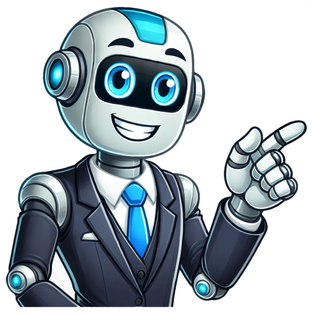
Click Here



Author Patrick Creation date Jan 5, 2016 Share — copy and redistribute the material in any medium or format for any purpose, even commercially. Adapt — remix, transform, and build upon the material for any purpose, even commercially. The licensor cannot revoke these freedoms as long as you follow the license terms. Attribution — You must give appropriate credit , provide a link to the license, and indicate if changes were made . You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use. ShareAlike — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original. No additional restrictions — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits. You do not have to comply with the license for elements of the material in the public domain or where your use is permitted by an applicable exception or limitation . No warranties are given. The license may not give you all of the permissions necessary for your intended use. For example, other rights such as publicity, privacy, or moral rights may limit how you use the material. To get access to any of MikroTik routers you need to know an IP address of the router and credentials, i.e. a username and password. All the MikroTik routers are pre-configured with the default IP address as well as with the default username and password. Cool Tip: Simple MikroTik WiFi configuration! Read more → MikroTik Default IP, Login & Password Every MikroTik router is factory pre-configured with the IP address 192.168.88.1/24. The default MikroTik username is admin. The default MikroTik password is empty (not set). MikroTik Defaults IP 192.168.88.1 Login admin Password none Check the sticker! For some models of MikroTik routers the default login and password, as well as the default WiFi password can be found on a sticker placed on the rear or underside of the device. It is also worth pointing out that on some of the routers, like MikroTik hAP AX³, for example, the sticker with the default network details is placed on a hidden tab on the rear of the device: ⚠ Factory Reset: If you keep getting “Authentication failed: invalid username or password“, you can try to reset your device. Connect to MikroTik Router To access a management interface of the MikroTik router, open your web browser and enter the IP 192.168.88.1. Alternatively, you can connect to your device using a WinBox (a free utility tool developed by MikroTik). With the WinBox you can also auto-discover and connect to your MikroTik router by a MAC address (if the router and your computer are on the same LAN): To connect to the MikroTik router using SSH, execute the following command from a Linux/MacOS terminal or a Windows command prompt (CMD) or PowerShell: $ ssh admin@192.168.88.1 - sample output - MMM MMM KKK TTTTTTTTTTT KKK MMMM MMMM KKK TTTTTTTTTTT KKK MMM MMMM MMM III KKK KKK RRRRRR OOOOOO TTT III KKK KKK MMM MM MMM III KKKKK RRR RRR OOO OOO TTT III KKKKK MMM MMM III KKK KKK RRRRRR OOO OOO TTT III KKK KKK MMM MMM III KKK KKK RRR RRR OOOOOO TTT III KKK KKK MikroTik RouterOS 6.47.9 (c) 1999-2020 [?] Gives the list of available commands command [?] Gives help on the command and list of arguments [Tab] Completes the command/word. If the input is ambiguous, a second [Tab] gives possible options / Move up to base level .. Move up one level /command Use command at the base level [admin@MikroTik] > Was it useful? Share this post with the world! Well I noticed this on the Routerboard.com site today: RouterBoard.com : CSS326-24G-2S+RM Great price for a basic L2 24 port GigE + 2x 10Gb SFP+ switch that'll handle simple functions. If you aren't doing any L3 or LACP this should be a great low power option. I use their RB260GS (also runs SwOS) for fiber links and/or port expansion when the customer doesn't require any special features. Never had a problem with them at all. Thought it was a typo at first. Was thinking the CRS226 has been around a long time but this CRS326 is a super reasonable price for those that need the basics with a pair of SFP+ cages. Don't see it for sale anywhere yet but I am sure it will find it's way to stores. Reactions: Patrick Streakwave has these available now. Got one delivered last week and configured it over the weekend. Seems functional. Normal "Mikrotik" build quality - metal box, but seems thin, etc. Came with rack ears and PSU. Couldn't power it via PoE from "standard" PoE switch - I think its proprietary, not "af". SwOS web management is basic (really basic...). STP seems to be broken (or it could be broken on the Ubiquiti it was connected to). STP was "blocking" everything but traffic to the switch itself. Disabled STP on all ports and now its happy. Would be nice to have STP, but not really necessary for me. With both 10Gbe active with SR optics and 15 of 24 ports connected it draws 12.2w. Running cool, no noticeable heat, no fans so dead silent (which was the main driver for getting it). BTW - there is no setting for it in the web gui, but it does appear to support jumbo frames. Passes them just fine, at least up to 9k, which is all I tested. SNMP is v1 only, which makes it a PITA to set up with Zabbix since all of the current templates are V2 or V3. Reactions: Patrick Mine turned up today, just a couple of notes on SFP compatibility, as that's a common request. CCS -> Other end Cisco SFP-10G-SR 10GBASE-SR SFP+ Transceiver | FS.COM (10G Multimode) -> Mellanox connectx 2 with Cisco SFP-10G-SR 10GBASE-SR SFP+ Transceiver | FS.COM - works. Cisco Linksys MGBBX1 1000BASE-BX-U SFP Transceiver | FS.COM (1G Bidi) -> Mikrotik RB2011 with Cisco 1000BASE-BX SFP 1490nm-TX/1310nm-RX 20km | FS.COM - needs more investigation. It's showing up in the SFP tab of the CCS, but just not