Base-Level Command for Mikrotik

/certificate	**/ppp**
/driver	**/queue**
/file	**/radius**
/interface	**/routing**
/ip	**/snmp**
/ipv6	**/special-login**
/lcd	**/store**
/log	**/system**
/metarouter	**/terminal**
/mpls	**/tool**
/partitions	**/user**
/port	**/wireless**

Sub-Level Command for Mikrotik

/ip	**/system**	ssh	ppp-server	mac-scan
accounting	backup	sup-out	pppoe-client	mac-server
address	check-disk	telnet	pppoe-server	mac-telnet
arp	check-installation	upgrade	pptp-client	netwatch
dhcp-client	clock	watchdog	pptp-server	ping-speed
dhcp-relay	console	**/interface**	sstp-client	profile
dhcp-server	default	bonding	sstp-server	sms
dns	health	bridge	traffic-eng	sniffer
firewall	history	eoip	virtual-ethernet	torch
hotspot	identity	ethernet	vlan	traceroute
ipsec	leds	gre	**/routing**	traffic-generator
neighbor	license	ipip	bfd	traffic-monitor
packing	logging	l2tp-client	bgp	wol
pool	note	l2tp-server	mme	bandwidth-server
proxy	ntp	lte	ospf	bandwidth-test
route	package	mesh	rip	**/log**
service	reboot	monitor-traffic	**/tool**	debug
settings	reset-configuration	ovpn-client	bandwidth-server	error
smb	resource	ovpn-server	bandwidth-test	info
socks	routerboard	ppp-client	dns-update	warning
ssh	scheduler	ppp-server	e-mail	
tftp	script	pppoe-client	fetch	
traffic-flow	serial-terminal	pppoe-server	graphing	
upnp	shutdown	pptp-client	ip-scan	

Starting Command for mikrotik

?	**?**	Give List of All Command
ip ?	**ip ?**	Give help tips for **ip** level command
tab	**int+press tab**	**Interface [autofill]**
/	**/**	Move up to base level
..	**..**	Move up to one level
/ip	**/ip**	Move up to **ip** level command

Example

/ip ?
ip route print
inter ether print

Connecting to the console

RS232/Serial
Telnet
SSH
MAC-Telnet
Winbox
Webfig
RJ45 Rollover

General Syntax of Command

add	move
edit/set	remove
find	export
print	import
get	enable
comment	disable

Start of using mikrotik command…….

Logging into the MikroTik Router

MikroTikv2.8
Login: admin
Password:

/password
[admin@MikroTik]>password
oldpassword:
newpassword:**********
retypenewpassword:**********
[admin@MikroTik]>

[admin@MikroTik]>	Base menu level
[admin@MikroTik]interface>	Interface management
[admin@MikroTik]ip address>	IP address management

[admin@MikroTik]> ?	Show all base level
Certificate	Certificate management
Driver	Driver management
File	Local router file storage.
Import	Run exported configuration script
Interface	Interface configuration
log	System logs
password	Change password
ping	Send ICMP Echo packets
port	Serial ports
quit	Quit console
radius	Radius client settings
redo	Redo previously undone action
setup	Do basic setup of system
snmp	SNMP settings
special-login	Special login users
undo	Undo previous action
user	User management
ip	IP options
queue	Bandwidth management
system	System information and utilities
tool	Diagnostics tools
export	Print or save an export script that can be used to restore configuration

[admin@MikroTik]> /ip?	Show all IP level command
Accounting	Traffic accounting
Address	Address management
Arp	ARP entries management
Dns	DNS settings
Firewall	Firewall management
Neighbor	Neighbors
Packing	Packet packing settings
Pool	IP address pools
Route	Route management
Service	IP services
policy-routing	Policy routing
upnp	Universal Plug and Play
vrrp	Virtual Router Redundancy Protocol
socks	SOCKS version4 proxy
hotspot	HotSpot management
ipsec	IP security
web-proxy	HTTP proxy
export	Print or save an export script that can be used to restore configuration

[admin@MikroTik]ip>/	to go to Base level menu
admin@MikroTik]>/driver	to go to Driver level menu
admin@MikroTik]>/ip	to go to IP level menu
admin@MikroTik]>/interface	to go to Interface level menu

[admin@MikroTik]iproute> print	Prints the routing table
[admin@MikroTik]iproute>..address print	Prints the IP address table
[admin@MikroTik]iproute>/ip address print	Prints the IP address table

IP address configuration, instead of using the 'address 'and 'netmask' arguments

/ip address add address 10.0.0.1/24 interface ether1
/ip address add address 10.0.0.1 netmask 255.255.255.0 interface ether1

Before configuring the IP addresses and routes please check the /interface menu to see the list of Available interfaces.

[admin@MikroTik]interface>print						
Flags: X-disabled, D-dynamic, R-running						
#		NAME	TYPE	RX-RATE	TX-RATE	MTU
0	R	ether1	ether	0	0	1500
1	R	ether2	ethe	r0	0	1500
2	X	wavelan1	wavelan	0	0	1500
3	X	prism1	wlan	0	0	1500

The interfaces need to be enabled

[admin@MikroTik]interface>enable0
[admin@MikroTik]interface>enable ether1
[admin@MikroTik]interface>enable ether2
[admin@MikroTik]interface>set 0 name=Local; set 1 name=Public

The device drivers for NE2000 compatible ISA cards need to be loaded using the add command under the**/drivers** menu

[admin@MikroTik]>/driver
[admin@MikroTik]driver>add name=ne2k-isa io=0x280
[admin@MikroTik]>setup

Setup uses Safe Mode. It means that all changes that are made during setup are reverted in case of error, or if Ctrl-C is used to abort setup. To keep changes exit setup using the 'x ' key. [SafeModetaken] Choose options by pressing one of the letters in the left column, before dash. Pressing 'x' will exit current menu, pressing Enter key will select the entry that is marked by an'*'.You can abort setup at any time by pressing Ctrl-C.
Entries marked by '+' are already configured.
Entries marked by'-' cannot be used yet.
Entries marked by 'X' cannot be used without installing additional packages.

r	reset all router configuration
+l	load interface driver
*a	configure ip address and gateway
d	setup dhcp client
s	setup dhcp server
p	setup pppoe client
t	setup pptp client
x	exit menu

Your choice [press Enter to configure ip address and gateway]: a
Your choice:a
Enable interface:
ether1 ether2 wlan1
enable interface:ether1
ip address/netmask : 10.1.0.66/24
#Enabling interface

/interface enable ether1
#Adding IP address
/ip address add address=10.1.0.66/24 interface=ether1 comment="added by setup"
+a- add ip address
*g- setup default gateway
x- exit menu
your choice:x

Add ip to interface:

[admin@MikroTik]ip address>add address 10.0.0.217/24 interface Public
[admin@MikroTik]ip address>add address 192.168.0.254/24 interface Local

Viewing Routes:

[admin@MikroTik]>/ip
[admin@MikroTik]ip>/route
[admin@MikroTik]ip route>print detail

Adding Default Routes

[admin@MikroTik]ip route>add gateway=10.0.0.1
[admin@MikroTik]ip route>print detail
[admin@MikroTik]ip route>add gateway=10.0.0.1
[admin@MikroTik]ip route>print detail

Testing the Network Connectivity

[admin@MikroTik]ip route>/ping10.0.0.4
[admin@MikroTik]ip route>/ping192.168.0.1

To access anything beyond the router(network10.0.0.0/24 and the Internet)use Add a static route and Have To use masquerading, a source NAT rule with action 'masquerade'should be added to the firewall configuration:

[admin@MikroTik]ip firewall src-nat>add action=masquerade out-interface=Public
[admin@MikroTik]ip firewall src-nat>print detail
[admin@MikroTik]ip firewall src-nat>

Bandwidth limitation is done by applying queues for outgoing interfaces

[admin@MikroTik]queue simple>add max-limit=64000/128000 interface=Local
[admin@MikroTik]queue simple>print detail
[admin@MikroTik]queue simple>

We want to make **address:port 192.168.0.4:80** accessible from the Internet at **address:port 10.0.0.217:80**

[admin@MikroTik]ip firewall dst-nat>add action=nat protocol=tcp\dst-address=10.0.0.217/32:80 to-dst-address=192.168.0.4
[admin@MikroTik]ip firewall dst-nat>print detail
[admin@MikroTik]ip firewall dst-nat>

/system backup

To save the router configuration to file test:
[admin@MikroTik]system backup>save name=test
Configuration back up saved
[admin@MikroTik]system backup>

To see the files stored on the router:
[admin@MikroTik]>file print

#	NAME	TYPE	SIZE	CREATION-TIME
0	test.backup	backup	12567	aug/12/200221:07:50

[admin@MikroTik]>

To load the saved backup file test:
[admin@MikroTik]system backup>load name=test
Restore and reboot ?[y/N]: y

/export
[admin@MikroTik]>ip address print
Flags: X-disabled, I-invalid, D-dynamic

#	ADDRESS	NETWORK	BROADCAST	INTERFACE
0	10.1.0.172/24	10.1.0.0	10.1.0.255	bridge1
1	10.5.1.1/24	10.5.1.0	10.5.1.255	ether1

[admin@MikroTik]>
To make an export file from only one item:
[admin@MikroTik]ipaddress>export file=address1 from=1
[admin@MikroTik]ipaddress>export file=address2 from=0

To see the files stored on the router:
[admin@MikroTik]>file print
To export the setting on the display use the same command without the file argument:
[admin@MikroTik]ip address>export from=0,1

/import
[admin@MikroTik]>import address1.rsc
/system
[admin@MikroTik]>system reset
Dangerous!Reset anyway?[y/N]:n
Action cancelled
[admin@MikroTik]>
/file
To see the files stored on the router:
[admin@MikroTik]>file print

/tool, /tool mac-server
To enable MAC telnet server on ether1 interface only:
[admin@MikroTik]tool mac-server>print
Flags: X-disabled

#	INTERFACE
0	all

[admin@MikroTik]tool mac-server>remove 0
[admin@MikroTik]tool mac-server>add interface=ether1 disabled=no
[admin@MikroTik]tool mac-server>print

Flags:X-disabled
INTERFACE
0 ether1
[admin@MikroTik]tool mac-server>

/tool mac-telnet
[admin@MikroTik]tool>mac-telnet "00:40:63:C1:23:C4"
Login:admin
Password:
/system serial-console
The Serial Console and Terminal are tools,used to communicate with devices and other systems that are interconnected via serial port
To enable Serial Console:
[admin@MikroTik]system serial-console>set enabled=yes
[admin@MikroTik]system serial-console>print
[admin@MikroTik]system serial-console>/port print detail
0 name=serial0 used-by=Serial-Console baud-rate=9600 data-bits=8 parity=none stop-bits=1 flow-control=none
1 name=serial1 used-by= Serial-Console baud-rate=9600 data-bits=8 parity=none stop-bits=1 flow-control=none
/system serial-terminal
The command is used to communicate with devices and other systems that are connected to router via serial port.
[admin@MikroTik]system>serial-terminal serial1
/ system package
[admin@MikroTik]system package>print
[admin@MikroTik]system package>downgrade
[admin@MikroTik]system package>upgrade
/system upgrade
[admin@MikroTik]system upgrade>
[admin@MikroTik]system upgrade>print
To upgrade chosen packages:
[admin@MikroTik]system upgrade>download 0,1,2,5,6,7,8,9,10,13,14
[admin@MikroTik]system upgrade>print
/system upgrade upgrade-package-source
To add a router,with user name admin and no password,from which the packages will be retrieved:
[admin@MikroTik]systemupgradeupgrade-package-source>print
ADDRESS USER
0 192.168.25.8 admin
[admin@MikroTik]system upgrade upgrade-package-source>
/ip service
[admin@MikroTik]ip service>set ssh port=65
[admin@MikroTik]ip service>print
/system ssh
[admin@MikroTik]ipservice>/system ssh
address:
[admin@MikroTik]ip service>/
[admin@MikroTik]>system ssh 10.1.0.1 user=admin port=22
Telnet Server
[admin@MikroTik]ip service>print detail
MikroTik Router OS telnet client is used to connect to other hosts in the network via Telnet
protocol.
[admin@MikroTik]>system telnet 10.1.0.1
[admin@MikroTik]>/ip route print
[admin@MikroTik]ip route>/ping10.0.0.1
[admin@MikroTik]>interface print

[admin@MikroTik]>interface x[TAB]_
[admin@MikroTik]>interface export_
[admin@MikroTik]>interface mt[TAB]_
[admin@MikroTik]>interface monitor-traffic_
[admin@MikroTik]interface>set 0 mtu=1200

[admin@MikroTik]>pi 10.1 c 3 s 100
Equals to:
[admin@MikroTik]>ping 10.0.0.1 count 3 size 100
There are some commands that are common to nearly all menu levels, namely:
print,set,remove,add,find,get,export,enable,disable,comment,move.These commands have similar behavior throughout different menu levels.
[admin@MikroTik]ip firewall rule input>[Ctrl]+[X]
[Safe Mode taken]
[admin@MikroTik]ip firewall rule input<SAFE>add
[admin@MikroTik]ip firewall rule input<SAFE>/system history print
[admin@MikroTik]ip address>add address=10.10.10.1/24 interface=ether2
[admin@MikroTik]ip address>print
/ip arp
If static arp entries
[admin@MikroTik]ip arp>add address=10.10.10.10 interface=ether2 mac-address=06\..\...:21:00:56:00:12
[admin@MikroTik]iparp>/interface ethernet set ether2 arp=reply-only

Before OSPF---Page-100
/routing ospf
[admin@MikroTik]routing ospf>set redistribute-connected=as-type-1\
\...metric-connected=1
[admin@MikroTik]routing ospf>print
/routing ospf area
[admin@WiFi]routing ospf area>add area-id=0.0.10.5 name=local_10
[admin@WiFi]routing ospf area>print
/routing ospf network
[admin@MikroTik]routing ospf network>add area=backbone network=10.10.1.0/24
[admin@MikroTik]routing ospf network>print
/routing ospf interface
[admin@MikroTik]routing ospf interface>add interface=ether2 hello-interval=5s
[admin@MikroTik]routing ospf interface>print
/routing ospf virtual-link
[admin@MikroTik]routing ospf virtual-link>add neighbor-id=10.0.0.201\
\...transit-area=ex
[admin@MikroTik]routing ospf virtual-link>print
/routing ospf neighbor
admin@MikroTik]routing ospf neighbor >print
Now let's setup the OSPF_MAIN router.
[admin@OSPF_MAIN]>
[admin@OSPF_MAIN]interface>print
[admin@OSPF_MAIN]ip address>print
configure OSPF_peer_1 router
[admin@OSPF_peer_1]interface>print
[admin@OSPF_peer_1]routing ospf>print
[admin@OSPF_peer_1]ip address>print

