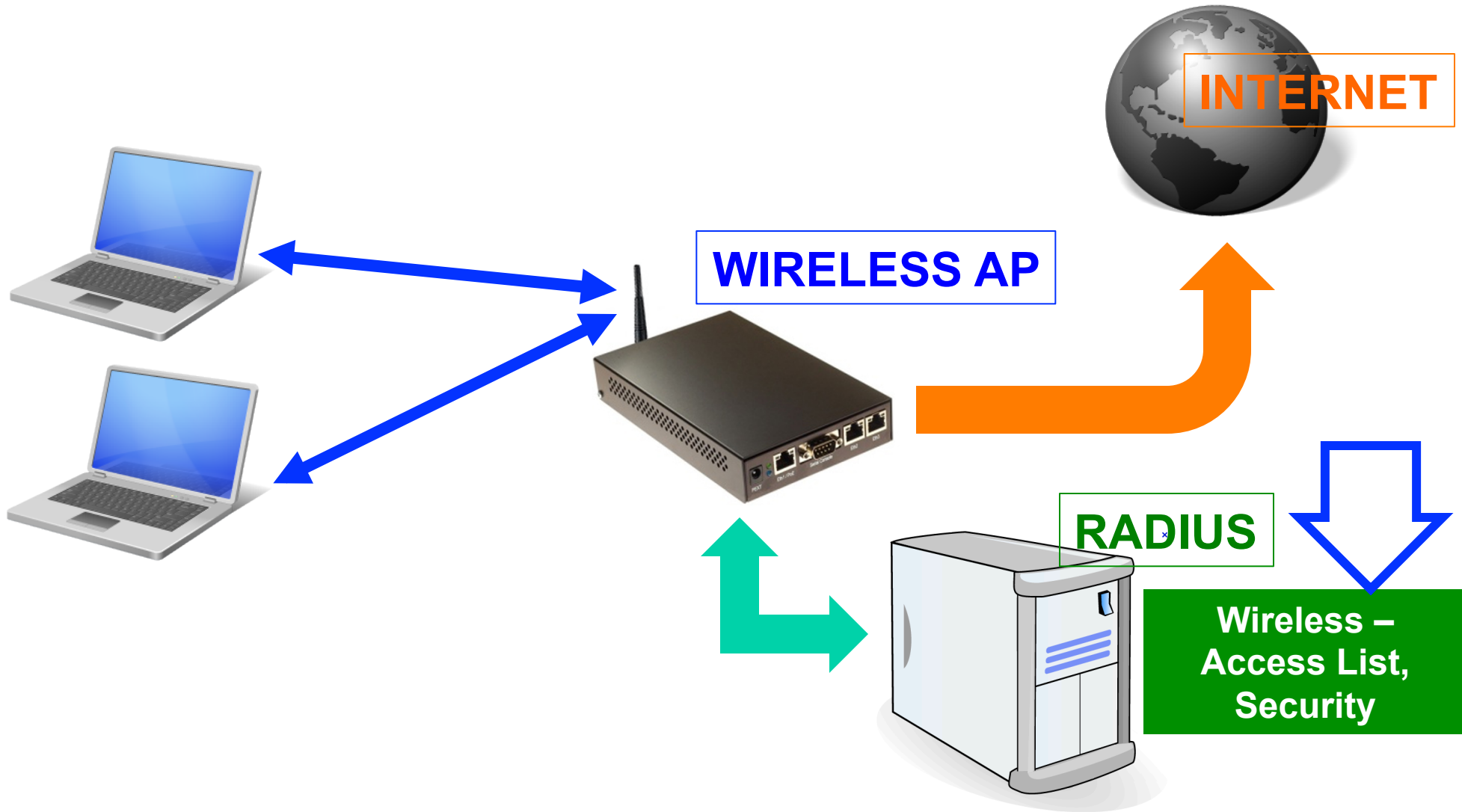
Called ID: ▾

Domain: ▾

Address:

Secret:

RADIUS Client – Wireless ACL



Radius Client – Wireless Config

Security Profile <default>

General RADIUS EAP Static Keys

MAC Authentication

MAC Accounting

EAP Accounting

Interim Update: 00:00:00

MAC Format: XX:XX:XX:XX:XX:XX

MAC Mode: as username

MAC Caching Time: disabled

Radius Server <192.168.130.1>

General Status

Service

ppp login

hotspot wireless

dhcp

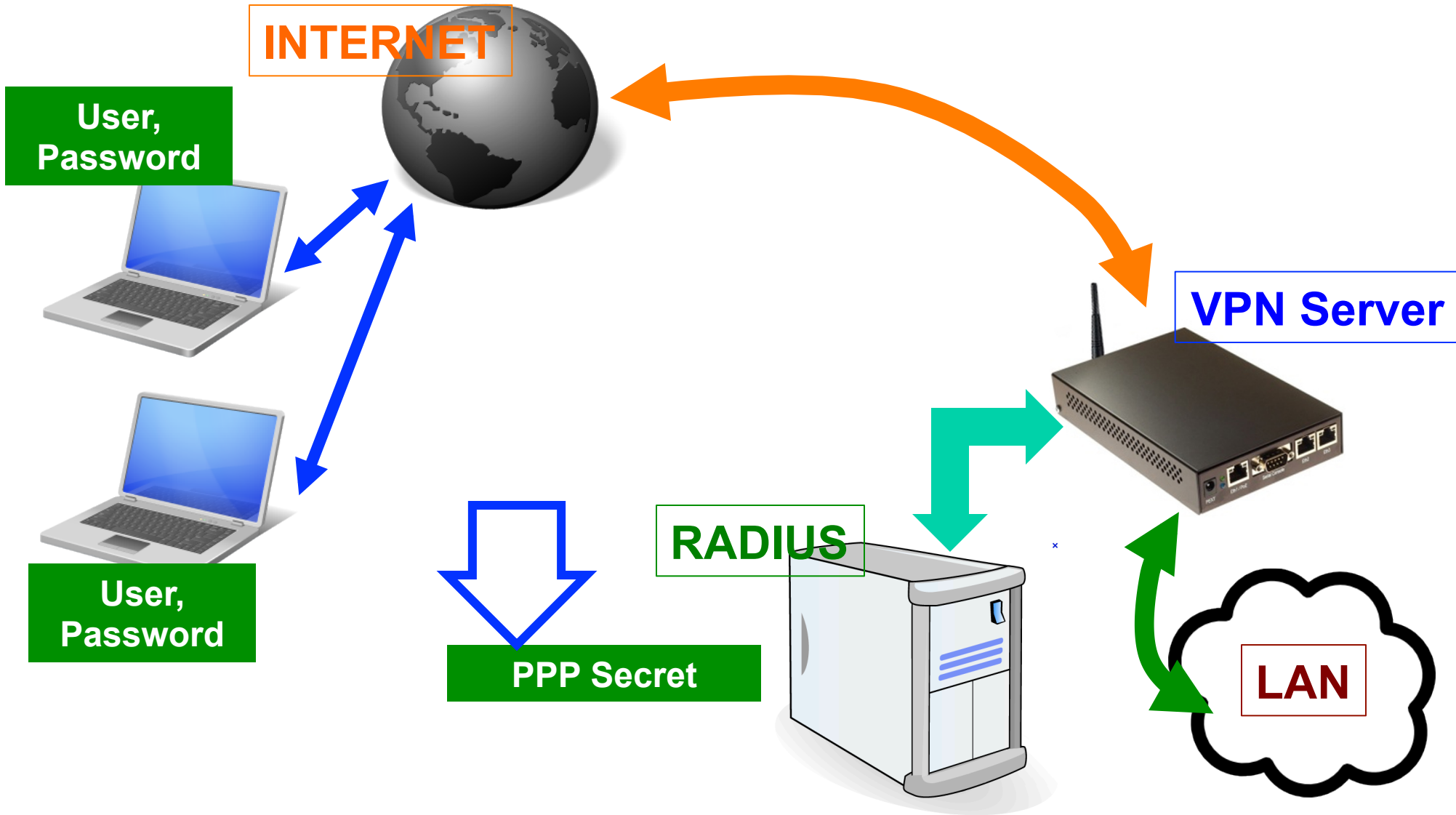
Called ID:

Domain:

Address: 192.168.130.1

Secret: rahasia

RADIUS - Implementation



Radius Client – VPN Server

PPP Authentication & Accounting

Use Radius

Accounting

Interim Update:

Radius Server <192.168.130.1>

General Status

– Service

- PPP login
- hotspot wireless
- dhcp

Called ID:

Domain:

Address: 192.168.130.1

Secret: rahasia

Radius Incoming

- Adalah Fitur yang memungkinkan sebuah Radius Server mengirimkan pesan-pesan penolakan yang dikirim ke Radius Client.
- Pesan penolakan ini memperpanjang perintah RADIUS protokol, yang memungkinkan untuk mengakhiri sesi yang telah terhubung dari server RADIUS.
- Untuk tujuan ini Pesan DM (Disconnect Message) digunakan yang menyebabkan sesi user segera diakhiri.

Radius

Buttons: +, -, ✓, ✗, 📁, 🌊, Reset Status, Incoming, Find

| # | Service | Called ID | Domain | Address | Secret |
|---|--------------|-----------|--------|---------------|---------|
| 0 | ppp wireless | | | 192.168.130.1 | rahasia |

Radius Incoming

Accept

Port: 3799

Requests: 0

Bad Requests: 0

Acks: 0

Naks: 0

Buttons: OK, Cancel, Apply, Reset Status

Radius Incoming Tips&Trik !

- Pesan DM akan hanya berlaku pada service yang menggunakan sesi (Session):
 - HOTSPOT
 - VPN (PPTP, PPPoE, L2TP dll)
- Port Radius Incoming yang disupport oleh User Manager adalah port 1700
- Aktifkan CoA pada UserManager



Quiz !

- OVPN (Open VPN) Authentication bisa menggunakan Radius (Ya/Tidak)
- Radius Incoming bisa digunakan untuk memutus koneksi client wireless yang Access List Pada sebuah AP wireless tersebut menggunakan Radius Authorization ? (Ya/Tidak)



Mikrotik User Manager



Certified Mikrotik Training - Advanced Class (MTCUME)

Organized by: Citraweb Nusa Infomedia
(Mikrotik Certified Training Partner)



Outline

- Mikrotik UserManager
- UserManager Installation
- UserManager Main Components
 - Customers
 - Routers
 - Users
 - Profile
 - Session
 - Report
- UserManager Example Config

Mikrotik UserManager

- UserManager adalah sebuah Radius Server yang dikembangkan oleh Mikrotik untuk memperkaya fungsi dari Mikrotik RouterOS.
- Adalah Software Add-on berbentuk paket (*.npk) tambahan yang tidak termasuk dalam Paket basic RouterOS.
- RoS v.3/4/5/6 Supported
 - Versi UserManager Harus sama dengan versi RoS !



UserManager Features

- Web Interface Configuration
- Supported Service:
 - Hotspot
 - VPN
 - DHCP
 - Wireless
 - RoS Login
- Backup / restore Database
- Report & Voucher Generator
- RoS External Disk storage
- Radius Incoming Supported (v.4/5/6)
- Customize LOGO & Template
- Payment Gateway (Paypal & Authorize.net)

UserManager Installation (1)

- Hardware :

- 32 MB RAM (Minimum)
- 2MB on hard drive (more recommended)
- x86 architecture / All RouterBOARDS

- UserManager Package :



Upgrade package



All packages



Netinstall



Torrent



Changelog



MD5

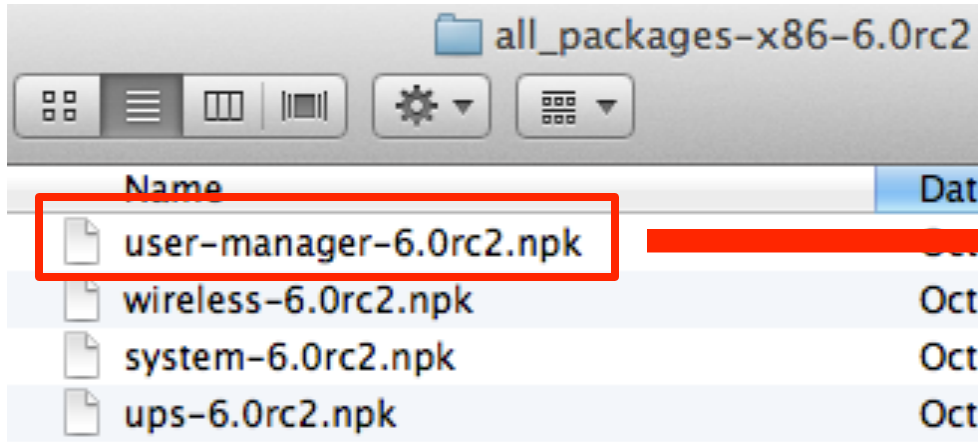


UserManager Installation (2)

- RouterOS license;
 - **Level 0** – 0 active sessions
 - **Level 1** – 0 active sessions
 - **Level 3** – 10 active sessions
 - **Level 4** – 20 active sessions
 - **Level 5** – 50 active sessions
 - **Level 6** – Unlimited

UserManager Installation (3)

- Upload package to the router, pastikan menggunakan versi yang sama !