showing link up - so there is some hope there. When I've got a bit more time, I'll test with a couple of other options, but at the price point, it seems ideal for a small home lab (ie, 2 nodes, or desktop + server where you want 10G between those two, and 1G to the rest of the network. Other notes - the port layout appears naff compared to what I've seen in the past. Port 1 is bottom left, port 2 is top left (I expected port 1 to be top left, a minor point I know, but not what I was expecting). Mine finally showed up today. I had forgotten about it. At least something to do outside of CPU reviews. I wish they had something with 10g or four SFP+ port Sent from my Pixel XL using Tapatalk Is that picture correct? The picture on the site is the 317 I think... I'm looking at getting one of those. I'd love to see an 8 to 10 port 10g in the 200 to 300 range .... Sent from my Pixel XL using Tapatalk I've got something similar to this - I use it as an access switch for 1GB connectivity with 10GB uplink to TOR switch. I tend not to go near it because frankly compared to other switches / network devices I have got (Gnodal / HP / Dlink / Cisco) its UI is as wierd as f********k!! Wish they'd make the OS more inline with other devices (or is it just me?!) Nice. What's the price on the 317?... I only need like 4 ports... Basically the crs106 I'm SFP+ Sent from my Pixel XL using Tapatalk SwOS 2.1 is now available on the Mikrotik download page. There's no changelog, but now there's a LAG tab in the GUI with options for passive/active/static per port. Edit: Also appears to support SNMPv2 and 64-bit counters. Last edited: Apr 19, 2017 Reactions: PigLover SwOS Changelog 2.2 is now updated. Someone had a chance to test LACP in CSS326 to see how it actually performs? Baltic now has this switch (CSS326-24G-2S+RM) on sale for $120. Amazing how prices are falling! thx mike So far I am very satisfied with mine. Basic, but all I needed was low power, fanless and a couple of SFP+. It's perfect. Sent from my SM-G950U using Tapatalk Connecting to the RouterThere are two types of routers:Routers with default configuration.Routers without default configuration. In cases where no specific configuration is present, the IP address 192.168.88.1/24 is assigned to ether1, combo1, sfp1, or MGMT/BOOT.For additional details regarding the current default configuration, please refer to the Quick Guide document provided with your device. This document outlines which ports to initially utilize for connection and instructions on device setup.This document describes the step-by-step process for configuring the device from scratch. Therefore, we recommend clearing all defaults when initiating the setup.When connecting the first time to the router with the default username admin and no password (or, for some models, check user and wireless passwords on the sticker). Upon the initial boot, a notification will appear, offering you the choice to either remove the default configuration (even if the default config has only an IP address), leading to a reboot with no configuration applied, or to "Show Script" and retain the current default configuration, applying it accordingly. Since this article assumes that there is no configuration on the router, you should remove it by pressing "r" on the keyboard when prompted or click on the "Remove Configuration" button in WinBox.Router without Default ConfigurationIf the router doesn't have a default configuration, there are multiple options to consider. However, in this case, we'll opt for a method that best fits our requirements.Connect the ISP cable to the router's ether1 port and connect your PC to any port except ether1. Then, launch WinBox and search for your router using the neighbor discovery feature. See detailed example in Winbox article.If the router appears in the list, select its MAC address and click Connect.The easiest method to ensure a completely clean router is to run the CLI command /system reset-configuration no-defaults=yes skip-backup=yes Or from WinBox:Configuring IP AccessAs MAC connection can sometimes be unreliable, our first step is to configure the router to enable IP connectivity:Create a bridge interface and assign bridge ports;Assign an IP address to the bridge interface;Configure a DHCP server.Setting up the bridge and assigning an IP address are straightforward processes: /interface bridge add name=bridge1 /interface bridge port add interface=ether2 bridge=bridge1 /ip address add address=192.168.88.1/24 interface=bridge1 If you prefer WinBox/WebFig as configuration tools:Open Bridge window, Bridge tab should be selected;Click on the + button to open a new dialog box. You can either enter a custom bridge name or retain the default bridge1, then click OK to proceed;Switch to the Ports tab and click on the + button to open another dialog box;Select interface ether2 and bridge bridge1 form drop-down lists and click on the OK button to apply settings;You may close the bridge dialog.Access the IP menu and navigate to the Addresses dialog;Select the + button to open a new dialog box;Enter IP address 192.168.88.1/24 select interface bridge1 from the drop-down list;Click OK to confirm the settings.Next, proceed with setting up a DHCP server. To simplify and expedite this process, we'll execute the setup command. [admin@MikroTik] > ip dhcp-server/ setup [enter] Select interface to run DHCP server on dhcp server interface: bridge1 [enter] Select network for DHCP addresses dhcp address space: 192.168.88.0/24 [enter] Select gateway for given network gateway for dhcp network: 192.168.88.1 [enter] Select pool of ip addresses given out by DHCP server addresses to give out: 192.168.88.2-192.168.88.254 [enter] Select DNS servers dns servers: 192.168.88.1 [enter]