Set up the OSPF_peer_2 router
[admin@OSPF_peer_2]interface>print
[admin@OSPF_peer_2]ip address>print
[admin@OSPF_peer_2]routing ospf area>print
[admin@OSPF_peer_2]routing ospf network>print
Now let's setup the OSPF_MAIN router.
[admin@OSPF_MAIN]ip route>print
configure OSPF_peer_1 router
[admin@OSPF_peer_1]ip route>print
configure OSPF_peer_2 router
[admin@OSPF_peer_2]ip route>print
We should change cost value in both routers: OSPF_peer_1 and OSPF_peer_2 to50
[admin@OSPF_peer_1]routing ospf interface>add interface=backup cost=50
[admin@OSPF_peer_1]routing ospf interface>print
[admin@OSPF_peer_2]routing ospf interface>add interface=to_peer_1 cost=50
[admin@OSPF_peer_2]routing ospf interface>print

[admin@OSPF_MAIN]ip route>print
[admin@OSPF_peer_2]>ip route print
/routing rip
To enable RIP protocol to redistribute the routes to the connected networks:
[admin@MikroTik]routing rip>set redistribute-connected=yes
[admin@MikroTik]routing rip>print
To add an entry RIP
[admin@MikroTik]routing rip>interface add interface=ether1\
\...prefix-list-out=plout
[admin@MikroTik]routingrip>interface print
/routing rip network
[admin@MikroTik]routing rip network>add address=10.10.1.0/24
To force RIP protocol to exchange routing information with the 10.0.0.1 router:
[admin@MikroTik]routing rip>neighbor add address=10.0.0.1
[admin@MikroTik]routing rip>neighbor print
/routing rip route
[admin@MikroTik]routing rip route>print
[admin@MikroTik]routing rip>set redistribute-connected=yes
[admin@MikroTik]routing rip>print
admin@MikroTik]routing rip route>print
/routing rip network
[admin@MikroTik]routing rip network>print
[MikroTik]routing rip>/ip route print
/ip route
[admin@MikroTik]ip route>add dst-address=192.168.0.0/16 gateway=10.10.10.2
[admin@MikroTik]ip route>add gateway 10.10.10.1
[admin@MikroTik]ip route>add dst-address=192.168.0.0/16 gateway=10.10.10.2
[admin@MikroTik]ip route>add gateway 10.10.10.1
[admin@MikroTik]iproute>set 0 gateway=10.10.10.2,10.10.10.254
/ip policy-routing
[admin@MikroTik]ip policy-routing>table main
[admin@MikroTik]ip policy-routing table main>print
To add a new table named mt:
[admin@MikroTik]ip policy-routing>add name=mt

To add the route to the 10.5.5.0/24 network via 10.0.0.22 gateway to the mt table:
[admin@MikroTik]ip policy-routing>table mt
[admin@MikroTik]ip policy-routing table mt>add dst-address=10.5.5.0/24\ \...gateway=10.0.0.22
[admin@MikroTik]ip policy-routing table mt>print
/ip policy-routing rule
To add the rule
[admin@MikroTik]ip policy-routing rule>add src-address=10.0.0.144/32\ \...table=mt action=lookup
[admin@MikroTik]ip policy-routing rule>print
[admin@MikroTik]ip policy-routing>add name=from_net1;add name=from_net2;add name=rest
Create the default route in each of the tables:
[admin@MikroTik]ippolicy-routing>table from_net1add gateway=10.0.0.1
[admin@MikroTik]ippolicy-routing>table from_net2 add gateway=10.0.0.2
[admin@MikroTik]ippolicy-routing>table rest add gateway=10.0.0.254
[admin@MikroTik]ippolicy-routing>table from_net1 print
Create rules that will direct traffic from sources to given tables,and arrange them in the Desire dorder:
[admin@MikroTik]ip policy-routing>rule
[admin@MikroTik]ip policy-routing rule>print
/routing bgp
[admin@MikroTik]routing bgp>
[admin@MikroTik]routing bgp>print
/routing bgp network
[admin@modux]routing bgp network>add network=159.148.150.192/27
[admin@modux]routing bgp network>print
/routing bgp peer
To enable routing information exchange with the neighbour(non-multihop) 192.168.0.254 that Belongs to 65002 AS:
[admin@MikroTik]routing bgp peer>add remote-address=192.168.0.254 remote-as=65002
[admin@MikroTik]routing bgp peer>print
/routing bgp peer print detail
To add the driver for Arlan 655 adapter
[admin@MikroTik]>driver add name=arlan io=0xD000
[admin@MikroTik]>driver print
/interface arlan
[admin@MikroTik]interface arlan>print
[admin@MikroTik]interface arlan>monitor 0
[admin@MikroTik]interface arlan>set 0 sid=0x03816788 tma-mode=yes
[admin@MikroTik]interface arlan>monitor 0
To put interface ether1 and ether2 in a bridge
/interface bridge add name="MyBridge" disabled=no
/interface bridge port set ether1,ether2 bridge=MyBridge
To add and enable a bridge interface that will forward all the protocols:
[admin@MikroTik]interface bridge>add;print.
/interface bridge port
[admin@MikroTik]interface bridge port>set ether1,ether2 bridge=bridge1
[admin@MikroTik]interface bridge port>print
/interface bridge monitor
[admin@MikroTik]interface bridge>monitor bridge1
/interface bridge port monitor
[admin@MikroTik]interface bridge port>mo 0
/interface bridge host
To get the active host table:
[admin@MikroTik]interface bridge host>print

/interface bridge firewall
[admin@MikroTik]interface bridge firewall>add mac-dst-address=FF:FF:FF:FF:FF:FF action=drop
[admin@MikroTik]interface bridge firewall>print
To make bridge,drop IP, ARP and RARP packets:
[admin@MikroTik]interface bridge firewall>add mac-protocol=2048 action=drop
[admin@MikroTik]interface bridge firewall>add mac-protocol=2054 action=drop
[admin@MikroTik]interface bridge firewall>add mac-protocol=32821 action=drop
[admin@MikroTik]interface bridge firewall>print
[admin@MikroTik]interface bridge>add forward-protocols=ip,arp,other
[admin@MikroTik]interface bridge>print
If you want to access the router through unnumbered bridged interfaces,it is required to add an IP address to the bridge interface:
[admin@MikroTik]ipaddress>add address=192.168.0.254/24 interface=bridge1
[admin@MikroTik]ipaddress>add address=10.1.1.12/24 interface=prism1
[admin@MikroTik]ipaddress>print
/interface pc
[admin@MikroTik]>interface print
[admin@MikroTik]interface>set 1 name aironet
[admin@MikroTik]interface>enable aironet
[admin@MikroTik]>interface print
[admin@MikroTik]>interface pc
[admin@MikroTik]interface pc>print
[admin@MikroTik]interface pc>monitor 0
[admin@MikroTik]interface pc>set 0 ssid1 mt
[admin@MikroTik]interface pc>monitor 0
[admin@MikroTik]ip address>add address 10.1.1.12/24 interface aironet
[admin@MikroTik]ip address>print
[admin@MikroTik]ip route>add gateway=10.1.1.254
[admin@MikroTik]ip route>print
Point-to-PointWireless LAN
[admin@MikroTik]interface pc>set 0 mode=ad-hoc ssid1=mt frequency=2442MHz\\...bitrate=auto
[admin@MikroTik]interface pc>
[admin@MikroTik]interface pc>monitor 0

[admin@wnet_gw]ip address>add address 192.168.11.2/30 interface aironet
[admin@wnet_gw]interface pc>/tool bandwidth-test 192.168.11.1 protocol tcp
[admin@wnet_gw]interface pc>/tool bandwidth-test 192.168.11.1 protocol udp size 1500

Cyclades PC300 PC Adapters
/interface Cyclades
[admin@MikroTik]ip address>add address=1.1.1.1/32 interface=cyclades1
[admin@MikroTik]ip address>print
[admin@MikroTik]ip address>/tool flood-ping 1.1.1.2 size=1500 count=50
[admin@MikroTik]ip route>add gateway 1.1.1.2 interface cyclades1
[admin@MikroTik]ip route>print
To view the list of available drivers,do the following:
[admin@MikroTik]driver>add name?
To see system resources occupied by the devices
[admin@MikroTik]system resource>io print
[admin@MikroTik]system resource>irq print
To add the driver
[admin@MikroTik]driver>add name=ne2k-isa io=0x280

[admin@MikroTik]interface ethernet>monitor ether1, ether2
[admin@MikroTik]>interface print
[admin@MikroTik]interface>enable farsync2
[admin@MikroTik]ip address>add address 1.1.1.1/32 interface farsync1\ \...network 1.1.1.2 broadcast 255.255.255.255
[admin@MikroTik]ip address>add address 1.1.1.2/32 interface fsync\ \...network 1.1.1.1 broadcast 255.255.255.255

MikroTik router to Cisco router using X.21 line

[admin@MikroTik]interfacefarsync>set farsync1 line-protocol=cisco-hdlc\ \...media-type=X21 clock-source=internal
[admin@MikroTik]interface farsync>/ip address add address=1.1.1.1/24\ \...interface=farsync1

MikroTik router to MikroTik router using Frame Relay

admin@office]interface pvc>add dlci=42 interface=farsync1
[admin@MikroTik]ip address>add interface=pvc1 address=1.1.1.1 netmask=255.255.255.0
[admin@MikroTik]interface cyclades>print
[admin@MikroTik]interface pvc>print

Cisco router setup

CISCO# show running-config
[admin@MikroTik]ip address>add interface=pvc1 address=1.1.1.1 netmask=255.255.255.0
[admin@MikroTik]interface moxa-c502>print
[admin@MikroTik]interface pvc>print
[admin@r1]interface moxa-c101>set 0 frame-relay-dce=yes
[admin@r1]interface pvc>add dlci=42 interface=moxa-c101-1
[admin@r2]interface pvc>add dlci=42 interface=moxa-c101-1
[admin@MikroTik]interface>monitor-traffic ether1,wlan1
admin@MikroTik]port>print

Enter the pin code from serial-terminal(in this case,PIN code is 3663):

/system serial-terminal serial1
AT+CPIN=”3663”
[admin@MikroTik]interface ppp-client>enable 0
[admin@MikroTik]interface ppp-client>mo 0

Change remote-address in --- /ppp profile,

/ppp profile set default remote-address=212.93.96.65

Add a ppp client:

/interface ppp-client add dial-command=ATD phone=*99***1#\\...modem-init="AT+CGDCONT=1,\"IP\",\"internet\"" port=serial1

/isdn-channels

[admin@MikroTik]isdn-channels>print

/interface isdn-client

[admin@MikroTik]interface isdn-client>add msn="142" user="test"\ \...password="test" phone="144" bundle-128K=no
[admin@MikroTik]interface ppp-client>enable 0
[admin@MikroTik]interface ppp-client>mo 0

ISDN client interfaces can be added using the add command:

[admin@MikroTik]interface isdn-client>add msn="142" user="test"\\...password="test" phone="144" bundle-128K=no
[admin@MikroTik]interface isdn-client>print

/interface isdn-client

/Interface isdn-server

[admin@MikroTik]interface isdn-server>add msn="142" bundle-128K=no
[admin@MikroTik]interface isdn-server>print
[admin@MikroTik]>/driver add name=w6692
[admin@MikroTik]isdn-channels>print
[admin@MikroTik]>/driver add name=w6692
[admin@MikroTik]isdn-channels>print
[admin@mikrotik]>/interface isdn-client add name="isdn-isp" phone="12345678" user="john" password="31337!)"add-default-route=yes dial-on-demand=yes
[admin@MikroTik]>/interface isdn-client print

[admin@MikroTik]ppp profile>print
[admin@Mikrotik]ppp profile>set default idle-timeout=30s
[admin@MikroTik]/interface set isdn-isp disabled=no
[admin@MikroTik]/interface isdn-client monitor isdn-isp
[admin@MikroTik]/driver add name=hfc
[admin@MikroTik]isdn-channels>print
[admin@MikroTik]interface isdn-server>add msn="7542159"\\...authentication=chap,pap bundle-128K=no
[admin@MikroTik]interface isdn-server>print
[admin@MikroTik]interface isdn-server>print
[admin@MikroTik]ppp profile>print
[admin@Mikrotik]pppprofile>set default idle-timeout=5s local-address=10.99.8.1\\...remote-address=10.9.88.1
[admin@MikroTik]ppp secret>add name=john password="31337!)" service=isdn
[admin@MikroTik]ppp secret>print
[admin@ISDN]ppp secret>print

Check the status of the ISDN server interface and wait for the call:

[admin@MikroTik]interface isdn-server>monitor isdn-in1

At first,you need to setup ISDN connection.To use ISDN,the ISDN card driver must be loaded:

[admin@MikroTik]driver>add name=hfc

The PPP connection must have a new user added to the routers one and two:

[admin@Mikrotik]ppp secret>add name=backup password=backup service=isdn

An ISDN server and PPP profile must be setup on the second router:

[admin@MikroTik]ppp profile>set default local-address=3.3.3.254 remote-address=3.3.3.1
[admin@MikroTik]interface isdn-server>add name=backup msn=7801032

An ISDN client must be added to the first router:

[admin@MikroTik]interface isdn-client>
Add name=backup user="backup" password="backup" phone=7801032 msn=7542159

The first router:

[admin@Mikrotik]ip route>add gateway 2.2.2.2 comment"route1"

The second router:

[admin@Mikrotik]ip route>add gateway 2.2.2.1 comment"route1" dst-address 1.1.1.0/24

And finally,you have to add script……. **/system script**

The first router:

[admin@Mikrotik]systemscript>addname=connection_down\\...source={/interfaceenablebackup;/iproutesetroute1gateway3.3.3.254}
[admin@Mikrotik]systemscript>addname=connection_up\\...source={/interfacedisablebackup;/iproutesetroute1gateway2.2.2.2}

The second router:

[admin@Mikrotik]systemscript>addname=connection_down\\...source={/iproutesetroute1gateway3.3.3.1}
[admin@Mikrotik]systemscript>addname=connection_up\\...source={/iproutesetroute1gateway2.2.2.1}

Add the following settings to the first and second router:

[admin@Mikrotik]toolnetwatch>addhost=2.2.2.1interval=5s\\...up-script=connection_updown-script=connection_down
[admin@Mikrotik]toolnetwatch>addhost=2.2.2.2interval=5s\\...up-script=connection_updown-script=connection_down