Drag Drop (Windows), FTP, SCP



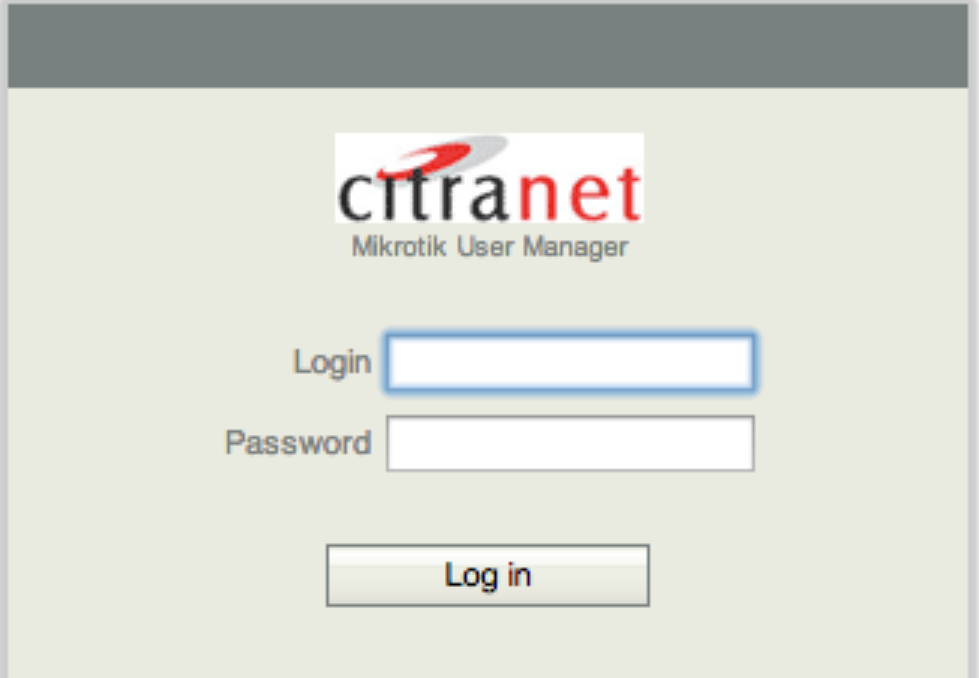
RoS v6.0rc2

UserManager Installation (3)

- Check the Installation :
- Console (CLI) :

```
[admin@ro-utama-mki] > /tool user-manager  
customer database history log payment router session user export
```

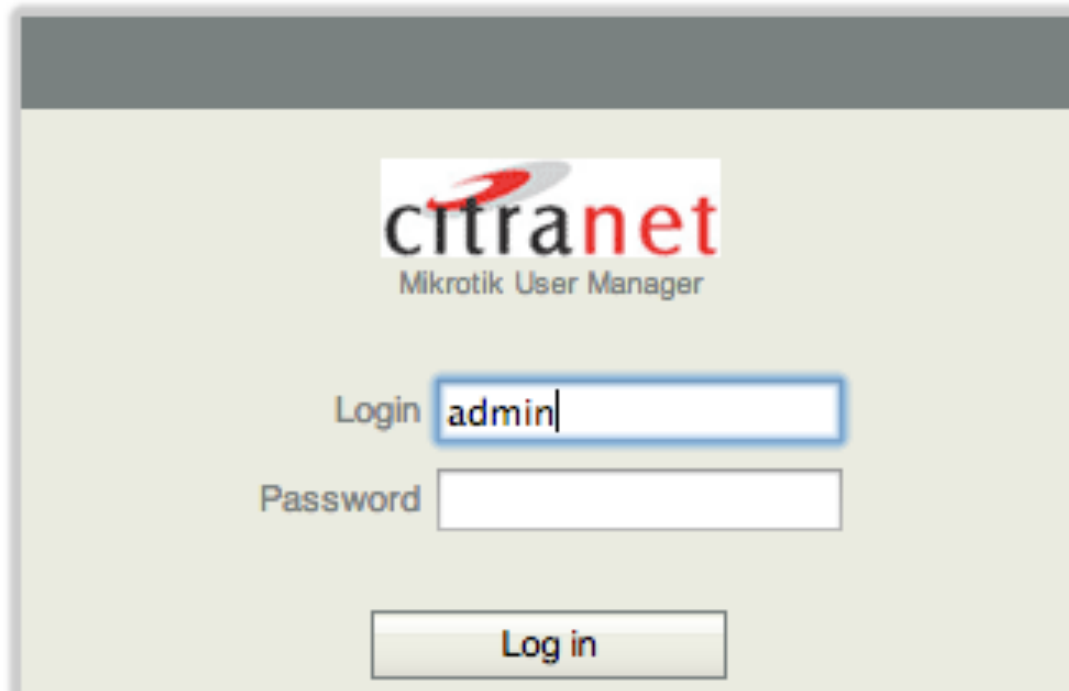
- Web Interface : <http://ip-router/userman>



The screenshot displays the web interface for Mikrotik User Manager. At the top center is the 'citranet' logo with the text 'Mikrotik User Manager' below it. Below the logo are two input fields: 'Login' and 'Password'. A 'Log in' button is positioned at the bottom center of the form area.

UserManager First Access

- Default Username : Admin Password: -
- **Customer** adalah Level admin dari UserManager.
- UserManager tidak berhubungan dengan User di Internal Router.



The image shows a web interface for Mikrotik User Manager. At the top center is the 'citranet' logo, with 'Mikrotik User Manager' written below it. Below the logo are two input fields. The first is labeled 'Login' and contains the text 'admin'. The second is labeled 'Password' and is empty. At the bottom of the form is a button labeled 'Log in'.