Select lease time lease time: 1800 [enter] Notice that most of the configuration options are automatically determined and you just simply need to hit the enter key.The setup tool is also accessible in WinBox/WebFig:Navigate to IP -> DHCP Server window, ensuring the DHCP tab is selected;Click on the DHCP Setup button to open a new dialog;Select the bridge1 as the DHCP Server Interface and click Next;Follow the wizard to complete the setup.Following these steps, the connected PC should now obtain a dynamic IP address. You can then close Winbox and reconnect to the router using the IP address (192.168.88.1).Configuring Internet ConnectionTo enable internet access for the router, you'll need to configure one of the following common types of internet connections:Dynamic public IP address.Static public IP address.PPPoE connection.Dynamic Public IPDynamic address configuration is the easiest option. Simply set up a DHCP client on the public interface. The DHCP client will obtain information from your Internet Service Provider (ISP), such as an IP address, DNS servers, NTP servers, and default route, making the setup process straightforward for you. /ip dhcp-client add disabled=no interface=ether1 After adding the client you should see the assigned address and status should be bound [admin@MikroTik] > ip dhcp-client print Columns: INTERFACE, USE-PEER-DNS, ADD-DEFAULT-ROUTE, STATUS, ADDRESS # INTERFACE USE-PEER-DNS ADD-DEFAULT-ROUTE STATUS ADDRESS 0 ether1 yes yes bound 1.2.3.100/24 Static Public IPWhen configuring a static address, your ISP provides specific parameters, such as:IP: 1.2.3.100/24Gateway: 1.2.3.1DNS: 8.8.8.8These are three basic parameters that you need to get the internet connection working.To configure this in RouterOS, we'll manually add an IP address, add a default route with a provided gateway, and set up a DNS server /ip address add address=1.2.3.100/24 interface=ether1 /ip route add gateway=1.2.3.1 /ip dns set servers=8.8.8.8 PPPoE ConnectionPPPoE connection also gives you a dynamic IP address and can configure dynamically DNS and default gateway. Typically service provider (ISP) gives you a username and password for the connection /interface pppoe-client add disabled=no interface=ether1 user=me password=123 \ add-default-route=yes use-peer-dns=yes Winbox/WebFig actions:In the PPP window, select the Interfaces tab and click the "+" button;Choose PPPoE Client from the dropdown list;Set the name and select ether1 as the interface;Go to the Dial Out tab, configure the username, password, and other parameters;Click OK to save the settings.Verify ConnectivityOnce the configuration is complete, you should be able to access the internet from the router. To verify IP connectivity, try pinging a known IP address, such as a Google DNS server. [admin@MikroTik] > /ping 8.8.8.8 SEQ HOST SIZE TTL TIME STATUS 0 8.8.8.8 56 55 14ms399us 1 8.8.8.8 56 55 18ms534us 2 8.8.8.8 56 55 14ms384us Verify DNS request [admin@MikroTik] > /ping google.com SEQ HOST SIZE TTL TIME STATUS 0 142.250.74.14 56 55 14ms475us 1 142.250.74.14 56 55 14ms308us 2 142.250.74.14 56 55 14ms238us If all settings are configured correctly, both pings should succeed. If there's a failure, please refer to the Troubleshooting section for assistance.Protecting the RouterAs the router is now accessible worldwide, it's important to protect it from potential intruders and basic attacks.User Password AccessFor MikroTik routers, it's essential to set up passwords. We recommend using a password generator tool to create robust passwords that meet the following criteria:At least 12 characters long;Consist of numbers, symbols, uppercase, and lowercase letters;Avoid using dictionary words or combinations thereof. /user set 0 password="!={Ba3N!40TyX+GvKBzjTLIUcx/," Another method to set a password for the current user:We highly recommend using a secondary method or the Winbox interface to update your router's password, as an added measure to safeguard against unauthorized access. [admin@MikroTik] > /password old-password: ******** new-password: ********** confirm-new-password: ********** Ensure you remember the password! If it's forgotten, there's no way to recover it. You'll have to reset the configuration or reinstall the router system!You can also add additional users with full or limited router access in the /user menu /user add name=myname password=mypassword group=full /user remove admin MAC Connectivity AccessBy default, the MAC server runs on all interfaces. To restrict MAC connectivity from the WAN port, we'll disable the default all entry and add a LAN interface.First, create an interface list: [admin@MikroTik] > /interface list add name=LAN Then, add your previously created bridge named "bridge1" to the interface list: [admin@MikroTik] > /interface list member add list=LAN interface=bridge1 Apply newly created interface list to the MAC server: [admin@MikroTik] > /tool mac-server set allowed-interface-list=LAN Do the same for Winbox MAC access [admin@MikroTik] > /tool mac-server mac-winbox set allowed-interface-list=LAN Winbox/Webfig actions:Navigate to Interfaces → Interface List → Lists window;Click on the "+" button to add a new list;Enter "LAN" into the Name field and click OK;Return to the Interfaces → Interface List section;Click on the "+" button;Select "LAN" from the dropdown List options;Choose "bridge1" from the dropdown Interface options;Click OK to confirm;Open Tools -> Mac Server window;Click on the MAC Telnet Server button;In the new dialog, select the newly created list "LAN" from the dropdown list;Click OK to apply settings.Do the same in the MAC Winbox Server tab to block Mac Winbox connections from the internet.Neighbor