M3P

[admin@MikroTik]ip packing>add interface=ether1 packing=compress-all\\...unpacking=compress-all
[admin@MikroTik]ip packing>print

/interface moxa-c101

[admin@MikroTik]interface moxa-c101>set 0 line-protocol=cisco-hdlc
[admin@MikroTik]interface moxa-c101>print
[admin@MikroTik]interface moxa-c101>monitor 0
admin@MikroTik]ip address>add address 1.1.1.1/32 interface wan\ \...network 1.1.1.2 broadcast 255.255.255.255
[admin@MikroTik]iproute>add gateway1.1.1.2
[admin@MikroTik]ip route>print

[admin@MikroTik]ip address>add address 1.1.1.2/32 interface moxa\\...network 1.1.1.1 broadcast 255.255.255.255
[admin@MikroTik]ip address>print
MikroTik Router to Cisco Router
[admin@MikroTik]ip address>add address 1.1.1.1/32 interface wan\ \...network 1.1.1.2 broadcast 255.255.255.255
[admin@MikroTik]ip route>add gateway1.1.1.2
[admin@MikroTik]ip route>print

CISCO#showrunning-config
CISCO#ping1.1.1.1

/interface moxa-c502
[admin@MikroTik]interface moxa-c502>set 0,1 line-protocol=cisco-hdlc
[admin@MikroTik]interface moxa-c502>print
[admin@MikroTik]interface moxa-c502>monitor 0
[admin@MikroTik]ip address>add address 1.1.1.1/32 interface wan\\...network 1.1.1.2 broadcast 255.255.255.255
[admin@MikroTik]ip route>add gateway 1.1.1.2 interface wan
[admin@MikroTik]ip route>print
[admin@MikroTik]ip address>add address 1.1.1.2/32 interface moxa\\...network 1.1.1.1 broadcast 255.255.255.255
MikroTik Router to Cisco Router
[admin@MikroTik]ip address>add address 1.1.1.1/32 interface wan\\...network 1.1.1.2 broadcast 255.255.255.255
[admin@MikroTik]ip address>print
[admin@MikroTik]ip route>add gateway 1.1.1.2
[admin@MikroTik]ip route>print
CISCO#show running-config
CISCO#ping1.1.1.1

PPP and Asynchronous Interfaces Page 200

/interface ppp-client, /interface ppp-server
[admin@MikroTik]>/port print
[admin@MikroTik]>set 9 baud-rate=38400
You can add a PPP server using the add command:
[admin@MikroTik]interface ppp-server>add name=test port=serial1
[admin@MikroTik]interface ppp-server>print
You can add a PPP client using the add command:
[admin@MikroTik]interface ppp-client>add name=test user=testport=serial1\\...add-default-route=yes
[admin@MikroTik]interface ppp-client>print
For a typical server setup we need to add one user to the R1 and configure the PPP server.
[admin@MikroTik]ppp secret>add name=test password=test local-address=3.3.3.1\\...remote-address=3.3.3.2
[admin@MikroTik]ppp secret>print
[admin@MikroTik]ppp secret>/int ppp-server
[admin@MikroTik]interface ppp-server>add port=serial1 disabled=no
[admin@MikroTik]interface ppp-server>print
[admin@MikroTik]interface ppp-server>
Now we need to setup the client to connect to the server:
[admin@MikroTik]interface ppp-client>add port=serial1 user=test password=test\\...phone=132
[admin@MikroTik]interface ppp-client>print
[admin@MikroTik]interface ppp-client>enable 0
/interface radiolan
[admin@MikroTik]interface radiolan>monitor radiolan1
[admin@MikroTik]interface radiolan>set 0 sid ba72 distance 4.7km-6.6km
[admin@MikroTik]interface radiolan>print
Now we'll monitor other cards with the same sid within range:
[admin@MikroTik]interface radiolan>neighbor radiolan1 print

[admin@MikroTik]interface radiolan>ping 00:a0:d4:20:3b:7f radiolan1\\...size=1500 count=50
[admin@MikroTik]ip address>add address=10.1.0.1/30 interface=radiolan1
[admin@MikroTik]ip route>add gateway=10.1.1.254
[admin@MikroTik]ip route>add gateway=10.1.1.254 preferred-source=10.1.0.1
[admin@MikroTik]ip route>add dst-address=192.168.0.0/24 gateway=10.1.0.2\\...preferred-source=10.1.0.1
/interface sangoma
/interface sbe
[admin@MikroTik]>/interface sbe set sbe1 line-protocol=cisco-hdlc\\...clock-source=internal circuit-type=t1 disabled=no
[admin@R1]>/interface sbe print
[admin@R1]>/ip address add address 10.10.10.1/24 interface=sbe1
called wlan1 to set it as an Access Point
/interface wireless set wlan1 ssid="test" frequency=2442 band=2.4ghz-b/g\mode=ap-bridge disabled=no
To make a point-to-point connection,using 802.11 a standard,frequency 5805MHz and Service Set Identifier p2p:
/interface wireless set wlan1 ssid="p2p" frequency=5805 band=5ghz\mode=bridge disabled=no
/interface wireless set wlan1 ssid="p2p" band=5ghz mode=station disabled=no
/interface wireless
[admin@MikroTik]interface wireless>set 0 ssid=hotspot band=2.4ghz-b\ disabled=no
[admin@MikroTik]interface wireless>mo 0
Nstreme Settings
/interface wireless nstreme
[admin@MikroTik]interface wireless nstreme>print
Nstreme2 Group Settings
/interface wireless nstreme-dual
To enable the nstreme2 protocol on a router:
[admin@MikroTik]interface wireless>set 0,1 mode=nstreme-dual-slave
Add nstreme2 interface with exact-size framing:
[admin@MikroTik]interface wireless nstreme-dual>add\\...framer-policy=exact-size
And configure which card will be receiving,and wich-transmitting
[admin@MikroTik]interface wireless nstreme-dual>set 0 disabled=no\\...tx-radio=wlan1 rx-radio=wlan2
Registration Table
/interface wireless registration-table
[admin@MikroTik]interface wireless registration-table>print
To get additional statistics
[admin@MikroTik]interface wireless>registration-table print stats
/interface wireless access-list
To allow authentication and forwarding for the client 00:01:24:70:3A:BB from the wlan1 interface using WEP 40bit algorithm with the key 1234567890:
[admin@MikroTik]interface wireless access-list>add mac-address=\\...00:01:24:70:3A:BB interface=wlan1 private-algo=40bit-wep private-key=1234567890
/interface wireless info
[admin@MikroTik]interface wireless info>print
Add a VAP:
/interface wireless add master-interface=wlan1 ssid=VAP1 disabled=no
[admin@MikroTik]interface wireless>print
/interface wireless wds
[admin@MikroTik]interface wireless wds>add master-interface=wlan1\\...wds address=00:0B:6B:30:2B:27 disabled=no
[admin@MikroTik]interface wireless wds>print
/interface wireless align
[admin@MikroTik]interface wireless align>print
/interface wireless align monitor
[admin@MikroTik]interface wireless align>monitor wlan2
[admin@MikroTik]interface wireless>scan wlan1 refresh-interval=1s

AP to Client Configuration Example

To change the settings for the wireless AP interface:

[admin@AP]interface wireless>set 0 mode=ap-bridge ssid=test1\\...disabled=no frequency=5180 band=5GHz

Then we need to configure the wireless client interface:

[admin@MikroTik]interface wireless>set 0 mode=station ssid=test1\\...disabled=no

[admin@AP]interface wireless>monitor 0

WDS Configuration Example

At first we should configure the wireless interface for router Home

[admin@Home]interface wireless>set wlan1 mode=ap-bridge ssid=wds-test\\...wds-mode=static disabled=no

Add and configure a WDS interface

[admin@Home]interface wireless wds>add wds-address=00:01:24:70:3B:AE\\...master-inteface=wlan1 disabled=no

Add the IP address to the WDS interface:

[admin@Home]ip address>add address=192.168.25.2/24 interface=wds1

At first we should configure the wireless interface for router Neighbour:

[admin@Neighbour]interface wireless>set wlan1 mode=ap-bridge ssid=wds-test\\...wds-mode=static disabled=no

Now the WDS interface configuration:

[admin@Neighbour]interface wireless wds>add wds-address=00:01:24:70:3A:83\\...master-inteface=wlan1 disabled=no

On the AP set the security to required and choose which encryption algorithm to use:

[admin@AP]interface wireless security>set 0 security=required\\...algo-1=40bit-wep key-1=0123456789 transmit-key=key-1

On the client side do the same:

[admin@Client]interface wireless security>set 0 security=required\\algo-1=40bit-wep key-1=0123456789 transmit-key=key-1

/interface expeed

[admin@r1]ip address>add inter=xpeed1 address1.1.1.1/24

[admin@r1]interface xpeed>print

[admin@r1]ip address>add inter=xpeed1 address1.1.1.1/24

[admin@r1]interface xpeed>print

/interface eoip

On router with IP address 10.5.8.1,add an EoIP interface and set its MAC address:

/interface eoip add remote-address=10.1.0.1 tunnel-id=1 mac-address=00-00-5E-80-00-01\\...disabled=no

On router with IP address 10.1.0.1,add an EoIP interface and set its MACaddress::

/interface eoip add remote-address=10.5.8.1 tunnel-id=1 mac-address=00-00-5E-80-00-02\\...disabled=no

To add and enable an EoIP tunnel named to_mt2 to the 10.5.8.1 router,specifying tunnel-id of 1:

[admin@MikroTik]interface eoip>add name=to_mt2 remote-address=10.5.8.1\\...tunnel-id1

[admin@MikroTik]interface eoip>print

[admin@MikroTik]interface eoip>enable 0

Create a PPTP tunnel between them. Our_GW will be the pptp server:

[admin@Our_GW]interface pptp-server>/ppp secret add name=joe service=pptp\\...password=top_s3local-address=10.0.0.1 remote-address=10.0.0.2

[admin@Our_GW]interface pptp-server>add name=from_remote user=joe

[admin@Our_GW]interface pptp-server>server set enable=yes

[admin@Our_GW]interface pptp-server>print

Configure the EoIP tunnel by adding the eoip tunnel interfaces at both routers

[admin@Our_GW]interface eoip>add name="eoip-remote"tunnel-id=0\\...remote-address=10.0.0.2

[admin@Our_GW]interface eoip>enable eoip-remote

[admin@Our_GW]interface eoip>print

[admin@Remote]interface eoip>add name="eoip"tunnel-id=0\\...remote-address=10.0.0.1

[admin@Remote]interface eoip>enable eoip-main

[admin@Remote]interface eoip>print

Enable bridging between the EoIP and Ethernet interfaces on both routers. On the Our_GW:

admin@Our_GW]interface bridge>add forward-protocols=ip,arp,other\\...disabled=no
[admin@Our_GW]interface bridge>port print
[admin@Our_GW]interface bridge>port set "0,1" bridge=bridge1
[admin@Remote]interface bridge>add forward-protocols=ip,arp,other\\...disabled=no
[admin@Remote]interface bridge>print
[admin@Remote]interface bridge>port print
[admin@Remote]interface bridge>port set"0,2" bridge=bridge1
/ip ipsec policy
To add a policy to encrypt all the traffic between two hosts(10.0.0.147 and 10.0.0.148),we need do the following:
[admin@WiFi]ip ipsec policy>add sa-src-address=10.0.0.147\\...sa-dst-address=10.0.0.148 action=encrypt
[admin@WiFi]ip ipsec policy>print stats
/ip ipsec peer
[admin@WiFi]ip ipsec peer>add address=10.0.0.147/32\\...secret=gwejimezyfopmekun
[admin@WiFi]ip ipsec peer>print
/ip ipsec remote-peers
[admin@WiFi]ip ipsec>remote-peers print
/ip ipsec installed-sa
[admin@WiFi]ip ipsec>installed-sa print
Flushing Installed SA Table
/ip ipsec installed-sa flush
To flush all the SAs installed:
[admin@MikroTik]ip ipsec installed-sa>flush
[admin@MikroTik]ip ipsec installed-sa>print
[admin@MikroTik]ip ipsec installed-sa>
/ip ipsec counters
[admin@WiFi]ip ipsec>counters print
Transport mode example using ESP with automatic keying
[admin@Router1]>ip ipsec policy add sa-src=1.0.0.1 sa-dst=1.0.0.2\\...action=encrypt
[admin@Router1]>ip ipsec peer add address=1.0.0.2\\...secret="gvejimezyfopmekun"
Transport mode example using ESP with automatic keying and automatic policy generating on Router1 and static policy on Router2
[admin@Router1]>ip ipsec peer addaddress=1.0.0.0/24\\...secret="gvejimezyfopmekun" generate-policy=yes
Tunnel mode example using AH with manual keying
[admin@Router1]>ip ipsec manual-sa add name=ah-sa1\\...ah-spi=0x101/0x100ah-key=abcfed
[admin@Router1]>ip ipsec policy add src-address=10.1.0.0/24\\...dst-address=10.2.0.0/24 action=encrypt ipsec-protocols=ah\\...tunnel=yes sa-src=1.0.0.1 sa-dst=1.0.0.2 manual-sa=ah-sa1
Add accept and masquerading rules in SRC-NAT
[admin@Router1]>ip firewall src-nat\\...add src-address=10.1.0.0/24 dst-address=10.2.0.0/24
[admin@Router1]>ip firewall src-nat add out-interface=public\\...action=masquerade
Configure IPsec
[admin@Router1]>ip ipsec policy add src-address=10.1.0.0/24\\...dst-address=10.2.0.0/24 action=encrypt tunnel=yes\
\...sa-src-address=1.0.0.1 sa-dst-address=1.0.0.2
[admin@Router1]>ip ipsec peer add address=1.0.0.2\\...exchange-mode=aggressive secret="gvejimezyfopmekun"
Add peer for MikroTik router
[admin@MikroTik]>ip ipsec peer add address=10.0.1.2\\...secret="gvejimezyfopmekun" enc-algorithm=des
Set encryption proposal
[admin@MikroTik]>ip ipsec proposal set default enc-algorithms=des
Add policy rule
[admin@MikroTik]>ip ipsec policy add\\...src-address=10.0.0.0/24 dst-address=10.0.2.0/24 action=encrypt\
\...tunnel=yes sa-src=10.0.1.1 sa-dst=10.0.1.2

Testing the IPsec tunnel
[admin@MikroTik]ip ipsec installed-sa>print
MikroTik Router configuration:
[admin@MikroTik]>/ip ipsec peer add address=192.168.0.108\\...secret="gvejimezyfopmekun"hash-algorithm=md5enc-algorithm=3des\\...dh-group=modp1024 lifetime=28800s