UserManager First Access



- Routers
- Users**
- Sessions
- Customers
- Logs
- Payments
- Profiles
- Settings
- Reports
- 0 A sessions
- 0 A users
- Advanced search
- Maintenance
- Logout

| Add Edit Generate | | | |
|--------------------------|--------------|------------|------------------|
| 1 | 2 | 3 | page 1 of 3 |
| <input type="checkbox"/> | ▽ First name | ▽ Username | ▽ Actual profile |
| <input type="checkbox"/> | pujo | 00: | wireless-profil |
| <input type="checkbox"/> | tso-bayu | D0: | wireless-profil |
| <input type="checkbox"/> | tso-listanto | 68: | wireless-profil |
| <input type="checkbox"/> | mas deb | 78: | wireless-profil |
| <input type="checkbox"/> | ibm tso | 00: | wireless-profil |
| <input type="checkbox"/> | pak iwan | D8: | wireless-profil |
| <input type="checkbox"/> | tso-yuli | D0: | wireless-profil |
| <input type="checkbox"/> | | 14: | wireless-profil |
| <input type="checkbox"/> | tso | 00: | wireless-profil |
| <input type="checkbox"/> | tso | 68: | wireless-profil |
| <input type="checkbox"/> | irwan | 70: | wireless-profil |
| <input type="checkbox"/> | bb pujo | 80: | wireless-profil |
| <input type="checkbox"/> | mas nov | D8: | wireless-profil |
| <input type="checkbox"/> | tso | D0: | wireless-profil |
| <input type="checkbox"/> | tso | D0: | wireless-profil |
| <input type="checkbox"/> | janu BB | 68: | wireless-profil |
| <input type="checkbox"/> | Yoga BB | 80: | wireless-profil |

UserManager Customers

- Routers
- Users
- Sessions
- Customers**
- Logs
- Payments
- Profiles
- Settings
- Reports
- 0 A sessions
- 0 A users
- Advanced search
- Maintenance
- Logout

Customer details

▲ Main

Login:

Password:

Disabled:

Parent: admin

Permissions:

Public ID:

Public host:

Backup allowed:

▼ Access

▼ Private information

▼ Signup options

▼ Format

- Read only
- Read write
- Full
- ✓ Owner**

- Permission "Owner" adalah level paling tinggi.
- Hanya boleh ada 1 Customer dengan permission "Owner" dalam UserManager

Customers Permissions

| | Read-only | Read-write | Full | Owner | | Read-only | Read-write | Full | Owner |
|-------------|-----------|------------|------|-------|---------------|-----------|------------|------|-------|
| View | | | | | Add | | | | |
| Routers | + | + | + | + | Routers | | + | + | + |
| Credits | + | + | + | + | Credits | | + | + | + |
| Users | + | + | + | + | Users | | + | + | + |
| Sessions | + | + | + | + | Sessions | | | | + |
| Customers | | | + | + | Customers | | | | |
| Reports | + | + | + | + | Remove | | | | |
| Logs | + | + | + | + | Routers | | | + | + |
| Edit | | | | | Credits | | | + | + |
| Routers | | + | + | + | Users | | | + | + |
| Credits | | | + | + | Customers | | | | + |
| Users | | + | + | + | Sessions | | | + | + |
| Customers | | | | + | Logs | | | + | + |

| Specific actions | | | |
|-------------------------|---|---|---|
| Reset user counters | | + | + |
| Reset router counters | + | + | + |
| Remove last user credit | + | + | + |
| Close active sessions | + | + | + |

Customers (1)

▲ Main

Login:

Password:

Disabled:

Parent: admin

Permissions:

Public ID:

Public host:

Backup allowed:

- Login & Password : Untuk menggunakan web interface
- Parent : Customers yang memiliki level hirarki di atasnya.
- Permission : limitasi kemampuan customers

- Public ID : Identifikasi Customer Untuk digunakan pada user sign-up.
- Public Host : IP Public / website yang valid dari UserManager.
- Backup Allowed : Boleh melakukan backup database

Customers (2)

▲ Access

| | |
|-------------------------------------|----------------------------------------------------------------|
| <input checked="" type="checkbox"/> | Own routers |
| <input type="checkbox"/> | Parents routers |
| <input checked="" type="checkbox"/> | Own users |
| <input type="checkbox"/> | Parents users |
| Access: | <input checked="" type="checkbox"/> Own profiles |
| | <input type="checkbox"/> Parents profiles |
| | <input checked="" type="checkbox"/> Own limitations |
| | <input type="checkbox"/> Parents limitations |
| | <input checked="" type="checkbox"/> Configure payment gateways |
| | <input type="checkbox"/> Use parent payment gateways |

- Own Access : Boleh membuat Data sendiri
- Parent Access : Boleh menggunakan data dari parent

Customers (3)

▲ Private information

Company:

City:

Country:

Email:

▲ Signup options

Signup allowed:

▲ Format

Currency:

Time zone:

- Private Information : Informasi Tambahan dari Customers
- Signup Options : Boleh mengaktifkan halaman SignUp
- Format : Menentukan Mata uang dan Time Zone

UserManager - Router

Routers

Users

Sessions

Customers

Logs

Payments

Profiles

Settings

Reports

0 A sessions

0 A users

Advanced search

Maintenance

Logout

Router details

△ Main

Name:

Owner:

IP address:

Shared secret:

Time zone:

Disabled:

Authorization success

Log events:

Authorization failure

Accounting success

Accounting failure

▲ Radius incoming

CoA support:

Use CoA

CoA port:

Router = NAS

- UserManager Router = Radius NAS (Network Access Server)
- Name : Identitas Router
- Owner : Identitas Customer
- IP Address : IP address dari router yang akan menggunakan UserManager
- Shared Secret : Key Password
- Radius Incoming – hanya untuk router yang sudah support Radius Incoming
 - Use CoA – jika Router support CoA (Mikrotik sudah support)
 - CoA Port – Mikrotik support dengan port 1700

UserManager Profile

Routers

Users

Sessions

Customers

Logs

Payments

Profiles

Settings

Reports

0 A sessions

0 A users

Advanced search

Maintenance

Logout

Profiles

Limitations

Profile: wireless-profil +

Name: wireless-profil

Name for users:

Owner: admin

Validity:

Starts: Now

Price: 0.00

Save profile

Remove profile

Profile limitations

Active

Always

Add new limitation

Remove selected limitations

UserManager Profile - Limitation

- Routers
- Users
- Sessions
- Customers
- Logs
- Payments
- Profiles**
- Settings
- Reports
- 0 A sessions
- 0 A users
- Advanced search
- Maintenance
- Logout

▲ Main

Name:

Owner:

▲ Limits

Download:

Upload:

Transfer:

Uptime:

▲ Rate limits

Rate limit: Rx Tx

Burst rate: Rx Tx

Burst threshold: Rx Tx

Burst time: Rx Tx

Min rate: Rx Tx

Priority:

▲ Constraints

Group name:

IP pool:

Address list:

UserManager – Users (1)

- Routers
- Users**
- Sessions
- Customers
- Logs
- Payments
- Profiles
- Settings
- Reports
- 0 A sessions
- 0 A users
- Advanced search
- Maintenance
- Logout

▲ Main

Username:

Password:

Disabled:

Owner:

▲ Constraints

IP address:

Bind on first use

Caller ID:

Shared users:

▲ Wireless

Preshared key:

Enc key:

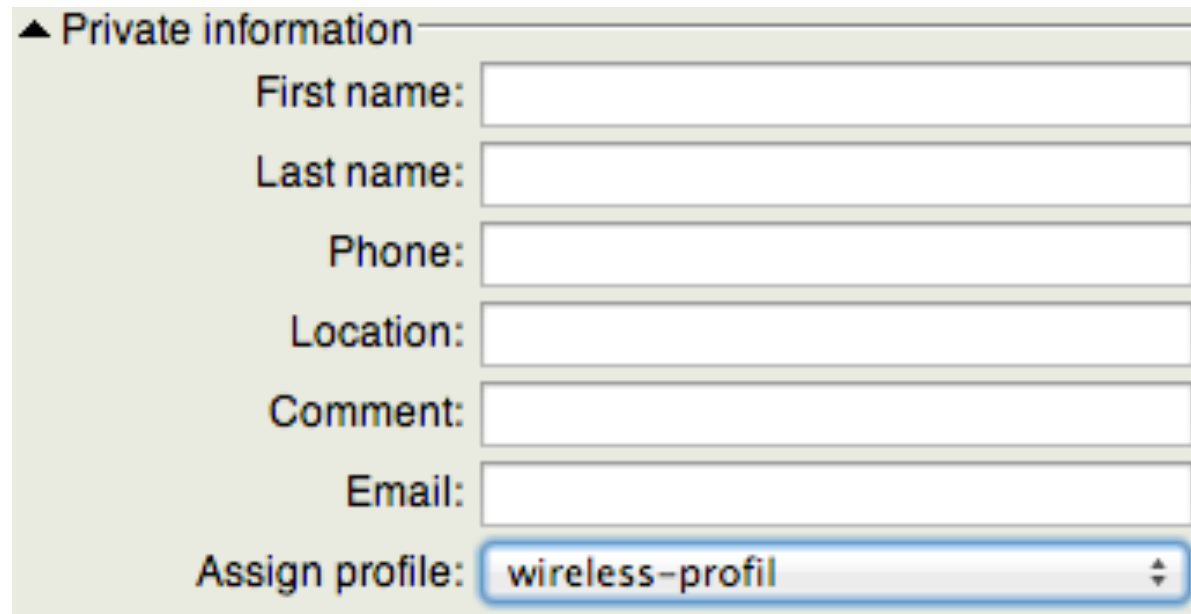
Enc algo:

UserManager – Users (2)

- Username & Password : Informasi login untuk akses user
- Owner : Identitas Customers
- Constrain - Batasan untuk user
 - IP address – user menggunakan ip address tertentu
 - Shared User – limit jumlah multi-login
- Wireless – limitasi untuk access-list wireless

UserManager – Users (3)

- Private Information – Informasi tambahan untuk profil user.
- Assign Profile – Profile yang digunakan ketika user tersebut login



▲ Private information

First name:

Last name:

Phone:

Location:

Comment:

Email:

Assign profile:

UserManager – Users (add Batch)

The screenshot displays the Citranet User Manager interface. On the left, a sidebar contains navigation buttons for 'Routers', 'Users', and 'Sessions'. The 'Users' button is highlighted. The main area is divided into two sections. The top section, titled 'Add Edit Generate', contains a table with columns for 'Batch' and 'First name'. The 'Batch' column has a red box around the 'Batch' header and a checkbox. The 'First name' column has a red box around the text 'tablet pujo'. The bottom section, titled 'User details', contains a form with various fields. A red box highlights the 'Owner' dropdown menu (set to 'admin'), the 'Number of users' text input (set to '999'), the 'Username prefix' text input (set to 'userku'), the 'Username length' dropdown menu (set to '6'), and the 'Password length' dropdown menu (set to '8'). Other fields include 'Pwd same as login' (checkbox), 'Assign profile' (dropdown menu set to 'wireless-profil'), and an 'Add' button at the bottom right.

- UserManager mampu membuat multiple user dengan sekali perintah.

UserManager – Generate Voucher

| Add | | Edit | Generate |
|-------------------------------------|-------------|----------|-------------------|
| 1 | 2 | 3 | page 3 |
| <input type="checkbox"/> | ▽ First | CSV File | Vouchers |
| <input type="checkbox"/> | tablet pujo | | ▽ Username |
| <input type="checkbox"/> | | | 00:08:D2:12:84:58 |
| <input type="checkbox"/> | | | test |
| <input checked="" type="checkbox"/> | | | userkuebdinp |
| <input checked="" type="checkbox"/> | | | userkuxutknm |
| <input checked="" type="checkbox"/> | | | userkuwpw7q6 |
| <input checked="" type="checkbox"/> | | | userku2567wn |
| <input checked="" type="checkbox"/> | | | userkuzfq4n2 |
| <input checked="" type="checkbox"/> | | | userkuwfx7cr |
| <input checked="" type="checkbox"/> | | | userkumrc98q |
| <input checked="" type="checkbox"/> | | | userkubs6qak |
| <input checked="" type="checkbox"/> | | | userkuq5gipe |
| <input checked="" type="checkbox"/> | | | userkuu9483u |



UserManager – Generate Voucher

Prepaid time: **Unlimited**

Login: **userkuebdinp**

After attempting to open a web page, you should enter this login information

Login: **userkuebdinp** (login name that you enter at the HotSpot login page)

Password: **ym5ubu** (password that you enter at the HotSpot login page)

If you want to extend time, please contact reception

Prepaid time: **Unlimited**

Login: **userkuxutknm**

After attempting to open a web page, you should enter this login information

Login: **userkuxutknm** (login name that you enter at the HotSpot login page)

Password: **xnf9he** (password that you enter at the HotSpot login page)

If you want to extend time, please contact reception

UserManager Session

- UserManager Session adalah database history dari session user yang sudah digunakan

A vertical menu with the following items: Routers, Users, Sessions (highlighted with a red border), Customers, Logs, Payments, Profiles, and Logout.

| <input type="checkbox"/> | ▼ Username | ▼ Status | ▼ User IP | ▼ From time | ▼ Till time | ▼ Uptime | ▼ Download | ▼ Upload |
|--------------------------|------------|------------------------|--------------|------------------------|------------------------|----------|------------|----------|
| <input type="checkbox"/> | test | Stop & Interim | 172.16.1.100 | 11/22/2012 14:01:06 | 11/22/2012 14:02:21 | 1m15s | 4.4 Kib | 4.3 Kib |
| <input type="checkbox"/> | test | Start & Stop | 172.16.1.100 | 11/22/2012 14:03:08 | 11/22/2012 14:04:07 | 58s | 2.0 Kib | 3.6 Kib |
| <input type="checkbox"/> | test | Start & Stop & Interim | 172.16.1.100 | 11/23/2012 17:01:23 | 11/23/2012 17:12:43 | 11m20s | 36.7 Kib | 16.5 Kib |