DiscoveryMikroTik Neighbor discovery protocol is used to show and recognize other MikroTik routers in the network. Disable neighbor discovery on public interfaces: /ip neighbor discovery-settings set discover-interface-list=LAN IP Connectivity AccessWhile the firewall protects your router from unauthorized access by external networks, it's also possible to restrict username access based on specific IP addresses /user set 0 address=x.x.x.x/yy x.x.x.x/yy - your IP or network subnet that is allowed to access your router.IP connectivity on the public interface must be limited in the firewall. We will accept only ICMP(ping/traceroute), IP Winbox, and ssh access. /ip firewall filter add chain=input action=accept connection-state=established,related,untracked comment="accept established,related,untracked" add chain=input action=drop connection-state=invalid comment="drop invalid" add chain=input in-interface=ether1 action=accept protocol=icmp comment="accept ICMP" add chain=input in-interface=ether1 action=accept protocol=tcp port=8291 comment="allow Winbox"; add chain=input in-interface=ether1 action=accept protocol=tcp port=22 comment="allow SSH"; add chain=input in-interface=ether1 action=drop comment="block everything else"; The first rule accepts packets from already established connections, assuming they are safe to not overload the CPU. The second rule drops any packet that connection tracking identifies as invalid. After that, we set up typical accept rules for specific protocols.If you are using Winbox/WebFig for configuration, here is an example of how to add an established/related/untracked rule:Open the IP -> Firewall window and navigate to the Filter Rules tab;Click on the "+" button to open a new dialog;Select "input" for the chain.Click on "Connection state" and check the boxes for "established," "related," and "untracked."Go to the Action tab and ensure that "accept" is selected.Click on OK to apply the settings.To add additional rules, click on the "+" button for each new rule and fill in the same parameters as provided in the console example.Administrative ServicesAlthough the firewall protects the router from the public interface, you may still want to disable RouterOS services.Most of RouterOS administrative tools are configured at the /ip service menuKeep only secure ones, /ip service disable telnet,ftp,www,api Change default service ports, this will immediately stop most of the random SSH brute force login attempts: /ip service set ssh port=2200 Additionally, each service can be secured by allowed IP address or address range(the address service will reply to), although more preferred method is to block unwanted access in firewall because the firewall will not even allow to open socket /ip service set winbox address=192.168.88.0/24 Other ServicesA bandwidth server is used to test throughput between two MikroTik routers. Disable it in the production environment. /tool bandwidth-server set enabled=no A router might have DNS cache enabled, which decreases resolving time for DNS requests from clients to remote servers. In case DNS cache is not required on your router or another router is used for such purposes, disable it. /ip dns set allow-remote-requests=no Some RouterBOARDs have an LCD module for informational purposes, set pin or disable it.It is good practice to disable all unused interfaces on your router, in order to decrease unauthorized access to your router. /interface print /interface set x disabled=yes Where "X" is a number of the unused interfaces.RouterOS utilizes stronger crypto for SSH, most newer programs use it, to turn on SSH strong crypto: /ip ssh set strong-crypto=yes Following services are disabled by default, nevertheless, it is better to make sure that none of then were enabled accidentally:MikroTik dynamic name service or IP cloud, /ip cloud set ddns-enabled=no update-time=no NAT ConfigurationAt this point, PC is not yet able to access the Internet, because locally used addresses are not routable over the Internet. Remote hosts simply do not know how to correctly reply to your local address.The solution for this problem is to change the source address for outgoing packets to routers public IP. This can be done with the NAT rule: /ip firewall nat add chain=srcnat out-interface=ether1 action=masquerade Another benefit of such a setup is that NATed clients behind the router are not directly connected to the Internet, that way additional protection against attacks from outside mostly is not required.Port ForwardingSome client devices may need direct access to the internet over specific ports. For example, a client with an IP address 192.168.88.254 must be accessible by Remote desktop protocol (RDP).After a quick search on Google, we find out that RDP runs on TCP port 3389. Now we can add a destination NAT rule to redirect RDP to the client's PC. /ip firewall nat add chain=dstnat protocol=tcp port=3389 in-interface=ether1 \ action=dst-nat to-address=192.168.88.254 Setting up WirelessFor ease of use bridged wireless setup will be made so that your wired hosts are in the same Ethernet broadcast domain as wireless clients.The important part is to make sure that our wireless is protected, so the first step is the security profile.Security profiles are configured from /interface wireless security-profiles menu in a terminal. /interface wireless security-profiles add name=myProfile authentication-types=wpa2-psk mode=dynamic-keys \ wpa2-pre-shared-key=1234567890 in Winbox/Webfig click on Wireless to open wireless windows and choose the Security Profile tab.If there are legacy devices that do not support WPA2 (like Windows XP), you may also want to allow WPA protocol.Now when the security profile is