[admin@MikroTik]>/ip ipsec proposal auth-algorithms=md5\\...enc-algorithms=3des pfs-group=none

[admin@MikroTik]>/ip ipsec policy add sa-src-address=192.168.0.155\\...sa-dst-address=192.168.0.108 src-address=10.0.0.0/24\\...dst-address=192.168.87.0/24 tunnel=yes

To make an IPIP tunnel between 2 MikroTik routers

Configuration on router with IP address 10.5.8.104:

1.Add an IPIP interface(by default,its name will be ipip1):
[admin@10.5.8.104]interface ipip>add local-address=10.5.8.104\remote-address=10.1.0.172 disabled=no
2.Add an IP address to created ipip1 interface:
[admin@10.5.8.104]ip address>add address=10.0.0.1/24 interface=ipip1

Configuration on router with IP address 10.1.0.172:

1.Add an IPIP interface(by default, its name will be ipip1):
[admin@10.1.0.172]interface ipip>add local-address=10.1.0.172\ remote-address=10.5.8.104 disabled=no
2.Add an IP address to created ipip1 interface:
[admin@10.1.0.172]ip address>add address=10.0.0.2/24 interface=ipip1

Configuration on L2TP server router:
1.Add a L2TP user:
[admin@L2TP-Server]ppp secret>add name=james password=pass\\...local-address=10.0.0.1remote-address=10.0.0.2
2.Enable the L2TP server
[admin@L2TP-Server]interface l2tp-server server>set enabled=yes
•Configuration on L2TP client router:
1.Add a L2TP client:
[admin@L2TP-Client]interface l2tp-client>add user=james password=pass\\...connect-to=10.5.8.104
/interface l2tp-server,/interface l2tp-client
L2TP Client Setup
[admin@MikroTik]interface l2tp-client>add name=test2 connect-to=10.1.1.12\\...user=john add-default-route=yes password=john
[admin@MikroTik]interface l2tp-client>print
[admin@MikroTik]interface l2tp-client>enable 0
[admin@MikroTik]interface l2tp-client>monitor test2
L2TP Server Setup
/interface l2tp-server server
[admin@MikroTik]interface l2tp-serve rserver>set enabled=yes
[admin@MikroTik]interface l2tp-server server>print
[admin@MikroTik]interface l2tp-server>add user=ex1
[admin@MikroTik]interface l2tp-server>print
On the L2TP server a user must be setup for the client:
[admin@HomeOffice]ppp secret>add name=ex service=l2tp password=lkjrht local-address=10.0.103.1 remote-address=10.0.103.2
[admin@HomeOffice]ppp secret>print detail

Then the user should be added in the L2TP server list:
[admin@HomeOffice]interface l2tp-server>add user=ex
[admin@HomeOffice]interface l2tp-server>print
And the server must be enabled:
[admin@RemoteOffice]interface l2tp-server server>set enabled=yes
[admin@RemoteOffice]interface l2tp-server server>print
Finally,the proxy APR must be enabled on the 'Office' interface:
[admin@RemoteOffice]interface ethernet>set Office arp=proxy-arp
[admin@RemoteOffice]interface ethernet>print

ToconfigureMikroTikRouterOStobeaPPPoEclient
1.Just add a pppoe-client:
/interfacepppoe-clientaddname=pppoe-user-mikeuser=mikepassword=123interface=wlan1\\...service name=internet disabled=no
To configure MikroTik RouterOS to be an Access Concentrator (PPPoE Server)
1.Add an address pool for the clients from 10.1.1.62 to 10.1.1.72,called pppoe-pool:
/ip pool add name="pppoe-pool" ranges=10.1.1.62-10.1.1.72
2.Add PPP profile,called pppoe-profile where local-address will be the router's address and clients will have an address from pppoe-pool:
/ppp profile add name="pppoe-profile" local-address=10.1.1.1 remote-address=pppoe-pool
3.Add a user with username mike and password 123:
/ppp secret add name=mike password=123 service=pppoe profile=pppoe-profile
4.Now add a pppoe server:
/interface pppoe-server server add service-name=internet interface=wlan1\\...default-profile=pppoe-profile
PPPoE Client Setup
/interface pppoe-client

To add and enable PPPoE client on the gig interface connecting to the AC that provides testSN service using username john with the password =password:
[admin@RemoteOffice]interface pppoe-client>add interface=gig\\...service-name=testSN user=john password=password disabled=no
[admin@RemoteOffice]interface pppoe-client>print
[admin@MikroTik]interface pppoe-client>monitor pppoe-out1
To add PPPoE server on ether1 interface providing ex service
[admin@MikroTik]interface pppoe-server server>add interface=ether1\\...service-name=ex one-session-per-host=yes
[admin@MikroTik]interface pppoe-server server>print
PPPoE Server Setup(Access Concentrator)
/interface pppoe-server server
PPPoE users are created in /ppp secret menu
To add PPPoE server on ether1 interface providing ex service
[admin@MikroTik]interface pppoe-server server>add interface=ether1\\...service-name=ex one-session-per-host=yes
[admin@MikroTik]interface pppoe-server server>print
To view the currently connected users:
[admin@MikroTik]interface pppoe-server>print
To disconnect the user ex:
[admin@MikroTik]interface pppoe-server>remove [find user=ex]
I can not connect to my PPPoE server.
[admin@MT]interface pppoe-server server>set 0 max-mtu=1440 max-mru=1440
[admin@MT]interface pppoe-server server>print
First of all,the Prism interface should be configured:
[admin@MT_Prism_AP]interface prism>set 0 mode=ap-bridge frequency=2442MHz\\...ssid=mt disabled=no
[admin@MT_Prism_AP]interface prism>print

We should add PPPoE server to the Prism interface:
[admin@MT_Prism_AP]interface pppoe-server server>add interface=prism1\\...service-name=mt one-session-per-host=yes disabled=no
[admin@MT_Prism_AP]interface pppoe-serve rserver>print
[admin@MT_Prism_AP]ip firewall mangle>add protocol=tcp tcp-options=syn-only\\..action=passthrough tcp-mss=1440
[admin@MT_Prism_AP]ip firewall mangle>print
And finally,we can setup PPPoE clients:
[admin@MT_Prism_AP]ip pool>add name=pppoe ranges=10.0.0.230-10.0.0.240
[admin@MT_Prism_AP]ip pool>print
[admin@MT_Prism_AP]ppp profile>.. secret
[admin@MT_Prism_AP]ppp secret>

PPTP
Setup on PPTP server:
1.Add a user:
[admin@PPTP-Server]ppp secret>add name=jack password=pass\\...local-address=10.0.0.1 remote-address=10.0.0.2
2.Enable the PPTP server:
[admin@PPTP-Server]interface pptp-server server>set enabled=yes
Setup on PPTP client:
1.Add the PPTP client:
[admin@PPTP-Client]interface pptp-client>add user=jack password=pass\\...connect-to=10.5.8.104 disabled=no

To setup PPTP client named test2 using username john with password john to connect to the 10.1.1.12 PPTP server and use it as the default gateway:

[admin@MikroTik]interface pptp-client>add name=test2 connect-to=10.1.1.12\\...user=john add-default-route=yes password=john
[admin@MikroTik]interface pptp-client>print
[admin@MikroTik]interface pptp-client>enable0
[admin@MikroTik]interface pptp-client>monitor test2
PPTP Server Setup
/interface pptp-server server
To enable PPTP server:
[admin@MikroTik]interface pptp-server server>set enabled=yes
[admin@MikroTik]interface pptp-server server>print
To add a static entry for ex1 user
[admin@MikroTik]interface pptp-server>add user=ex1
[admin@MikroTik]interface pptp-server>print
Onthe Preforma PPTP server a user must be setup for the client:
[admin@HomeOffice]ppp secret>add name=ex service=pptp password=lkjrht local-address=10.0.103.1 remote-address=10.0.103.2
[admin@HomeOffice]ppp secret>print detail
Then the user should be added in the PPTP serverlist:
[admin@HomeOffice]interface pptp-server>add user=ex
[admin@HomeOffice]interface pptp-server>print
[admin@HomeOffice]interface pptp-server server>set enabled=yes
[admin@HomeOffice]interface pptp-server server>print
Add a PPTP client to the Remote Office router:
[admin@RemoteOffice]interface pptp-client>add connect-to=192.168.80.1 user=ex\\...password=lkjrht disabled=no
[admin@RemoteOffice]interface pptp-client>print
To route the local Intranets over the PPTP tunnel you need to add these routes:
[admin@HomeOffice]>ip route add dst-address 10.150.1.0/24 gateway 10.0.103.2
[admin@RemoteOffice]>ip route add dst-address 10.150.2.0/24 gateway 10.0.103.1

On the PPTP server a user must be setup for the client:
[admin@RemoteOffice]ppp secret>add name=ex service=pptp password=lkjrht
local-address=10.150.1.254 remote-address=10.150.1.2
[admin@RemoteOffice]ppp secret>print detail
Then the user should be added in the PPTP server list:
[admin@RemoteOffice]interfacepptp-server>add name=FromLaptop user=ex
[admin@RemoteOffice]interface pptp-server>print
And the serve rmust be enabled:
[admin@RemoteOffice]interface pptp-server server>set enabled=yes
[admin@RemoteOffice]interface pptp-server server>print
Finally, the proxy APR must be enabled on the 'Office' interface:
[admin@RemoteOffice]interface ethernet>set Office arp=proxy-arp
[admin@RemoteOffice]interface ethernet>print

Vlan Interface – Page-300

VLAN Setup
/interface vlan
[admin@MikroTik]interface vlan>add name=test vlan-id=1 interface=ether1
[admin@MikroTik]interface vlan>print
[admin@MikroTik]interface vlan>add name=test vlan-id=32 interface=ether1
[admin@MikroTik]interface vlan>print
[admin@MikroTik]ip address>add address=10.10.10.1/24interface=test
[admin@MikroTik]ip address>print
[admin@MikroTik]ip address>add address=10.10.10.2/24 interface=test
[admin@MikroTik]ip address>print
SNMP Service
/snmp
To enable the service, specifying some info:
[admin@MikroTik]snmp>set contact="admin@riga-2" location="3rdfloor" enabled="yes"
[admin@MikroTik]snmp>print
/snmp community
[admin@MikroTik]snmp community>print
[admin@MikroTik]snmp community>set 0 read-access=no
[admin@MikroTik]snmp community>print
To see available OID values
[admin@motors]systemre source>print oid
To use the 10.5.13.11 host,listening on 514 port,as the default remote system-log server:
[admin@MikroTik]system logging>set default-remote-address=10.5.13.11 default-remote-port=514
[admin@MikroTik]system logging>print
To force the router to send Firewall-Log to the 10.5.13.11 server:
[admin@MikroTik]system logging facility>set Firewall-Log remote=syslog\\...remote-address=10.5.13.11 remote-port=514
[admin@MikroTik]system logging facility>print
To view the local logs:
[admin@MikroTik]>log print
To monitor the system log:
[admin@MikroTik]>log print follow
To add red queue type with minimum threshold of 0,without any burst and named CUSTOMER-def:
[admin@MikroTik]queue type>add name=CUSTOMER-def kind=red\\...red-min-threshold=0 red-burst=0
[admin@MikroTik]queue type>print

/queue interface
[admin@MikroTik]queue interface>print

To add a simple queue that will limit download traffic for network 192.168.0.0/24 to 128000 bits Per second,and upload traffic from the network 192.168.0.0/24 to 64000 bits per second on the interface ether1:interface:
[admin@MikroTik]queue simple>add target-address=192.168.0.0/24 interface=ether1\\...max-limit=64000/128000
[admin@MikroTik]queue simple>print
Home menu level: /queue tree
The queue trees should be used when you want to use sophisticated data rate allocation based on protocols, ports, groups of IP addresses,etc.

To apply queues on flows,the mangle feature should be used first to mark incoming packets.
The router tries to apply queue trees before simple queues.
To mark all the traffic going from web-servers(TCP port 80)with abc-http mark:
[admin@MikroTik]ip firewall mangle>add action=passthrough mark-flow=abc-http\ \...protocol=tcp target-port=80
[admin@MikroTik]ip firewall mangle>print

You can add queue using the **/queue tree add** command:

[admin@MikroTik]queue tree>add name=HTTP parent=ether1 flow=abc-http\max-limit=128000
[admin@MikroTik]queue tree>print

Add a simple queue rule which will limit download traffic to 128kbps and upload traffic to 64kbps For clients on local network(192.168.0.0/24):
/queue simple add name=Limit-Local target-address=192.168.0.0/24\ interface=Local max-limit=65536/131072
[admin@MikroTik]queue simple>print
[admin@MikroTik]interface>monitor-traffic Local

If you want to exclude the server from being limited,add a queue for it without limitation(max-limit=0/0 which means no limitation)and move it to the top:

/queue simple add name=Exclude-Server interface=Local\target-address=192.168.0.1/32/queue simple move 1 0
[admin@MikroTik]queue simple>print

Mark server's download and upload traffic.At first we will mark the outgoing connection and Then all packets which belong to this connection.
/ip firewall mangle add src-address=192.168.0.1/32 action=passthrough mark-connection=server-con
Add connection=server-conaction=accept mark-flow=server
The same for laptop and workstation:
/ip firewall mangle addsrc-address=192.168.0.2/32 action=passthrough\mark-connection=lap_work-con
add src-address=192.168.0.3/32 action=passthrouth\mark-connection=lap_work-con
add connection=lap_work-conaction=accept mark-flow=lap_work

Now add rules in **/queue tree** server
/queue tree
Add name=Server-Down parent=Local flow=server limit-at=131072\max-limit=262144
add name=Server-Up parent=Public flow=server limit-at=65536\max-limit=131072

And the same for Laptop and Workstation
/queue tree add name=Laptop-WorkStation-Down parent=Local flow=lap_work\limit-at=65536 max-limit=262144
Add name=Laptop-WorkStation-Up parent=Public flow=lap_work\limit-at=32768 max-limit=131072

Limit the overall download(256k)and upload(128k)traffic:
/queue tree
Add parent=Local max-limit=262144 name=Download
Add parent=Public max-limit=131072 name=Upload