UserManager Settings

- Routers
- Users
- Sessions
- Customers
- Logs
- Payments
- Profiles
- Settings**
- Reports
- 0 A sessions
- 0 A users
- Advanced search
- Maintenance
- Logout

Appearance | Style | Templates | Language | Payment gateways | Signup

△ Table columns

| Table | Visible | Hidden |
|-------------|----------------|-----------|
| Routers | First name | Password |
| Users | Username | Disabled |
| Sessions | Actual profile | Owner |
| Customers | Upload Used | Last name |
| Logs | Download Used | Phone |
| Payments | | Location |
| Limitations | | Comment |

< << > >>

▽ First page

Users

Save

Settings - Logo

Appearance Style Templates Language

Main background: eaebe1

Disabled row foreground: 788180

Main foreground: 788180

Logo: /umfiles/logo.jpg

Logo text: Citranet User Manager

Window title: Citranet User Manager

Save Reset

- o Untuk mengubah Logo upload logo anda di directory "umfiles"

File List

Backup Restore

| File Name | Type |
|-------------------------------|----------------|
| BackupRB1000.backup | backup |
| BackupRB1000.rsc | script |
| MikroTik-28042012-1502.backup | backup |
| RB1000-160712.backup | backup |
| RB1000-160712.rsc | script |
| RB1000-160712.umb | userman backup |
| backup-akhir.backup | backup |
| backup-akhir.rsc | script |
| console-dump.txt | .txt file |
| um-before-migration.tar | .tar file |
| umfiles | directory |
| umfiles/logo.jpg | .jpg file |
| umfiles/logo.png | .png file |
| userman-160712.rsc | script |
| userman160512.umb | userman backup |

Settings – Template Voucher

| Appearance | Style | Templates | Language | Payment gateways | Signup |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|----------|------------------|--------|
| Name: | <input type="text" value="Vouchers"/> | | | | |
| Header: | <pre><!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <head> <title>Vouchers</title> <style> @media print { .nopr { display: none; } .pagebreak { page-break-after: always; }} </style> </head> <body></pre> | | | | |
| Row: | <pre><table align="center" style="color: black; font-size: 11px;"> <tr class="space1"><td colspan="3"></td> </tr> <tr> <td>Prepaid time:</td> <td>%u_timeLeft%</td> </tr> <!-- <tr> <td>Price: </td> <td>%u_totalPrice%</td> </tr> <tr> --> <td>Login:</td> <td>%u_username% </td> </tr> <tr class="space2"><td colspan="3"></td></tr> <tr> <td colspan="3"> After attempting to open a web page, you should enter this login information </td> </tr> <tr height="5px"><td colspan="3"></td></tr> <tr> <td>Login:</td> <td>%u_username% </td> <td style="padding-left: 20px">(login name that you enter at the HotSpot login page)</td> </tr> <tr> <td>Password:</td> <td>%u_password%</td> <td></pre> | | | | |
| Footer: | <pre></body></html></pre> | | | | |
| Break: | <pre><p class="nopr " style="font-size: 10px"> page break </p> <p class="pagebreak">&nbsp;</p></pre> | | | | |
| File extension: | <input type="text"/> | | | | |

UserManager Reports

Routers

Users

Sessions

Customers

Logs

Payments

Profiles

Settings

Reports

0 A sessions

0 A users

Advanced search

Maintenance

Logout

Title: test

- Price
- Traffic
- Sessions
-

Owner:

Period: (mm/dd/yyyy)

Type: HTML
 CSV

Download as file

Generate

Generated Report

test

| User | Profile | Price | From | Until | Session From | Session Until | Uptime | Download | Upload |
|----------------------|----------|---------------------|---------------------|---------------------|---------------------|---------------------|--------|-----------|-----------|
| | | | | | 11/26/2012 12:56:01 | 11/26/2012 13:09:55 | 13m53s | 118.7 Kib | 108.7 Kib |
| testing 2 jam - 50rb | 50000.00 | 11/26/2012 12:53:13 | 11/27/2012 12:53:13 | 11/26/2012 13:11:06 | 11/26/2012 13:11:27 | 20s | | | |
| | | | | | 11/26/2012 13:14:48 | 11/26/2012 13:16:48 | 2m | 22.9 Kib | 27.0 Kib |

test

| User | Profile | From | Until | Session From | Session Until | Uptime | Download | Upload |
|-------------------|-----------------|---------------------|-------|--------------|---------------|--------|----------|--------|
| 00:26:82:AF:1B:A1 | wireless-profil | 04/30/2012 15:27:37 | - | - | - | - | - | - |
| D0:DF:9A:01:2A:D2 | wireless-profil | 04/30/2012 15:33:58 | - | - | - | - | - | - |
| 68:A3:C4:D1:1F:F8 | wireless-profil | 04/30/2012 15:34:03 | - | - | - | - | - | - |
| 78:CA:39:AF:70:EC | wireless-profil | 04/30/2012 15:34:06 | - | - | - | - | - | - |
| 00:0C:42:1B:96:D5 | wireless-profil | 04/30/2012 15:34:09 | - | - | - | - | - | - |
| D8:9E:3F:09:A4:DD | wireless-profil | 04/30/2012 15:34:11 | - | - | - | - | - | - |

UserManager Maintenance

Routers

Users

Sessions

Customers

Logs

Payments

Profiles

Settings

Reports

0 A sessions

0 A users

Advanced search

Maintenance

Logout

Database

Database size: 89.0 Kib

In use: 100%

Last rebuild: Never

Last backup: 07/16/2012 10:04:44

Last restore: Never

Free disk space: 18.0 Mib

▲ Database backups

| | File name | Main DB | Log DB | Languages |
|--------------------------|-------------------------|---------|--------|-----------|
| <input type="checkbox"/> | RB1000-160712.umb | No | No | No |
| <input type="checkbox"/> | userman160512.umb | No | No | No |
| <input type="checkbox"/> | um-before-migration.tar | Yes | Yes | No |