ready we can enable the wireless interface and set the desired parameters /interface wireless enable wlan1; set wlan1 band=2ghz-b/g/n channel-width=20/40mhz-Ce distance=indoors \ mode=ap-bridge ssid=MikroTik-006360 wireless-protocol=802.11 \ security-profile=myProfile frequency-mode=regulatory-domain \ set country=latvia antenna-gain=3 To do the same from Winbox/Webfig:Open Wireless window, select wlan1 interface, and click on the enable button;Double click on the wireless interface to open the configuration dialog;In the configuration dialog click on the Wireless tab and click the Advanced mode button on the right side. When you click on the button additional configuration parameters will appear and the description of the button will change to Simple mode;Choose parameters as shown in the screenshot, except for the country settings and SSID. You may want to also choose a different frequency and antenna gain;Next, click on the HT tab and make sure both chains are selected;Click on the OK button to apply settings.The last step is to add a wireless interface to a local bridge, otherwise connected clients will not get an IP address: /interface bridge port add interface=wlan1 bridge=bridge1 Now wireless should be able to connect to your access point, get an IP address, and access the internet.Protecting the ClientsNow it is time to add some protection for clients on our LAN. We will start with a basic set of rules. /ip firewall filter add chain=forward action=fasttrack-connection connection-state=established,related \ comment="fast-track for established,related"; add chain=forward action=accept connection-state=established,related \ comment="accept established,related"; add chain=forward action=drop connection-state=invalid add chain=forward action=drop connection-state=new connection-nat-state=!dstnat \ in-interface=ether1 comment="drop access to clients behind NAT from WAN" A ruleset is similar to input chain rules (accept established/related and drop invalid), except the first rule with action=fasttrack-connection. This rule allows established and related connections to bypass the firewall and significantly reduce CPU usage.Another difference is the last rule which drops all new connection attempts from the WAN port to our LAN network (unless DstNat is used). Without this rule, if an attacker knows or guesses your local subnet, he/she can establish connections directly to local hosts and cause a security threat.For more detailed examples on how to build firewalls will be discussed in the firewall section.Blocking Unwanted WebsitesSometimes you may want to block certain websites, for example, deny access to entertainment sites for employees, deny access to porn, and so on. This can be achieved by redirecting HTTP traffic to a proxy server and use an access-list to allow or deny certain websites.First, we need to add a NAT rule to redirect HTTP to our proxy. We will use RouterOS built-in proxy server running on port 8080. /ip firewall nat add chain=dst-nat protocol=tcp dst-port=80 src-address=192.168.88.0/24 \ action=redirect to-ports=8080 Enable web proxy and drop some websites: /ip proxy set enabled=yes /ip proxy access add dst-host=www.facebook.com action=deny /ip proxy access add dst-host=*.youtube.* action=deny /ip proxy access add dst-host=:vimeo action=deny Using Winbox:On the left menu navigate to IP -> Web ProxyWeb proxy settings dialog will appear.Check the "Enable" checkbox and click on the "Apply" buttonThen click on the "Access" button to open the "Web Proxy Access" dialogIn the "Web Proxy Access" dialog click on "+" to add a new Web-proxy ruleEnter Dst hostname that you want to block, in this case, "www.facebook.com", choose the action "deny"Then click on the "Ok" button to apply changes.Repeat the same to add other rules.TroubleshootingRouterOS has built-in various troubleshooting tools, like ping, traceroute, torch, packet sniffer, bandwidth test, etc.We already used the ping tool in this article to verify internet connectivity.Troubleshoot if ping failsThe problem with the ping tool is that it says only that destination is unreachable, but no more detailed information is available. Let's overview the basic mistakes.You cannot reach www.google.com from your computer which is connected to a MikroTik device: Info updated May 23, 2025 The majority of MikroTik routers have a default username of admin, a default password of -, and the default IP address of 192.168.88.1. These MikroTik credentials are needed when doing a login to the MikroTik router's web interface to change any settings. Since some of the models don't follow the standards, you can see those in the table below. Below the table are also instructions on what to do incase you forget your MikroTik router password, need to reset your MikroTik router to its factory default password, or the password reset doesn't work. Tip: Press ctrl+f (or cmd+f on Mac) to quickly search for your model number. MikroTik default Password List (Valid May 2025) Instructions and common questions Forgot your MikroTik router password? Have you changed the username and/or password of your MikroTik router and forgotten what you changed it to? Don't worry: all MikroTik routers come with a default factory set password that you can revert to by following the instructions below. Reset MikroTik router to default password If you decide to revert your MikroTik router to it's factory defaults, you should do the 30-30-30 reset as follows: When your MikroTik router is powered on, press and hold the reset button for 30 seconds. While still holding the reset button pressed, unplug the power of the router and hold the reset button for another 30 seconds While still holding the reset button down, turn on