Mark FTP connection,initiated byFTP server(will not work for FTP passive mode!):
/ip firewall mangle add src-address=192.168.0.1/32 src-port=20-21\mark-connection=ftp-con protocol=tcp action=passthrough
Mark all packets belonging to this connection with a mark ftp:
/ip firewall mangle add connection=ftp-con mark-flow=FTP_Server action=accept
Mark other traffic:
/ip firewall mangle add action=accept mark-flow=other
Add queues for FTP Server download and upload:
/queue tree add name=Server_Upload parent=Upload limit-at=65536\flow=FTP_Server max-limit=131072 priority=7
/queue tree add name=Server_Download parent=Download limit-at=32768\flow=FTP_Server max-limit=262144 priority=7
Add queues for other's download and upload:
/queue tree add name=Other_Upload parent=Upload flow=other
/queue tree add name=Other_Download parent=Download flow=other

Assume that you already have configured your web-proxy:
[admin@MikroTik]ip web-proxy>print

Add a mangle rule for marking all packets coming from interface Public:
/ip firewall mangle add in-interface=Public mark-flow=all-down action=accept
Add a mangle rule for marking all packets coming from interface Local:
/ip firewall mangle add in-interface=Local mark-flow=all-up action=accept
Add a queue tree rule that will limit all traffic coming from interface Public (flow=all-down) to 512kbps:
/queue tree add parent=global-in max-limit=524288 flow=all-down
Add a queue tree rule that will limit all traffic coming from interface Local (flow=all-up)to 256kbps:
/queue tree add parent=global-out max-limit=262144 flow=all-up

In situations when you want to limit users in your network to a specific bandwidth, you can use **PCQ.**

1.Mark all packets with flow all:
/ip firewall mangle add action=accept mark-flow=all
2.Create two PCQ queue types-one for download and one for upload.For download traffic Queues will be classified by dst-address and for upload-by src-address:
/queue type add name=PCQ-Download kind=pcq pcq-rate=65536\pcq-classifier=dst-address
/queue type add name=PCQ-Upload kind=pcq pcq-rate=32768\pcq-classifier=src-address
3.Add two queue rules-one for download and one for upload:
/queue tree add parent=global-in queue=PCQ-Download flow=all
/queue tree add parent=global-out queue=PCQ-Upload flow=all

Let us consider that we want to mangle all packets which are leaving the network 192.168.0.0/24 and are destined to a HTTP web-server(protocolTCP,port80),with a flow, labeled http-traffic:

[admin@MikroTik]ip firewall mangle>src-address=192.168.0.0/24\\...dst-port=80 mark-flow=http-traffic

/ip firefall mangle

[admin@test_1]ip firewall mangle>add action=passthrough mark-flow=myflow
[admin@test_1]ip firewall mangle>print
[admin@test_1]ip fire wall mangle>add protocol=tcp\\..tcp-options=syn-only action=passthrough tcp-mss=1448
[admin@test_1]ip firewall mangle>print

Suppose you need to limit both download and upload peer-to-peer data rate for NATted local users.It can be achieved using queue trees and mangle facility.

/ip firewall mangle add src-address=192.168.0.0/24 action=passthrough mark-connection=nat_conn
/ip firewall mangle add connection=nat_connmark-flow=my_clients

Network Address Translation(NAT) provides ways for hiding local networks as well as to maintain Public services on servers from these networks.

Let us consider that we have a private network 192.168.0.0/24 and we want it to be able to use A single public IP address,which is assigned to interface Public.This can be done with masquerading:
[admin@MikroTik]ip firewall src-nat>add src-address=192.168.0.0/24\...out-interface=Public action=masquerade

Let us consider that we have a Web-Server in our private network 192.168.0.0/24 with IP address 192.168.0.2.To redirect all HTTP traffic from the router'saddress(10.5.8.104) to the Web-Server,use the following command:

[admin@MikroTik]ip firewall dst-nat>add dst-address=10.5.8.104/32 dst-port=80\\...to-dst address=192.168.0.2 protocol=tcp action=nat

/ip firefall src-nat,/ip firewall dst-nat

To use masquerading, a source NAT rule with action=masquerade should be added to the src-nat Rule set:
[admin@test_1]ip firewall src-nat>add src-address=192.168.0.0/24\\...out-interface=wlan1 action=masquerade
[admin@test_1]ip firewall src-nat>print
If you want to change the source address:port to specific adress:port,use the action=nat instead of action=masquerade:
[admin@test_1]ip firewall src-nat>add src-address=192.168.0.1/32 out-interface =wlan1 action=nat to-src-address=1.1.1.1
[admin@test_1]ip firewall src-nat>print

This example shows how to add a dst-NAT rule that gives access to the http server 192.168.0.4on The local network via external address 10.0.0.217:
[admin@MikroTik]ip firewall dst-nat>add action=nat protocol=tcp\\...dst-address=10.0.0.217/32:80 to-dst address=192.168.0.4
[admin@MikroTik]ip firewall dst-nat>print

To set www service to use 8081 port accessible from the 10.10.10.0/24 network:

[admin@MikroTik]ip service>print
[admin@MikroTik]ip service>set www port=8081 address=10.10.10.0/24
[admin@MikroTik]ip service>print

Services, Protocols ,and Ports

Port/Protocol	Description
20/tcp	File Transfer [Default Data]
21/tcp	File Transfer [Control]
22/tcp	SSH Remote Login Protocol (Only with security package)
23/tcp	Domain Name Server
53/tcp	Domain Name Server
67/udp	Bootstrap Protocol Server, DHCP Client (only with dhcp package)
68/udp	Bootstrap Protocol Client, DHCP Client (only with dhcp package)
80/tcp	World Wide Web HTTP
123/tcp	Network Time Protocol (Only with ntp package)
161/tcp	SNMP (Only with snmp package)
443/tcp	Secure Socket Layer Encrypted HTTP(Only with hotspot package)
500/udp	IKE protocol (Only with ipsec package)
179/tcp	Border Gateway Protocol (Only with routing
	package)
1719/udp	h323gatestat (Only with telephony package)
1720/tcp	h323hostcall (Only with telephony package)
1723/tcp	pptp (Only with ppp package)
2000/tcp	bandwidth-test server
3986/tcp	proxy for winbox
3987/tcp	sslproxy for secure winbox (Only with security package)
5678/udp	MikroTik Neighbor Discovery Protocol
8080/tcp	HTTP Alternate (Only with web-proxy package)
/1	ICMP - Internet Control Message
/4	IP - IP in IP (encapsulation)
/47	GRE - General Routing Encapsulation (Only for PPTP and EoIP)
/50	ESP - Encapsulating Security Payload for IPv4 (Only with security package)
/51	AH - Authentication Header for IPv4 (Only with security package)
/89	OSPFIGP - OSPF Interior Gateway Protocol

DHCP Client and Server

Setup of a DHCP-Server.
1.Create an IP address pool
/ip pool add name=dhcp-pool1 ranges=172.16.0.10-172.16.0.20
2. Add a DHCP network which will concern to the network 172.16.0.0/12 and will Distribute a gateway with IP address 172.16.0.1 to DHCP clients:
/ip dhcp-server network add address=172.16.0.0/12 gateway=172.16.0.1
3. Finally, add a DHCPserver:
/ip dhcp-server add interface=wlan1 address-pool=dhcp-pool
Setup of the DHCP-Client (which will get a lease from the DHCP server, configured above).
1.Add the DHCP client:
/ip dhcp-client set interface=wlan1 enabled=yes
2.Check whether you have obtained a lease:
[admin@DHCP-Client]ip dhcp-client lease>print
[admin@DHCP-Client]ip dhcp-client lease>
To enable DHCP client on ether1 interface
[admin@MikroTik]ip dhcp-client>set enabled=yes interface=ether1
To check the obtained lease:
[admin@MikroTik]ip dhcp-client lease>print
To add a DHCP server to the ether1 interface
[admin@MikroTik]ip dhcp-server>add name=dhcp-office disabled=no\\...address-pool=dhcp-clients interface=ether1 lease-time=2h
[admin@MikroTik]ip dhcp-server>print

/ip dhcp-server network
/ip dhcp-server lease
/ip dhcp-relay

To add a DHCP relay named relay on ether1 interface resending all received requests to the 10.0.0.1 DHCP server:
[admin@MikroTik]ip dhcp-relay>add name=relay interface=ether1\\...dhcp-server=10.0.0.1 disabled=no
[admin@MikroTik]ip dhcp-relay>print
/ip dhcp-server setup

To configure DHCP server on ether1 interface to lend addresses from 10.0.0.2 to 10.0.0.254 which Belong to the 10.0.0.0/24 network with 10.0.0.1 gateway and 159.148.60.2 DNS server for the time Of 3 days:

[admin@MikroTik]ip dhcp-server>setup
[admin@MikroTik]ip dhcp-server>print
[admin@MikroTik]ip dhcp-server>network print
[admin@MikroTik]ip dhcp-server>/ip pool print

DNS Client and Cache

To set 159.148.60.2 as the primary DNS server,do the following:
[admin@MikroTik]ip dns>set primary-dns=159.148.60.2

/ip dns cache, /ip dns static
To add a static DNS entry for www.example.com to be resolved to 10.0.0.1 IP address:
[admin@MikroTik]ip dns static>add name www.example.com address=10.0.0.1
[admin@MikroTik]ip dns static>print

To configure HotSpot on ether1 interface
[admin@MikroTik]ip hotspot>setup
Select interface to run HotSpot on
Hotspot interface:ether1
Use SSL authentication?
Use ssl:no
Add hotspot authentication for existing interface setup?
Interface already configured:yes
Create local hotspot user
Name of local hotspot user: admin
Password for the user: rubbish
Use transparent web proxy for hotspot clients?
Use transparent web proxy:yes
[admin@MikroTik]ip hotspot>
To enable cookie support:
[admin@MikroTik]ip hotspot>set auth-http-cookie=yes
[admin@MikroTik]ip hotspot>print
/ip hotspot profile
[admin@MikroTik]ip hotspot profile>set default login-method=enabled-address\\...mark-flow=logged-in keepalive-timeout=1m
[admin@MikroTik]ip hotspot profile>print

To define an additional profile that will also limit download speed to 64 kilobyte/s and upload data Rate to 32 kilobyte/s and call it limited:

[admin@MikroTik]ip hotspot profile>add copy-from=default tx-bit-rate=65536\\...rx-bit-rate=32768 name=limited
[admin@MikroTik]ip hotspot profile>print

To add user Ex with password Ex that is allowed to login only with 01:23:45:67:89:AB MAC Address and is limited o 1 hour of work:
[admin@MikroTik]ip hotspot user>add name=Ex password=Ex\\...mac-address=01:23:45:67:89:AB limit-uptime=1h
[admin@MikroTik]ip hotspot user>print

/ip hotspot active
To get the list of active users:
[admin@MikroTik]ip hotspot active>print
/ip hotspot aaa
To enable RADIUS AAA:
[admin@MikroTik]ip hotspot aaa>set use-radius=yes
[admin@MikroTik]ip hotspot aaa>print
To add a HotSpot server named dhcp1 to the DHCP server hotspot-dhcp giving IP addresses from the hotspot address pool:
[admin@MikroTik]ip hotspot server>add name=dhcp1 dhcp-server=hotspot-dhcp\\...address-pool=hotspot
[admin@MikroTik]ip hotspot server>print

/ip hotspot set http-cookie-lifetime=3d
To get the list of valid cookies:
[admin@MikroTik]ip hotspot cookie>print

/ip hotspot walled-garden
Walled garden is a system which allows unauthorized use of some resources

Currently you cannot place HTTPS servers inside theWalledGarden.However,there is a work around on this.You can add a mangle rule that allows you to pass traffic to an IP address of secure web server, exempli gratia:
/ip firewall mangle add dst-address=159.148.108.1/32 mark-flow=hs-auth
To allow unauthorized requests to the www.example.com domain's /paynow.html page:
[admin@MikroTik]ip hotspot walled-garden>add path="^/paynow\\.html$"\\...dst-host="^www\\.example\\.com$"
[admin@MikroTik]ip hotspot walled-garden>print

HotSpot Step-by-Step User Guide for dhcp-pool Method
ARP should be set to reply-only mode on the prism1 interface
/interface prism set prism1 arp=reply-only
Add two IP addresses to the prism1 interface
/ip address add address=192.168.0.1/24 interface=prism1\ comment="hotspot temporary network"
/ip address add address=10.5.50.1/24 interface=prism1\ comment="hotspot real network"
add2 IP address pools:
/ip pool add name=hs-pool-temp ranges=192.168.0.2-192.168.0.254
/ip pool add name=hs-pool-real ranges=10.5.50.2-10.5.50.254
Add masquerading rule for temporary IP pool,which is not routed:
/ip firewall src-nat add src-address=192.168.0.0/24 action=masquerade\ comment="masquerade hotspot temporary network"
Add dhcp server
/ip dhcp-server add name="hs-dhcp-server" interface=prism1 lease-time=14s\address-pool=hs-pool-temp add-arp=yes disabled=no
/ip dhcp-server network add address=192.168.0.0/24 gateway=192.168.0.1\dns server=159.148.60.2,159.148.108.1 domain="example.com"
Add hotspot server setup(for real IP addresses):
/ip hotspot server add name=hs-server dhcp-server=hs-dhcp-server\ address-pool=hs-pool-real
/ip dhcp-server network add address=10.5.50.0/24 gateway=10.5.50.1\ dns-server=159.148.60.2,159.148.108.1 domain="example.com"
Add local hotspot user:
/ip hotspot user add name=Ex password=Ex
Setup hotspot service to run on port 80(www service has to be assigned another port,e.g.,8081):
/ip service set www port=8081
/ip service set hotspot port=80
Redirect all TCP requests from temporary IP addresses to hotspot service:
/ip firewall dst-nat add src-address=192.168.0.0/24 dst-port=443 protocol=tcp\action=redirect to-dst port=443\comment="redirect unauthorized hotspot clients to hotspot service"
/ip firewall dst-nat add src-address=192.168.0.0/24 protocol=tcp\action=redirect to-dst-port=80\comment="redirect unauthorized hotspot clients to hotspot service"
Allow DNS requests and ICMP ping from temporary addresses and reject everything else:
/ip firewall add name=hotspot-temp comment="limit unauthorized hotspot clients"
/ip firewall rule forward add src-address=192.168.0.0/24 action=jump\jump-target=hotspot-temp comment="limit access for unauthorized hotspot clients"
/ip firewall rule input add src-address=192.168.0.0/24 dst-port=80\ protocol=tcp action=accept comment="accept requests for hotspot servlet"
/ip firewall rule input add src-address=192.168.0.0/24 dst-port=443\ protocol=tcp action=accept comment="accept request for hotspot servlet"
/ip firewall rule input add src-address=192.168.0.0/24 dst-port=67\ protocol=udp action=accept comment="accept requests for local DHCP server"