Download

Load

Delete

▼ Upload backup

▲ Actual data base

Save

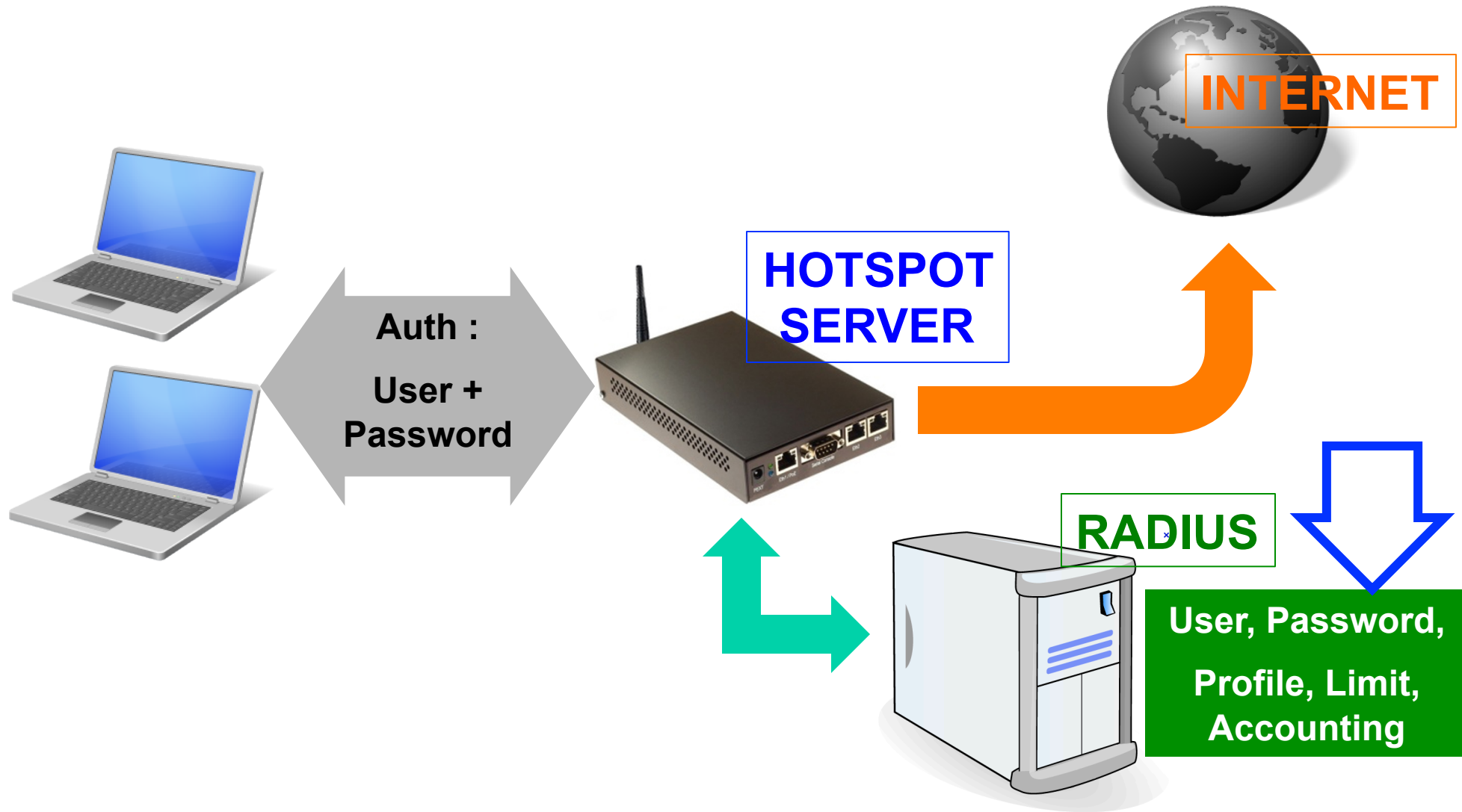
Rebuild



Quiz !

- Bagaimana mengatasi kondisi lupa username dan password untuk login di UserManager ?
- Sebuah Router mengaktifkan Service VPN dan juga Hotspot, Apakah bisa hanya menggunakan 1 UserManager sebagai Server Autentikasinya Untuk kedua service tersebut ?

[LAB-1] UserManager + Hotspot



● ● ● | [LAB-1] Example Config (1)

- Siapakan Radius Client dan UserManager untuk digunakan di Network Hotspot Anda yang sudah dibuat sebelumnya :
 - Konfigurasi Hotspot supaya menggunakan Radius.
 - Konfigurasi Radius Client aktifkan service Hotspot dan gunakan ip 127.0.0.1 untuk radius server.
 - Install UserManager ke dalam Router Anda.
 - Buat dan Gunakan Customer Baru yang memiliki hak akses Full.

Config Hotspot Using Radius

Hotspot Server Profile <hsprof1 >

General Login **RADIUS**

Use RADIUS

Default Domain:

Location ID:

Location Name:

MAC Format:

Accounting

Interim Update:

NAS Port Type:

Config Radius Client for Hotspot

New Radius Server

General Status

— Service —

ppp login

hotspot wireless

dhcp

Called ID:

Domain:

Address:

Secret:

Authentication Port:

Accounting Port:

Timeout: ms

New Customer

Customer details

▲ Main

Login: saya-sendiri

Password:

Disabled:

Parent: admin

Permissions: Full

Public ID:

Public host:

Backup allowed:

▼ Access

▼ Private information

▼ Signup options


▲ Format

Currency: Rp

Time zone: +07:00

Add

Login using New Customer



citranet
Citranet User Manager

Login

Password

New Router

Router details

▲ Main

Name:

Owner:

IP address:

Shared secret:

Time zone:

Disabled:

Log events:

- Authorization success
- Authorization failure
- Accounting success
- Accounting failure

▲ Radius incoming

CoA support: Use CoA

CoA port:

Limitation details

▼ Main

Name: 2 jam - 50rb

Owner: saya-sendiri

▲ Limits

Download: 0B

Upload: 0B

Transfer: 0B

Uptime: 2h

△ Rate limits

Rate limit: Rx 512k Tx 512k

Burst rate: Rx

Tx

Burst threshold: Rx

Tx

Burst time: Rx

Tx

Min rate: Rx

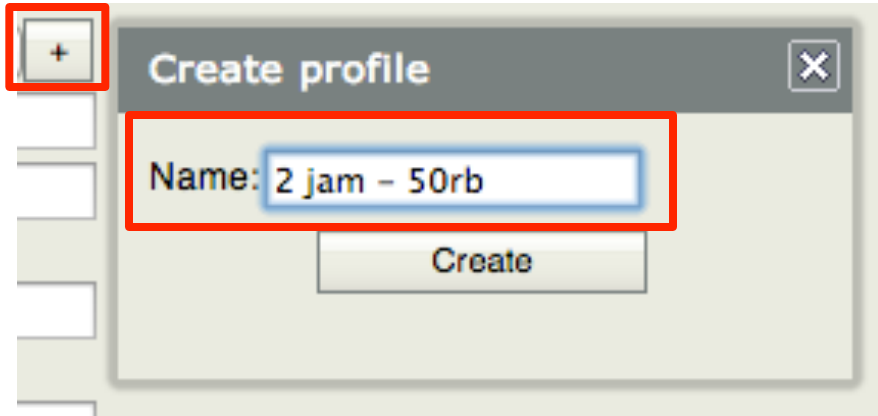
Tx

Priority: Not specified

▼ Constraints

Add

New Profile

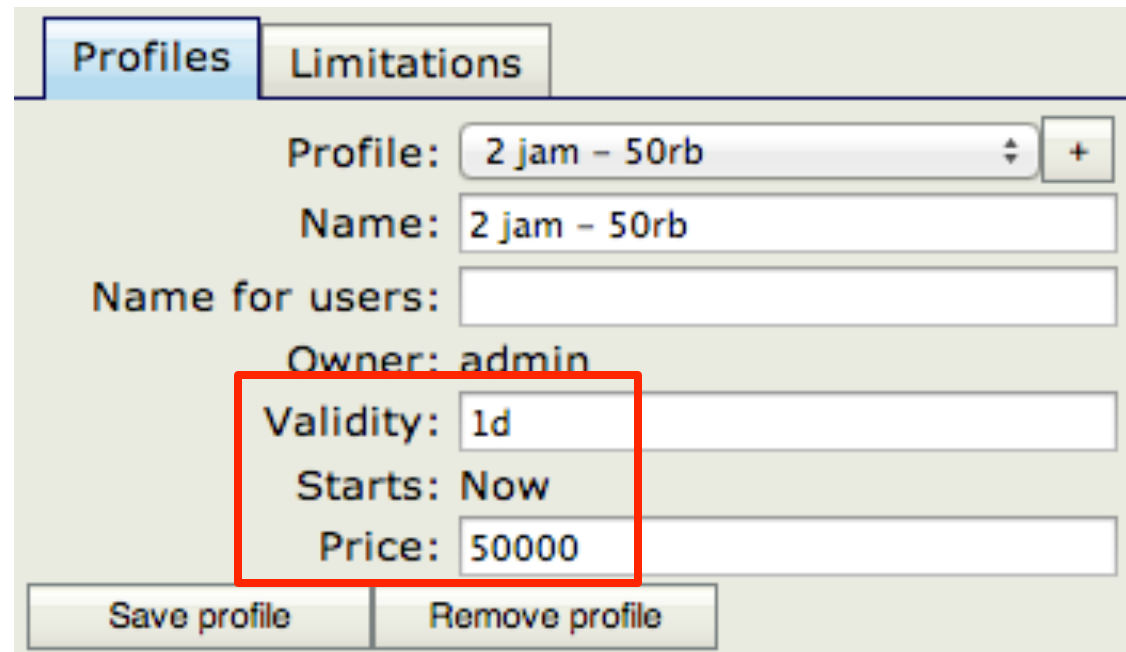


+

Create profile

Name: 2 jam - 50rb

Create



Profiles Limitations

Profile: 2 jam - 50rb

Name: 2 jam - 50rb

Name for users:

Owner: admin

Validity: 1d

Starts: Now

Price: 50000

Save profile Remove profile

Assign Limitation to Profile

Unlimited profile

Add new limitation

Profile part

▼ Period

- Days: Sunday
 Monday
 Tuesday
 Wednesday
 Thursday
 Friday
 Saturday

Time: 0:00:00 - 23:59:59

▲ Limits

- unlimited
 spv
 tso

2 jam - 50rb

Apply limit

Cancel

Add

Profile limitations

| <input checked="" type="checkbox"/> | Active | Constraints |
|-------------------------------------|--------|--------------------------------------------------------------------|
| <input checked="" type="checkbox"/> | Always | Uptime Limit: 2h Rate limits: 512K/512K 0/0 0/0 0/0 0 512K/512K |

Add new limitation Remove selected limitations

Add New User

User details

▼ Main

Username:

Password:

Disabled:

Owner:

▼ Constraints

▼ Wireless

▼ Private information

Assign profile:


Add

Check Hotspot Server

Hotspot

User Profiles Active Hosts IP Bindings Service Ports Walled Garden Walled Garden IP List



[-] [Filter]

| | Server | User | Domain | Address | Uptime | Idle Time |
|---|--------------------------------------------------------------------------------------------|---------|--------|-----------|----------|-----------|
| R |  hotspot2 | testing | | 10.5.50.3 | 00:07:13 | 00:00:02 |

Queue List

Simple Queues Interface Queues Queue Tree Queue Types

[+] [-] [Check] [X] [Info] [Filter] [00] Reset Counters [00] Reset All Co

| # | | Name | Target Ad... | Rx Max Limit | Tx Max Limit |
|---|---|-------------------------------------------------------------------------------------------------------|--------------|--------------|--------------|
| 1 | D |  hs- <hotspot2> | | unlimited | unlimited |
| 0 | D |  <hotspot-testing> | 10.5.50.3 | 524288 | 524288 |



Quiz !

- Ketika menggunakan UserManager, user yang ada di Local Router Hotspot apakah bisa digunakan ?
- Jika User Local di Router Hotspot bisa digunakan, Mana yang akan digunakan jika kebetulan username nya sama ?
- Ketika menggunakan UserManager, User Profile yang ada di Local Router Hotspot apakah bisa digunakan ?

UserManager Disconnecting Client

The screenshot shows the Mikrotik User Manager interface. On the left is a sidebar menu with items: Routers, Edit, Remove, Close, Logs, Payments, Profiles, Settings, Reports, 0 A sessions, 0 A users, Advanced search, Maintenance, and Logout. The 'Close' menu item is highlighted with a red box. The main area displays a table with columns: Username, Status, User IP, From time, and Till time. One row is selected with a checkmark in the first column, showing 'testing' as the username, 'Start' as the status, '10.5.50.3' as the user IP, and '11/26/2012 12:56:01' for both from and till times. A confirmation dialog box is overlaid on the right, asking 'Do you really want to PERMANENTLY close selected sessions?' with 'Cancel' and 'OK' buttons.

| | Username | Status | User IP | From time | Till time |
|-------------------------------------|----------|--------|-----------|---------------------|---------------------|
| <input checked="" type="checkbox"/> | testing | Start | 10.5.50.3 | 11/26/2012 12:56:01 | 11/26/2012 12:56:01 |