the power to the unit again and hold for another 30 seconds. Your MikroTik router should now be reset to its brand new factory settings, Check the table to see what those are (Most likely admin/-). If the factory reset didn't work, check out the MikroTik 30 30 30 factory reset guide . Important: Remember to change the default username and password to increase the security of your router after the factory reset, as the default passwords are available all over the web (like here). I still can't access my MikroTik router with the default password Make sure that you have followed the reset instructions correctly as the MikroTik routers should always rever to their factory default settings when reset. Otherwise, there is always the risk that your router is damaged and might need to be repaired or replaced. VPN (Virtual Private Network) is a technology that provides a secure and encrypted tunnel across a public network. A private network user can send and receive data to any remote private network using this VPN Tunnel as if his/her network device was directly connected to that private network.Site to Site VPN technique establishes a secure tunnel between two routers across public network and local networks of these routers can send and receive data through this VPN tunnel. MikroTik RouterOS offers IPsec (Internet Protocol Security) VPN Service that can be used to establish a site to site VPN tunnel between two routers. IPsec is a network protocol suite that authenticates and encrypts the packets of data send over a network.The goal of this article is to configure a site to site IPsec VPN Tunnel with MikroTik RouterOS. So, rest of this article I will show how to configure IPsec VPN between two MikroTik Routers so that an IPsec VPN Tunnel can be established between them and local networks of these routers can communicate with each other.Network DiagramTo configure a site to site IPsec VPN Tunnel between two MikroTik Routers, I am following a network diagram like below image.Site to Site IPsec NetworkIn this network, Office1 Router is connected to internet through ether1 interface having IP address 192.168.70.2/30. In your real network this IP address will be replaced with your public IP address. Office1 Router’s ether2 interface is connected to local network having IP network 10.10.11.0/24. Similarly, Office2 Router is connected to internet through ether1 interface having IP address 192.168.80.2/30. In your real network this IP address will also be replaced with public IP address. Office 2 Router’s ether2 interface is connected to local network having IP network 10.10.12.0/24. We will configure site to site IPsec VPN Tunnel between these two routers so that local network of these routers can communicate to each other through this VPN tunnel across public network.Core Devices and IP InformationTo configure a site to site IPsec VPN with MikroTik RouterOS, I am using two MikroTik RouterOS v6.38.1. IP information that I am using for this network configuration are given below.Office 1 Router WAN IP: 192.168.70.2/30 and LAN IP Block 10.10.11.0/24Office 2 Router WAN IP: 192.168.80.2/30 and LAN IP Block 10.10.12.0/24This IP information is just for my RND purpose. Change this information according to your network requirements.We will now start our site to site IPsec VPN configuration according to the above network diagram. Complete configuration can be divided into four parts.MikroTik RouterOS basic configurationIPsec Peer configurationIPsec Policy and Proposal ConfigurationNAT Bypass ConfigurationBasic RouterOS configuration includes assigning WAN IP, LAN IP, DNS IP and Route, NAT configuration. According to our network diagram, we will now complete these topics in our two MikroTik RouterOS (Office 1 Router and Office 2 Router).Office 1 Router Basic ConfigurationThe following steps will guide you how to perform basic configuration in your Office 1 RouterOS.Login to Office 1 RouterOS using winbox and go to IP > Addresses. In Address List window, click on PLUS SIGN (+). In New Address window, put WAN IP address (192.168.70.2/30) in Address input field and choose WAN interface (ether1) from Interface dropdown menu and click on Apply and OK button. Click on PLUS SIGN again and put LAN IP (10.10.11.1/24) in Address input field and choose LAN interface (ether2) from Interface dropdown menu and click on Apply and OK button.Go to IP > DNS and put DNS servers IP (8.8.8.8 or 8.8.4.4) in Servers input field and click on Apply and OK button.Go to IP > Firewall and click on NAT tab and then click on PLUS SIGN (+). Under General tab, choose srcnat from Chain dropdown menu and click on Action tab and then choose masquerade from Action dropdown menu. Click on Apply and OK button.Go to IP > Routes and click on PLUS SIGN (+). In New Route window, click on Gateway input field and put WAN Gateway address (192.168.70.1) in Gateway input field and click on Apply and OK button.Basic RouterOS configuration has been completed in Office 1 Router. Now we will do similar steps in Office 2 RouterOS.Office 2 Router Basic ConfigurationThe following steps will guide you how to perform basic configuration in your Office 2 RouterOS.Login to Office 2 RouterOS using winbox and go to IP > Addresses. In Address List window, click on PLUS SIGN (+). In New Address window, put WAN IP address (192.168.80.2/30) in Address input field and choose WAN interface (ether1) from Interface dropdown menu and click on Apply and OK button. Click on PLUS SIGN again and put LAN IP (10.10.12.1/24) in Address input field and choose LAN interface (ether2) from Interface dropdown menu and click on Apply and OK button.Go to IP > DNS and put DNS servers IP (8.8.8.8 or 8.8.4.4) in Servers input field and