/ip firewall rule input add src-address=192.168.0.0/24 action=jump\jump-target=hotspot-temp comment="limit access for unauthorized hotspot clients"
/ip firewall rule hotspot-temp add protocol=icmp action=return\comment="allow ping requests"
/ip firewall rule hotspot-temp add protocol=udp dst-port=53 action=return\comment="allow dns requests"
/ip firewall rule hotspot-temp add action=reject\comment="rejectaccessforunauthorizedhotspotclients"
Add hotspot chain:
/ip firewall add name=hotspot comment="account authorized hotspot clients"
Pass all through-going traffic to the hotspot chain:
/ip firewall rule forward add action=jump jump-target=hotspot\comment="account traffic for authorized hotspot clients"

HotS pot Step-by-Step User Guide for enabled-address Method Page-388
1.Setup hotspot service to run on port80 (www service has to be assigned another port,e.g.,8081):

/ip service set www port=8081
/ip service set hotspot port=80

2.Setup hotspot profile to mark authenticated users with flow name" hs-auth":

/ip hotspot profile set default mark-flow="hs-auth" login-method=enabled-address

3.Add local hotspot user:

/ip hotspot user add name=Ex password=Ex

4.Redirect all TCP requests from unauthorized clients to the hotspot service:

/ip firewall dst-nat add in-interface="prism1" flow="!hs-auth" protocol=tcp\ dst-port=443 action=redirect to-dst-port=443\ comment="redirect unauthorized hotspot clients to hotspot service"

/ip firewall dst-nat add in-interface="prism1" flow="!hs-auth" protocol=tcp\ action=redirect to-dst-port=80\ comment="redirect unauthorized clients to hotspot service"

5.Allow DNS requests and ICMP ping from temporary addresses and reject everything else:

/ip firewall add name=hotspot-temp comment="limit unauthorized hotspot clients"

/ip firewall ruleforward add in-interface=prism1 action=jump\jump-target=hotspot-temp comment="limit access for unauthorized hotspot clients"

/ip firewall rule input add in-interface=prism1 dst-port=80 protocol=tcp\ action=accept comment="accept requests for hotspot servlet"

/ip firewall rule input add in-interface=prism1 dst-port=443protocol=tcp\ action=accept comment="accept request for hotspot servlet"

/ip firewall rule input add in-interface=prism1 dst-port=67 protocol=udp\ protocol=udp action=accept comment="accept requests for local DHCP server"

/ip firewall rule input add in-interface=prism1 action=jump\jump-target=hotspot-temp comment="limit access for unauthorized hotspot clients"

/ip firewall rule hotspot-temp add flow="hs-auth" action=return\ comment="return if connection is authorized"

/ip firewall rule hotspot-temp add protocol=icmp action=return\comment="allow ping requests"
/ip firewall rule hotspot-temp add protocol=udp dst-port=53 action=return\comment="allow dns requests"
/ip firewall rule hotspot-temp add action=reject\comment="reject access for unauthorized clients"

6.Create a hotspot chain for authorized hotspot clients:
/ip firewall add name=hotspot comment="account authorized hotspot clients"
7.Pass all through-going traffic to the hotspot chain:
/ip firewall rule forward add action=jump jump-target=hotspot\comment="account traffic for authorized hotspot clients"

Note that: in order to use SSL authentication, you should install an SSL certificate. This topic is not Covered by this manual section. Please see the respective manual section on how to install Certificates in MikroTik Router OS

It is possible to add hotspot authentication for one more interface(prism2) by adding only 4 additional firewall rules:

Setup dst-nat to redirect unauthorized clients to the hotspot service:
/ip firewall dst-nat add in-interface="prism2" flow="!hs-auth"protocol=tcp\ dst-potr=443 action=redirect to-dst-port=443\ comment="redirect unauthorized prism2 clients to hotspot service"

/ip firewall dst-nat add in-interface="prism2" flow="!hs-auth"protocol=tcp\ action=redirect to-dst-port=80\ comment="redirect unauthorized prism2 clients to hotspot service"

Limit access for unauthorized prism2 interface clients:

/ip firewall rule forward add in-interface=prism2 action=jump\jump-target=hotspot-temp comment="limit access for unauthorized prism2 clients"

/ip firewall rule input add in-interface=prism2 action=jump\jump-target=hotspot- temp comment="limit access for unauthorized prism2 clients"

You may want to translate the destination addresses of all TCP port 25 connections(SMTP) from HotSpot users to your local mail sever for mail relaying. Thus, users can retain their mail Client setup and use your mail server for outgoing mail without reconfiguring their mail clients.
If 10.5.6.100 is your mail server accepting connections from network 10.5.50.0/24,then the Required destination NAT rule would be:
/ip firewall dst-nat add src-address=10.5.50.0/24 dst-port=25protocol=tcp\ to-dst-address=10.5.6.100 action=nat\ comment="Translate SMTP TCP 25 port to our mail server"
One more option is to allow access certain pages without authentication(walled garden).For example,if http://hotspot.example.com is your web server's name:
[admin@MikroTik]ip hotspot walled-garden>add\ \...dst-host="^hotspot\\.example\\.com$"

For HotSpot clients to use transparent web-proxy on the same router, following configuration Can be used:
1.make sure, web-proxy software package is installed and DNS client is configured.
2.it is assumed,that HotSpot is setup and successfully running on port8088.Hotspot clients are connected to the interface named prism1
3. setup HotSpot to use one of the router's local IP addresses(10.5.50.1):
/ip hotspot set hotspot-address=10.5.50.1
4. setup web-proxy to run on the same IP address on the port 3128:
/ip web-proxy set enabled=yes src-address=10.5.50.1:3128 transparent-proxy=yes
5.configure hotspot service to use this web proxy as its parent proxy:
/ip hotspot set parent-proxy=10.5.50.1:3128

6.redirect all requests from hotspot interface to port 80(except to 10.5.50.1),to the web-proxy:
/ip firewall dst-nat add in-interface=prism1 dst-address=!10.5.50.1/32\dst-port=80 protocol=tcp action=redirect to-dst-port=8088 comment="transparent proxy"
7.Now,everythingshouldbeworkingfine.Onlytrafficoftheredirectedrequeststothe
web-proxywillnotbeaccounted.It'sbecausethistrafficwillnotpassthroughthe
forwardchain.
toenableaccountingfortheHotSpotusertrafficto/fromtransparentweb-proxy,
additionalfirewallrulesshouldbeadded:
/ipfirewallruleinputaddin-interface=prism1dst-port=3128\
protocol=tcpaction=jumpjump-target=hotspot\
comment="accounttrafficfromhotspotclienttolocalweb-proxy"
/ipfirewallruleoutputaddsrc-port=3128protocol=tcp\
out-interface=prism1action=jumpjump-target=hotspot\
comment="accounttrafficfromlocalweb-proxytohotspotclient"
You may want to allow multiple logins using the same username/password.Set the argument value of shared-users to the number of simultaneous user sessions using the same username in HotSpot profile.For example, to allow 10 clients to use the same username simultaneously:
/ip hotspot profile set default shared-users=10
If you want the router to resolve DNS requests, enable DNS cache,and redirect all the DNS requests to the router itself(159.148.60.2) is this example mean the external DNS server the router will work with):
/ip dns set primary-dns=159.148.60.2
/ip dns set allow-remote-requests=yes
/ip firewall dst-nat add protocol=udp dst-port=53 action=redirect\comment="intercept all DNS requests"

IP Pools
IP pools are used to define range of IPaddresses that is used for DHCP server and Point-to-Point servers
/ip pool
To define a pool named ip-pool with the 10.0.0.1-10.0.0.125 address range excluding gateway's address 10.0.0.1 and server'saddress 10.0.0.100,and the other pool dhcp-pool, with the 10.0.0.200-10.0.0.250 address range:
[admin@MikroTik]ip pool>add name=ip-pool ranges=10.0.0.2-10.0.0.99, 10.0.0.101,10.0.0.126
[admin@MikroTik]ip pool>add name=dhcp-pool ranges=10.0.0.200-10.0.0.250
[admin@MikroTik]ip pool>print
SOCKS Proxy Server
/ip socks
SOCKS is a proxy server that allows TCP based application data to relay across the firewall, even if The firewall would block the packets.
[admin@MikroTik]ip socks>set enabled=yes
[admin@MikroTik]ip socks>print
In the SOCKS access list you can add rules which will control access to SOCKS server. This list is Similar to firewall lists.
/ip socks connections
The Active Connection list shows all established TCP connections, which are maintained through The SOCKS proxy server.
[admin@MikroTik]ip socks connections>print
FTP service through SOCKS server

Let us consider that we have a network 192.168.0.0/24 which is masqueraded, using a router with a Public IP 10.1.0.104/24 and a private IP 192.168.0.1/24.Somewhere in the network is an FTP Server with IP address 10.5.8.8.We want to allow access to this FTP server for a client in our local Network with IP address 192.168.0.2/24.

We have already masqueraded our local network:
[admin@MikroTik]ip firewall src-nat>print

And the access to public FTP servers is denied in firewall:
[admin@MikroTik]ip firewall rule forward>print
We need to enable the SOCKS server:
[admin@MikroTik]ip socks>set enabled=yes
[admin@MikroTik]ip socks>print
Add access to a client with an IP address 192.168.0.2/32 to SOCKS access list, allow data transfer From FTP server to client (allow destination ports from 1024 to 65535 for any IP address),and Drop everything else:
[admin@MikroTik]ip socks access>add address=192.168.0.2/32 dst-port=21 action=allow
[admin@MikroTik]ip socks access>add dst-port=1024-65535 action=allow
[admin@MikroTik]ip socks access>add action=deny
[admin@MikroTik]ip socks access>print
That's all-the SOCKS server is configured. To see active connections and data transmitted and received:
[admin@MikroTik]ip socks connections>print
UPnP
The UPnP protocol is used for most of DirectX games as well as for various Windows Messenger features(remote asisstance, application sharing, file transfer, voice, video)from behind a firewall.
/ip upnp
[admin@MikroTik]ip upnp>set enable=yes
[admin@MikroTik]ip upnp>print
/ip upnp interfaces
[admin@MikroTik]ip upnp interfaces>/ip firewall src-nat print
Now all we have to do is to add interfaces and enable UPnP:
[admin@MikroTik]ip upnp interfaces>add interface=ether1 type=external
[admin@MikroTik]ip upnp interfaces>add interface=ether2 type=internal
[admin@MikroTik]ip upnp interfaces>print
[admin@MikroTik]ip upnp interfaces>enable 0,1
[admin@MikroTik]ip upnp interfaces>..set enabled=yes
[admin@MikroTik]ip upnp interfaces>
Web Proxy
/ip web-proxy
To enable the proxy on port 8080:
[admin@MikroTik]ip web-proxy>set enabled=yes src-address=0.0.0.0:8080
[admin@MikroTik]ip web-proxy>print
/ip web-proxy monitor
[admin@MikroTik]>ip web-proxy monitor
/ip web-proxy access
[admin@MikroTik]ip web-proxy access>print
To disallow download of .MP3 files and FTP connections other than from the 10.0.0.1 server:
[admin@MikroTik]ip web-proxy access>add url=\\.mp3$ action=deny
[admin@MikroTik]ip web-proxy access>add src-address=10.0.0.1/32 action=allow
[admin@MikroTik]ip web-proxy access>add url="ftp://" action=deny
[admin@MikroTik]ip web-proxy access>print
/ip web-proxy direct
/ip web-proxy cache
[admin@MikroTik]ip web-proxy cache>print
/ip web-proxy clear-cache
Web proxy will automatically detect any problems with cache and will try to solve them without loosing any cache data. But in case of a heavy damage to the file system, the web proxy can't Rebuild cache data.Cache can be deleted and new cache directories created using this feature.
[admin@MikroTik]ip web-proxy>set enabled=no
[admin@MikroTik]ip web-proxy>clear-cache
Clear all web proxy cache, yes?[y/N]:y

Transparent Mode

To enable the transparent mode, firewall rule in destination NAT has to be added, specifying which connections(to which ports)should be transparently redirected to the proxy.

For example,if we want all connections coming from ether1 interface to port 80 to be handled Transparently by web proxy, and if our web proxy is listening on port 8080,then we should add the Following destination NAT rule:

[admin@MikroTik]ip firewall dst-nat>add in-interface=ether1 protocol=tcp\dst-address=!10.0.0.1/32:80 action=redirect to-dst-port=8080

[admin@MikroTik]ip firewall dst-nat>print

Certificate Management

SSL (Secure Socket Layer) is a security technology to ensure encrypted transactions over a public network. To protect the data, an encryption key should be negotiated. SSL protocol is using Certificates to negotiate a key for data encryption.

/certificate

To import a certificate and the respective private key already uploaded on the router:

[admin@MikroTik]certificate>import

passphrase:xxxx

[admin@MikroTik]certificate>decrypt

passphrase:xxxx

[admin@MikroTik]certificate>

Now the certificate may be used by HotSpot servlet:

[admin@MikroTik]ip service>print

[admin@MikroTik]ip service>set hotspot-ssl certificate=cert1 none

[admin@MikroTik]ip service>set hotspot-ssl certificate=cert1

[admin@MikroTik]ip service>print

DDNS Update Tool

Dynamic DNS Update Tool gives a way to keep domain name pointing to dynamic IP address. It Works by sending domain name system update request to name server, which has a zone to be updated. Secure DNS updates are also supported.

The DNS update tool supports only one algorithm- hmac-md5.It's the only proposed algorithm for Signing DNS messages.

Dynamic DNS Update is a tool that should be manually run to update dynamic DNS server.