click on Apply and OK button.Go to IP > Firewall and click on NAT tab and then click on PLUS SIGN (+). Under General tab, choose srcnat from Chain dropdown menu and click on Action tab and then choose masquerade from Action dropdown menu. Click on Apply and OK button.Go to IP > Routes and click on PLUS SIGN (+). In New Route window, click on Gateway input field and put WAN Gateway address (192.168.80.1) in Gateway input field and click on Apply and OK button.Basic RouterOS configuration has been completed in Office 2 Router. Now we are going to start IPsec Peer configuration.After MikroTik Router basic configuration, we will now configure IPsec Peer in both MikroTik RouterOS. In IPsec Peer configuration, we will specify peer address, port and pre-shred-key.IPsec Peer Configuration in Office 1 RouterThe following steps will show how to configure IPsec Peer in your Office 1 RouterOS.Go to IP > IPsec and click on Peers tab and then click on PLUS SIGN (+).In New IPsec Peer window, put Office 2 Router’s WAN IP (192.168.80.2) in Address input field and put 500 in Port input field.Choose pre shared key option from Auth. Method dropdown menu.Provide a suitable password in Secret input field. This password is required for IPsec authentication and must be same in both routers.Click Apply and OK button.IPsec Peer configuration in Office 1Router has been completed. Now we will configure IPsec Peer in Office 2 Router.IPsec Peer Configuration in Office 2 RouterWe will do the same steps as Office 1 Router’s IPsec Peer configuration in Office 2 Router but only address parameter will be changed.Go to IP > IPsec and click on Peers tab and then click on PLUS SIGN (+).In New IPsec Peer window, put Office 1 Router’s WAN IP (192.168.70.2) in Address input field and put 500 in Port input field.Choose pre shared key option from Auth. Method dropdown menu.Provide a suitable password in Secret input field. This password is required for IPsec authentication and must be same in both routers.Click Apply and OK button.IPsec Peer configuration in our both Office Routers has been completed. Now we will start Policy and Proposal configuration for our IPsec VPN Tunnel.After IPsec Peer configuration it is time to configure IPsec Policy and Proposal. It is important that proposed authentication and encryption algorithms must match on both routers. In this example, we will use predefined default proposal. You will find default proposed authentication algorithms and encryption algorithms in Proposals tab. In this part we will only configure IPsec Policy on both routers. In Policy configuration we will specify source and destination network that will pass through IPsec tunnel and the mode of this IPsec VPN.IPsec Policy Configuration in Office 1 RouterThe following steps will show how to configure IPsec Policy in Office 1 RouterOS.IPsec Policy configuration in Office 1 Router has been completed. Similarly we will configure IPsec Policy in Office 2 Router.IPsec Policy Configuration in Office 1 RouterThe following steps will show the configuration of IPsec Policy in Office 1 RouterOS.Go to IP > IPsec and click on Polices tab and then click on PLUS SIGN (+). New IPsec Policy window will appear.In General tab put your source network (Office 1 Router’s network: 10.10.12.0/24) that will be matched in data packets in Address input field and keep Src. Port untouched .Put your destination network (Office 2 Router’s network: 10.10.11.0/24) that will be matched in packets in Address input field and keep Dst. Port untouched.Now click on Action tab and click on Tunnel checkbox to enable tunnel mode.Put Office 1 Router’s WAN IP (192.168.80.2) in SA Src. Address input field and Office 2 Router’s WAN IP (192.168.70.2) in SA Dst. Address input field.Make sure default option is selected in Proposal dropdown menuClick Apply and OK button.IPsec Policy configuration in Office 1 Router has been completed. At this point IPsec tunnel will be created between two office routers but local networks cannot communicate with each other. This is because both routers have NAT rules that is changing source address after packet is encrypted. Remote router receives encrypted packet but is unable to decrypt it because source address do not match address specified in policy configuration. The Solution is to set up NAT Bypass rule.We will now configure NAT Bypass rule in our both Office Routers otherwise local network will not be able to communicate with each other.NAT Bypass Rule Configuration in Office 1 RouterThe following steps will show how to create NAT Bypass rule in your Office 1 RouterOS.Go to IP > Firewall and click on NAT tab and then click on PLUS SIGN (+). New NAT Rule window will appear.In General tab, choose srcnat from Chain dropdown menu.Put Office 1 Router’s LAN network (10.10.11.0/24) that wants to communicate to Office 2 Router, in Src. Address input field.Put Office 2 Router’s LAN network (10.10.12.0/24) where Office 1 Router wants to reach, in Dst. Address input field.Click on Action tab and choose accept option from Action dropdown menu.Click Apply and OK button.Your newly created rule will be available in the list table. Now place this rule at first position by drag and drop otherwise this rule will not be workable.NAT Bypass rule in Office 1 Router has been completed. Similarly we will create NAT Bypass rule in Office 2 RouterOS.NAT Bypass Rule Configuration in Office 1 RouterThe following steps will show the configuration of NAT Bypass rule in Office2 RouterOS. Go to IP > Firewall and click on NAT tab and then click on PLUS SIGN (+). New NAT Rule window will appear.In General tab, choose srcnat from Chain dropdown menu.Put Office 2 Router’s LAN network (10.10.12.0/24) that wants to communicate to Office 1 Router, in Src. Address input field.Put Office 1 Router’s LAN network (10.10.11.0/24) where Office 2 Router wants to reach, in Dst. Address input field.Click on Action tab and choose accept option from Action dropdown menu.Click Apply and OK button.Your newly created rule will be available in the list table. Now place this rule at first position by drag and drop otherwise this rule will not be workable. NAT Bypass rule in Office 2 Router has been completed. Now Office 1 Router’s local network will able to reach Office 2 Router’s local network through IPsec VPN Tunnel across public network and vice versa. To check your configuration, do a ping request from any local network machine to other local network machine. If everything is OK, your ping request will be success. If you face any confusion to do above steps properly, watch my video about MikroTik IPsec Site to Site VPN Configuration. I hope it will reduce your any confusion. MikroTik IPsec Site to Site VPN Configuration has been explained in this article. I hope you are now able to configure site to site IPsec VPN between two routers following the above steps properly. However, if you face any problem to configure IPsec site to site VPN, feel free to discuss in comment or contact with me from Contact page. I will try my best to stay with you. Applies to RouterOS: All After you have installed the RouterOS software, or turned on the Router for the first time, there are various ways how to connect to it: Accessing Command Line Interface (CLI) via Telnet, SSH, serial cable or even keyboard and monitor if your router has a VGA card. Accessing Web based GUI (WebFig) Using the WinBox configuration utility (Windows app, compatible with Wine) Every router is factory pre-configured with the IP address 192.168.88.1/24 on the ether1 port. The default username is admin with no password (or, for some models with password, check it on the sticker). After you log in for the first time, please create a new user with a password in the "full" group, re-login and delete the default admin user. We highly recommend you to follow the general guidelines of the article Securing your router to protect the device from any unauthorised access. Additional configuration may be set depending on RouterBOARD model. Most models have the ether1 configured as a WAN port and any communication with the router through that port is not possible, since it is firewalled to protect from any outside access. List of RouterBOARD models and their default configurations can be found in this article. Winbox Winbox is a configuration utility that can connect to the router via MAC or IP protocol. Latest winbox version can be downloaded from our download page. Connecting to a device 1) Run the Winbox utility 2) Navigate to "Neighbors" 3) See if Winbox finds your Router and it's MAC address Info: Winbox neighbor discovery will discover all routers on the broadcast network 4) If you see your router on the list, connect to it by clicking on IP/MAC address and pressing Connect button Winbox will try download plugins from the router, if it is connecting for the first time to the router with current version. Note that it may take up to one minute to download all plugins if winbox is connected with MAC protocol 5) After winbox have successfully downloaded plugins and authenticated, main window will be displayed: If winbox cannot find any routers, make sure that:) Your Windows computer is directly connected to the router with an Ethernet cable or they are in the same broadcast domain) As MAC connection works on Layer2, it is possible to connect to the router even without proper IP address configuration, but might be required due to most driver not enabling IP stack if there is no IPv4 configuration. Due to the use of broadcasting MAC connection is not stable enough to use continuously, therefore it is not wise to use it on a real production / live network!. MAC connection should be used only for initial configuration. Follow winbox manual for more information. QuickSet and WebFig If you have a router with default configuration, the IP address of the router can be used to connect to the Web interface. The first screen to come up will be QuickSet, where you can set the password and basic settings to secure your device. For more advanced settings, click the WebFig button to open the Advanced mode, which has almost the same configuration functionality as Winbox. Please see following articles to learn more about web interface configuration: Initial Configuration with WebFig General WebFig Manual CLI Command Line Interface (CLI) allows configuration of the router's settings using text commands. Since there is a lot of available commands, they are split into groups organized in a way of hierarchical menu levels. Follow console manual for CLI syntax and commands. There are several ways how to access CLI: Winbox terminal menu Telnet SSH serial cable etc. Serial Cable If your device has a Serial port, you can use a console cable (or Null modem cable) Plug one end of the serial cable into the console port (also known as a serial port or DB9 RS232C asynchronous serial port) of the RouterBOARD and the other end in your PC (which hopefully runs Windows or Linux). You can also use a USB-Serial adapter. Run a terminal program (HyperTerminal, or Putty on Windows) with the following parameters for All RouterBOARD models except 230: 115200bit/s, 8 data bits, 1 stop bit, no parity, flow control=none by default. RouterBOARD 230 parameters are: 9600bit/s, 8 data bits, 1 stop bit, no parity, hardware (RTS/CTS) flow control by default. If parameters are set correctly you should be able to see login prompt. Now you can access router by