/tool dns-update

To tell 23.34.45.56 DNS server to(re)associate my domain name in the myzone.com zone with 68.42.14.4 IP address specifying that the name of the key is dns-update-key and the actual key is update:

[admin@MikroTik]tool>dns-update dns-server=23.34.45.56 name=mydomain\\...zone=myzone.com address=68.42.14.4 key-name=dns-update-key key=update

GPS Synchronization

Global Positioning System(GPS) is used for determining precise location of a GPS receiver. There Are two types of GPS service:

1. **Precise Positioning Service(PPS)**
2. **Standard Positioning Service(SPS)**

To enable GPS communication through serial 0 port:

[admin@MikroTik]system gps>print

admin@MikroTik]system gps>print

[admin@MikroTik]system gps>monitor

LCD Management

/system lcd

[admin@MikroTik]system lcd>print

To enable Crystalfontz serial LCD on serial1:

[admin@MikroTik]system lcd>set type=crystalfontz

ERROR:can't acquire requested port-already used

[admin@MikroTik]system lcd>set type=crystalfontz serial-port=serial1

[admin@MikroTik]system lcd>/port print

/system lcd page
The sub menu is used for configuring LCD information display:what pages and how long will be shown. To enable displaying all the pages:
[admin@MikroTik]system lcd page>print
To set "System date and time"page to be displayed for 10 seconds:
[admin@MikroTik]system lcd page>set 0 display-time=10s

MNDP

/ip neighbor
MNDP basic function is to assist with automatic configuration of features that are only available Between MikroTik routers.
/ip neighbor discovery
To disable MNDP protocol on Public interface:
[admin@MikroTik]ip neighbor discovery>set Public discover=no
[admin@MikroTik]ip neighbor discovery>print
To view the table of discovered neighbours:
[admin@MikroTik]ip neighbor>print

NTP(Network Time Protocol)
/system ntp
Network Time Protocol(NTP) is used to synchronize time with some NTP servers in a network.
/system ntp client
To enable the NTP client to synchronize with the 159.148.60.2 server:
[admin@MikroTik]system ntp client>set enabled=yes primary-ntp=159.148.60.2
[admin@MikroTik]system ntp client>print
/system ntp server
NTP server activities only when local NTP client is in synchronized or using-local-clock mode.
If NTP server is disabled, all NTP requests are ignored.
If NTP server is enabled, all individual time requests are answered
To enable NTP server to answer unicast requests only:
[admin@MikroTik]system ntp server>set manycast=no enabled=yes
[admin@MikroTik]system ntp server>print
/system clock
[admin@MikroTik]system clock>print
If local time is before GMT time, time-zone value will be negative. For example, if GMT is 18:00:00,but correct local time is 15:00:00,time-zone has to be set to-3hours:
[admin@MikroTik]system clock>set time-zone=-3
[admin@MikroTik]system clock>print

Router Board-specific functions
/system routerboard
To check the current and available firmware version numbers:
[admin@MikroTik]>system routerboard print
To upgrade the BIOS version:
[admin@MikroTik]>system routerboard upgrade
Firmware upgrade requires reboot of the router. Continue?[y/n]y

BIOS Configuration
/system routerboard bios
In addition to BIOS own setup possibilities, it is possible to configure BIOS parameters in RouterOS console
To set high debug level with RAM test:
[admin@MikroTik]>system routerboard bios print
[admin@MikroTik]>system routerboard bios set debug-level=high ram-test=yes
[admin@MikroTik]>system routerboard bios print

System Health Monitoring
/system routerboard health
To check system health:
[admin@MikroTik]>/system routerboard health print
To turn LED1 on for a minute:
[admin@MikroTik]>:led led1=yes length=1m
Fan voltage control
/system routerboard fan-control
Support Output File
The support file is used for debugging MikroTik RouterOS and to solve the support questions faster.
/system sup-output
To make a Support Output File:
[admin@MikroTik]>system sup-output
To see the files stored on the router:
[admin@MikroTik]>file print
System Resource Management
To view the basic system resource status:
[admin@MikroTik]>system resource print
To view the current system CPU usage and free memory:
[admin@MikroTik]>system resource monitor
IRQ Usage Monitor
IRQ usage shows which IRQ(Interrupt requests)are currently used by hardware.
/system resource irq print
[admin@MikroTik]>system resource irq print
IO Port Usage Monitor
/system resource io print
IO usage shows which IO(Input/Output)ports are currently used by hardware.
[admin@MikroTik]>system resource io print
USB Port Information
/system resource usb print
Shows all USB ports available for the router.
To list all available USB ports:
[admin@MikroTik]system resource usb>print
PCI Information
/system resource pci print
To see PCI slot details:
[admin@MikroTik]system resource pci>print

Reboot

/system reboot

The system reboot is required when upgrading or installing new software packages. The packages Are installed during the system shutdown.

[admin@MikroTik]>system reboot
Reboot,yes?[y/N]:y

/system shutdown

[admin@MikroTik]>system shutdown
Shutdown,yes?[y/N]:y

Router Identity

/system identity

To view the router identity:

[admin@MikroTik]>system identity print
name:"MikroTik"
[admin@MikroTik]>

To set the router identity:

[admin@MikroTik]>system identity set name=Gateway
[admin@Gateway]>

Date and Time

/system clock

To view the current date and time settings:

[admin@Gateway]system clock>print

To set the system date and time:

[admin@Gateway]system clock>set date=dec/31/2022 time=12:11:32 time-zone=+0
[admin@Gateway]system clock>print

Configuration Change History

/system history,/undo,/redo

To show the list of configuration changes:

[admin@MikroTik]system history>print

Bandwidth Test

Server Configuration

/tool bandwidth-server

[admin@MikroTik]tool bandwidth-server>print
[admin@MikroTik]tool>bandwidth-server session print

To enable bandwidth-test server without client authentication:

[admin@MikroTik]tool bandwidth-server>set enabled=yes authenticate=no
[admin@MikroTik]tool bandwidth-server>print

Client Configuration

/tool bandwidth-test

To run 15-second long bandwidth-test to the 10.0.0.211 host sending and receiving 1000-byte UDP Packets and using username=admin to connect

[admin@MikroTik]tool>bandwidth-test 10.0.0.211 duration=15s direction=both\\...size=1000 protocol=udp user=admin

ICMP Bandwidth Test

The ICMP test uses two standard echo-requests per second. The time between these pings can be changed….
In the following example we will test the bandwidth to a host with IPaddress 159.148.60.2.The interval between repetitions will be 1 second.

[admin@MikroTik]tool>ping-speed 159.148.60.2 interval=1s

Packet Sniffer
It allows you to"sniff" packets going through the router (and any other traffic that gets to the router, When there is no switching in the network) and view them using specific software.
/tool sniffer
In the following example streaming-server will be added, streaming will be enabled, file-name Will be set to test and packet sniffer will be started and stopped after sometime:
[admin@MikroTik]tool sniffer>set streaming-server=10.0.0.241\\...streaming-enabled=yes file-name=test

Running Packet Sniffer
/tool sniffer start,/tool sniffer stop,/tool sniffer save
The commands are used to control runtime operation of the packet sniffer
admin@MikroTik]tool sniffer>start
[admin@MikroTik]tool sniffer>stop
Below the sniffed packets will be saved in the file named test:
[admin@MikroTik]tool sniffer>save file-name=test
[admin@MikroTik]tool sniffer>/file print
/tool sniffer packet
[admin@MikroTik]tool sniffer packet>print
Packet Sniffer Protocols
/tool sniffer protocol
[admin@MikroTik]tool sniffer protocol>print
Packet Sniffer Host
/tool sniffer host
Shows the list of hosts that were participating in data exchange you've sniffed.
[admin@MikroTik]tool sniffer host>print

Packet Sniffer Connections
/tool sniffer connection
Here you can get a list of the connections that have been watched during the sniffing time. The example show to get the list of connections:
[admin@MikroTik]tool sniffer connection>print

Sniff MAC Address
You can also see the source and destination MAC Addresses. To do so, at first stop the sniffer if it Is running, and select a specific interface:
[admin@MikroTik]tool sniffer>stop
[admin@MikroTik]tool sniffer>set interface=bridge1
[admin@MikroTik]tool sniffer>start
[admin@MikroTik]tool sniffer>print
Now you have the source and destination MAC Addresses:
[admin@MikroTik]tool sniffer packet>print detail

Ping
/tool mac-server ping
Ping uses Internet Control Message Protocol(ICMP)Echo messages to determine if a remote host Is active or inactive and to determine the round-trip delay when communicating with it. Ping sends ICMP echo (ICMP type 8) message to the host and waits for the ICMP echo-reply (ICMP type 0)from that host.
/ping
[admin@MikroTik]>ping 159.148.60.2 count=5 interval=40 ms size=64

MAC Ping Server
/tool mac-server ping
To disable MAC pings:
[admin@MikroTik]tool mac-server ping>set enabled=no
[admin@MikroTik]tool mac-server ping>print

Torch(Real timeTraffic Monitor)
Real timeTraffic Monitor called also torch is used for monitoring traffic that is going through an interface.
/tool torch
The following example monitors the traffic that goes through the ether1 interface generated by telnet protocol:
[admin@MikroTik]tool>torch ether 1 port=telnet
To see what IP protocols are going through the ether 1 interface:
[admin@MikroTik]tool>torch ether1 protocol=any-ip
To see what IP protocols are interacting with 10.0.0.144/32 host connected to the ether1 interface:
[admin@MikroTik]tool>torch ether1 src-address=10.0.0.144/32 protocol=any
To see what tcp/udp protocols are going through the ether1 interface:
[admin@MikroTik]tool>torch ether1 protocol=any-ip port=any

Traceroute

/tool traceroute
Traceroute is a TCP/IP protocol-based utility, which allows user to determine how packets are Being routed to a particular host.
To trace the route to 216.239.39.101 host using ICMP protocol with packet size of 64 bytes, setting ToS field to 8 and extending the timeout to 4 seconds:
[admin@MikroTik]tool>traceroute 216.239.39.101 protocol=icm psize=64 tos=8 timeout=4s

Scripting Host and Complementary Tools

In the example below monitor action will execute given script each time it prints stats on the screen, and it will assign all printed values to local variables with the same name:
[admin@MikroTik]interface>monitor-traffic ether2 once do={:environment print}

/system script

The following example is a script for writing message"Hello World!"to the system log:

[admin@MikroTik]system script>add name=log-test source={:log\\...message="Hello World!"}
[admin@MikroTik]system script>print

/system script job

This facility is used to manage the active or scheduled tasks
[admin@MikroTik]system script>job print
[admin@MikroTik]system script>job remove0
[admin@MikroTik]system script>job print

/system script edit
RouterOS console has a simple full-screen editor for scripts with support for multiline script writing.

System Scheduler

/system scheduler
We will add a task that executes the script log-test every hour:
[admin@MikroTik]system script>add name=log-test source=:log message=test
[admin@MikroTik]system script>print
[admin@MikroTik]system script>..scheduler
[admin@MikroTik]system scheduler>add name=run-1h interval=1h on-event=log-test
[admin@MikroTik]system scheduler>print

In another example there will be two scripts added that will change the bandwidth setting of a queue rule"Cust0".Everyday at 9AM the queue will be set to 64Kb/s and at 5PM the queue will be set to 128Kb/s. The queue rule,the scripts,and the scheduler tasks are below:

[admin@MikroTik]queue simple>add name=Cust0 interface=ether1\\...dst-address=192.168.0.0/24 limit-at=64000
[admin@MikroTik]queue simple>print
[admin@MikroTik]queue simple>/system script
[admin@MikroTik]system script>add name=start_limit source={/queue simple set\\...Cust0 limit-at=646000}
[admin@MikroTik]system script>add name=stop_limit source={/queue simple set\\...Cust0 limit-at=128000}
[admin@MikroTik]system script>print
[admin@MikroTik]system script>..scheduler
[admin@MikroTik]system scheduler>add interval=24h name="set-64k"\\...start-time=9:00:00on-event=start_limit
[admin@MikroTik]system scheduler>add interval=24h name="set-128k"\\...start-time=17:00:00 on-event=stop_limit
[admin@MikroTik]system scheduler>print

The following example schedules a script that sends each week a backup of router configuration by e-mail.

[admin@MikroTik]system script>add name=e-backup source={/system backup {...save name=email;/tool e-mail send to="root@host.com"subject=([/system{...identity get name]."Backup")file=email.backup}
[admin@MikroTik]system script>print
[admin@MikroTik]system script>..scheduler
[admin@MikroTik]system scheduler>add interval=7d name="email-backup"\\...on-event=e-backup
[admin@MikroTik]system scheduler>print

Do not forget to set the e-mail settings, i.e., the SMTP server and From:address under /tool e-mail.
For example:

[admin@MikroTik]toole-mail>set server=159.148.147.198 from=SysAdmin@host.com
[admin@MikroTik]tool e-mail>print

Example below will put 'x' in logs each hour from midnight til lnoon:

[admin@MikroTik]system script>add name=enable-x source={/system scheduler{...enable x}
[admin@MikroTik]system script>add name=disable-x source={/system scheduler{...disable x}
[admin@MikroTik]system script>add name=log-x source={:log message=x}
[admin@MikroTik]system script>..scheduler
[admin@MikroTik]system scheduler>add name=x-up start-time=00:00:00\\...interval=24h on-event=enable-x
[admin@MikroTik]systemscheduler>add name=x-down start-time=12:00:00\...interval=24h on-event=disable-x
[admin@MikroTik]system scheduler>add name=x start-time=00:00:00 interval=1h\\...on-event=log-x
[admin@MikroTik]system scheduler>print

Network Watching Tool
/tool netwatch

Netwatch monitors state of hosts on the network.It does so by sending ICMP pings to the list of specified IP addresses. For each entry in netwatch table you can specify IP address, ping interval and console scripts. The main advantage of netwatch is it's ability to issue arbitrary console commands on host state changes.

This example will run the scripts gw_1 or gw_2 which change the default gateway depending on the status of one of the gateways:

[admin@MikroTik]system script>add name=gw_1 source={/ip route set{...[/ip route find dst 0.0.0.0] gateway 10.0.0.1}
[admin@MikroTik]system script>add name=gw_2 source={/ip route set{..[/ip route find dst 0.0.0.0] gateway 10.0.0.217}
[admin@MikroTik]system script>/tool netwatch
[admin@MikroTik]tool netwatch>add host=10.0.0.217 interval=10s timeout=998ms\\...up-script=gw_2 down script=gw_1
[admin@MikroTik]tool netwatch>print

Thescript"gw_2" is executed once when status of host becomes down. It does the following:
[admin@MikroTik]>/ip route set[/ip route find dst 0.0.0.0] gateway 10.0.0.217
Thescript"gw_1"is executed once when status of host becomes down. It does the following:
[admin@MikroTik]>/ip route set[/ip route find dst 0.0.0.0] gateway 10.0.0.1

Here is another example,that sends e-mail notification whenever the 10.0.0.215 host goes down:

[admin@MikroTik]system script>add name=e-down source={/tool e-mail send {...from=”rieks@mt.lv “server="159.148.147.198" body="Router down"{...subject="Router at second floor is down" to="rieks@latnet.lv"}
[admin@MikroTik]system script>add name=e-up source={/tool e-mail send {...from=”rieks@mt.lv “server="159.148.147.198" body="Routerup"{..subject="Router at second floor is up"to="rieks@latnet.lv"}
[admin@MikroTik]system script>
[admin@MikroTik]system script>/tool netwatch
[admin@MikroTik]system netwatch>add host=10.0.0.215 timeout=999ms\\...interval=20s up-script=e-up down-script=e-down
[admin@MikroTik]toolnetwatch>print detail

Traffic Monitor
/tool traffic-monitor
The traffic monitor tool is used to execute console scripts when interface traffic crosses a given threshold.

In this example the traffic monitor enables the interface ether2,if the received traffic exceeds 15kbps on ether1, and disables the interface ether2,if the received traffic falls below 12kbps on ether1.

[admin@MikroTik]system script>add name=eth-up source={/interface enable ether2}
[admin@MikroTik]system script>add name=eth-down source={/interface disable{...ether2}
[admin@MikroTik]system script>/tool traffic-monitor
[admin@MikroTik]tool traffic-monitor>add name=turn_on interface=ether1\\...on-event=eth-up threshold=15000 trigger=above traffic=received
[admin@MikroTik]tool traffic-monitor>add name=turn_off interface=ether1\\...on-event=eth-down threshold=12000 trigger=below traffic=received
[admin@MikroTik]tooltraffic-monitor>print

Sigwatch
/tool sigwatch
Sigwatch canbe used to monitor the state of serial port pins.
In the following example we will add a new sigwatch item that monitors whether the port serial1 Has cts signal.
[admin@10.179]tool sigwatch>print

By typing a command print detail interval=1s,we can check whether a cable is connected or it is not. See the state argument-if the cable is connected to the serial port, its hows on, otherwise it will be off.
[admin@MikroTik]tool sigwatch>print detail

In the port menu you can see what signal is used by serial cable. For example, without any cables it looks like this:
[admin@MikroTik]port>print stats _____**{Got cts}**

This means that the line-state besides the dtr and rts signals has also cts when a serial cable is connected.

IPTelephony

/ip telephony
IP telephony,known as Voice over IP(VoIP),is the transmission of telephone calls over a data network like one of the many networks that make up the Internet. There are four ways that you might talk to someone using VoIP:
C TO C | C TO P | P TO C | P TO P
/ip telephony voice-port
/ip telephony numbers
/ip telephony voice-port voice tronix
/ip telephony voice-port phone jack
/ip telephony voice-port zaptel
/ip telephony voice-port isdn
/ip telephony voice-port voip
The voip voice ports are virtual ports,which designate a voip channel to another host over the IP network. You must have at least one voip voice port to be able to make calls to other H.323 devices over IP network.

[admin@MikroTik]ip telephony numbers>print.

/ip telephony region
Regional settings are used to adjust the voice port properties to the PSTN system or the PBX

/ip telephony codec
CODECs are listed according to their priority of use.The highest priority is at the top
[admin@MikroTik]ip telephony codec>print

/ip telephony aaa
AAA(Authentication Authorization Accounting)can be used to configure the RADIUS accounting feature.

/ip telephony gatekeeper

For each H.323 endpoint gatekeeper stores its telephone numbers. So, gatekeeper knows all telephone numbers for all registered endpoints. And it knows which telephone number is handled by which endpoint. Mapping between endpoints and their telephone numbers is the main functionality of gatekeepers.

In most simple case with one phone jackcard and some remote gatekeeper, configuration can be as follows:
[admin@MikroTik]ip telephony voice-port>print
[admin@MikroTik]ip telephony numbers>print
[admin@MikroTik]ip telephony gatekeeper>print

For example,if numbers table is like this:
[admin@MikroTik]ip telephony numbers>print

If IP address of local endpoint is 10.0.0.100,then gatekeeper voip and numbers tables will look as follows:
[admin@MikroTik]ip telephony voice-port voip>print
[admin@MikroTik]ip telephony numbers>print

- **Setting up the MikroTik IP Telephone**

If you pick up the handset,a dialtone should be heard.
The basic telephony configuration should be as follows:
Add a voip voice port to the /ip telephony voice-port voip for each of the devices you want to call, or want to receive calls from, i.e.,(the IP telephony gateway 10.1.1.12 and the Well tech IP telephone 10.5.8.2):
[admin@Joe]ip telephony voice-port voip>add name=gw remote-address=10.1.1.12
[admin@Joe]ip telephony voice-port voip>add name=rob remote-address=10.5.8.2
[admin@Joe]ip telephony voice-port voip>print
You should have three voice ports now:
[admin@Joe]ip telephony voice-port>print
Add at least one unique number to the /ip telephony numbers for each voice port. This number will be used to call that port:
[admin@Joe]ip telephony numbers>add dst-pattern=31 voice-port=rob
[admin@Joe]ip telephony numbers>add dst-pattern=33 voice-port=linejack1
[admin@Joe]ip telephony numbers>add dst-pattern=1.voice-port=gw prefix=1
[admin@Joe]ip telephony numbers>print
[admin@Joe]ip telephony numbers>

Here,the dst-pattern=31 is to call the Welltech IP Telephone,if the number 31 is dialed on the dial pad. The dst-pattern=33 is to ring the local telephone, if a call for number 33 is received over the network. Anything starting with digit '1' would be sent over to the IP Telephony gateway.

Making calls from the IP telephone 10.0.0.224:
•To call the IP telephone 10.5.8.2, it is enough to lift the handset and dial the number 31
•To call the PBX extension 13, it is enough to lift the handset and dial the number 13

After establishing the connection with 13, the voice port monitor shows:
[admin@Joe]ip telephony voice-port linejack>monitor linejack status : connection port: phone direction: port-to-ip line-status: unplugged phone-number:13 remote-party-name: PBX_Line [10.1.1.12] codec:G.723.1-6.3k/hw duration:16s
[admin@Joe]ip telephony voice-port linejack>

- **Setting up the IP Telephony Gateway**

Set the regional setting to match our PBX. The mikrotik region will be used in thisn example:
[admin@voip_gw]ip telephony voice-port linejack>set linejack1 region=mikrotik
[admin@voip_gw]ip telephony voice-port linejack>print

Add a voip voice port to the /ip telephony voice-port voip for each of the devices you want to call, or want to receive calls from,i.e.,(the IP telephone 10.0.0.224 and the Welltech IP telephone 10.5.8.2):
[admin@voip_gw]ip telephony voice-port voip>add name=joe\\...remote-address=10.0.0.224
[admin@voip_gw]ip telephony voice-port voip>add name=rob\\...remote-address=10.5.8.2 prefered-codec=G.723.1-6.3k/hw
[admin@voip_gw]ip telephony voice-port voip>print

Add number records to the /ip telephony numbers,so you are able to make calls:
[admin@voip_gw]ip telephony numbers>add dst-pattern=31 voice-port=rob prefix=31
[admin@voip_gw]ip telephony numbers>add dst-pattern=33 voice-port=joe prefix=33
[admin@voip_gw]ip telephony numbers>add dst-pattern=1. voice-port=linejack1\\...prefix=1
[admin@voip_gw]ip telephony numbers>print

Making calls through the IP telephony gateway:

To dial the IP telephone 10.0.0.224 from the office PBX line, the extension number 19 should be dialed,and,after the dial tone has been received,the number 33 should be entered. Thus, the telephone[Joe] is ringed. After establishing the voice connection with '33' (the call has been answered),the voice port monitor shows:
[admin@voip_gw]ip telephony voice-port linejack>monitor linejack1 status:connection port:line direction:port-to-ip line-status:plugged phone-number:33 remote-party-name:linejack1 [10.0.0.224] codec:G.723.1-6.3k/hw duration:1m46s
[admin@voip_gw]ip telephony voice-port linejack>
To dial the IP telephone 10.5.8.2 from the office PBX line, the extension number 19 should be dialed, and, after the dial tone has been received, the number 31 should be entered

- **Setting up the Welltech IP Telephone**

Please follow the documentation from www.welltech.com.tw on how to setup the Welltech LAN Phone101.Here we give just brief recommendations:

1. **We recommend to upgrade the Welltech LAN Phone 101 with the latest application software.Telnet to the phone and check what you have, for example:**

   usr/config$ rom-print
   ---
   usr/config$

2. **Check if you have the codecs arranged in the desired order:**
   usr/config$ voice-print
   Voice codec setting relate information
   ---
   usr/config$
3. **MakesureyouhavesettheH.323operationmodetophonetophone(P2P),notgatekeeper (GK):**
   usr/config$ h323-print
   H.323 stack relate information
   ---
   usr/config$

4. **Add the gateway's address to the phonebook:**
   usr/config$ pbook-add name gw ip 10.1.1.12
   usr/config$
   ---
   usr/config$ pbook-print
   usr/config$
   add a phonebook record for it:
   usr/config$ pbook-add name Joe ip 10.0.0.224 e164 33

Setting up MikroTik Router and CISCO Router

- **Configuration on the MikroTik side**

•G.729a codec MUST be disabled(otherwise connections are not possible at all!!!)
/ip telephony codec disable G.729A-8k/sw
•G.711-ALaw codec should not be used (in some cases there is no sound)
/ip telephony code cdisable"G.711-ALaw-64k/sw G.711-ALaw-64k/hw"
•Fast start has to be used(otherwise no ring-back tone and problems with codec negotiation)
/ip telephony voice-port set cisco fast-start=yes
•Telephone number we want to call to must be sent to Cisco,for example
/ip telephony numbers add destination-pattern=101 voice-port=cisco prefix=101
•Telephone number,cisco will call us,must be assigned to some voice port, for example,
/ip telephony numbers add destination-pattern=098 voice-port=linejack

- **Configuration on the CISCO side:**

IP routing has to be enabled
Ip routing
Default values for fast start can be used:
Voice service pots default h323 call start exit voice service voip default h323 call start exit
Enable opening of RTP streams:
Voice rtp send-recv
Assign some E.164 number for local telephone,for example, 101 to port 0/0
dial-peer voice1 pots destination-pattern 101 port 0/0 exit
create preferred codec listing:
voice class codec codec_class_number codec preference 1 g711ulaw codec preference 2 g723r63 exit
Tell,that some foreign E.164 telephone number canbe reached by calling to some IP address, for example,098 by calling to 10.0.0.98
dial-peer voice11 voip destination-pattern 098 session target ipv4:10.0.0.98
voice-class codec codec_class_number exit
NOTE: instead of codec class,one specified codec could be specified:
Codec g711ulaw

- **Setting up PBX to PBX Connection over an IP Network**

To inter connect two telephone switch boards(PBX) over an IP network, two IP telephony gateways should be configured. The setup is shown in the following diagram:
We want to be able to use make calls from local telephones of one PBX to local telephones or external lines of the other PBX.
Assume that:
•The IP telephony gateway#1 has IP address 10.0.0.182, and the name of the Voicetronix first line is'vctx1'.
•The IP telephony gateway#2 has IP address 10.0.0.183, and the name of the Voicetronix first line is'vctx1'.

The IP telephony configuration should be as follows:

IP telephony gateway#1 should have:
/ip telephony voice-port voip add name=gw2 remote-address=10.0.0.183
/ip telephony numbers add dst-pattern=1..voice-port=gw2 prefix=2 add dst-pattern=2..voice-port=vctx1 prefix=1
IP telephony gateway#2 should have
/ip telephony voice-port voip add name=gw1 remote-address=10.0.0.182
/ip telephony numbers add dst-pattern=2..voice-port=vctx1 prefix=1 adddst-pattern=1..voice-port=gw1 prefix=2

The system works as follows:

To dial from the main office PBX#1 any extension of the remote office PBX#2,the extension with the connected gateway at PBX#1 should be dialed first. Then, after the dial tone of the gateway#1 is received, the remote extension number should be dialed.

To dial from the main officePBX#2 any extension of the remote officePBX#1, the actions are the same as in first situation

System Watchdog

System watchdog feature is needed to reboot the system in case of software failures.
/system watchdog

This menu allows to configure system to reboot on kernel panic, when an IP address does not respond, or in case the system has locked up.Software watchdog timer is used to provide the last option, so in very rare cases(caused by hardware malfunction)it can lockup by itself .There is a hardware watchdog device available in RouterBOARD hardware,which can reboot the system in anycase.

To make system reboot in case of any software failure:
[admin@MikroTik]system watchdog>set reboot-on-failure=yes watchdog-timer=yes
[admin@MikroTik]system watchdog>print

UPS Monitor
/system ups
In order to enable UPS monitor, the serial port should be available
To enable the UPS monitor for port serial1:
[admin@MikroTik]system ups>set port=serial1 enabled=yes
[admin@MikroTik]system ups>print
/system ups run-time-calibration
The run-time-calibration command causes the UPS to start a runtime calibration until less than 25% of full battery capacity is reached. This command calibrates the returned runtime value.
[MikroTik]system ups>run-time-calibration
/system ups monitor
[admin@MikroTik]system ups>monitor

VRRP
/ip vrrp
Virtual Router Redundancy Protocol is an election protocol that provides high availability for Routers .A number of routers may participate in one or more virtual routers. One or more IP addresses may be assigned to a virtual router. A node of a virtual router can be in one of the following states:
MASTER state.
BACKUP state

To add a VRRP instance on ether1 interface, forming(because priority is 255)a virtual router with vrid of 1:
[admin@MikroTik]ip vrrp>add interface=ether1 vrid=1 priority=255
[admin@MikroTik]ip vrrp>print

Virtual IP addresses

/ip vrrp address
The virtual IP addresses should be the same for each node of a virtual router.
To add a virtual address of 192.168.1.1/24 to the vr1 VRRP router:
[admin@MikroTik]ip vrrp>address add address=192.168.1.1/24\\...virtual-router=vr1
[admin@MikroTik]ip vrrp>address print

VRRP protocol may be used to make a redundant Internet connection with seamless fail-over.
First of all we should create a VRRP instance on this router.We will use the priority of 255 for this router as it should be preferred router.
[admin@MikroTik]ip vrrp>add interface=local priority=255
[admin@MikroTik]ip vrrp>print

Next the virtual IP address should be added to this VRRP instance
[admin@MikroTik]ip vrrp>address add address=192.168.1.1/24\\...virtual-router=vr1
[admin@MikroTik]ip vrrp>address print
Now this address should appear in /ip address list:
[admin@MikroTik]ip address>print

Configuring Backup VRRP router

Now we will create VRRP instance with lower priority(we can use the default value of 100),so this router will backup the preferred one:
[admin@MikroTik]ip vrrp>add interface=local
[admin@MikroTik]ip vrrp>print
Now we should add the same virtual address as was added to the master node:
[admin@MikroTik]ip vrrp>address add address=192.168.1.1/24\\...virtual-router=vr1
[admin@MikroTik]ip vrrp>address print
Note that this address will not appear in /ip address list:
[admin@MikroTik]ip address>print

Testing failover

Now, when we will disconnect the master router, the backup one will switch to the master state:
[admin@MikroTik]ip vrrp>print