

Mikrotik SXTsq 5 ac

The SXTsq 5 ac is a small client access antenna that is 802.11 standards compliant antenna (and also nstream mikrotik if available).

The device was released in early 2018 and is capable of gigabit-level speeds with 80Mhz wide 802.11ac wifi connections.

Please be sure to see [MikroTik Specifics](#) for extra info about Mikrotik devices, how to connect, etc.

MikroTik SXTsq 5 ac

Device specs are available at mikrotik.com.

Uses

- Wirelessly connect SXTsq to OmniTik ([instructions](#))
 - [Legacy OSPF configurations](#)
- Connect SXTsq to LinkNYC kiosk ([instructions](#)) ([more info](#))
- Create a Point-to-Point link ([instructions](#))
- Legacy Client Node ([instructions](#))

Device idiosyncrasies

License

Mikrotik software usually requires a license, though all Mikrotik devices come with an internal license, which varies with the model. This antenna comes with a "Level 3" license which technically only allows it to function as a CPE, not an AP. Therefore this device can not be used as a base station.

US vs International version

On the positive side, it is a great CPE and can connect to DFS channels (international version) and has other interesting features such as EAP TTLS authentication.

Be aware during purchase -- this antenna has a US version and an International version. The US version is locked to "united states3" channels which are the non-DFS range. The international version also has US settings, but it has two additional "united states" channel selections all for valid legal US channels. You cannot connect to a LinkNYC kiosk with the US version.

To function on LinkNYC and other DFS networks, the international version is required, but be sure to put it in "united states2" mode before using it.

Configurations

Wirelessly connect SXTsq to OmniTik

1. Download configuration file

First, download the configuration file for your network number. If you only have an install number, enter this number below. If `error: no address for ****` is displayed, please reach out to us on [Slack](#) at #install or via [email](#) to register your installation. If `Sorry, unable to open the file at this time` is displayed, try using Incognito Mode or Private Browsing.

Install Number:

Once you have your Network Number, go to the Configgen utility to download the correct configuration for your use case.

[Plug SXTsq into port 5 of an OmniTik](#)

[Plug SXTsq directly into indoor home router](#)

Enter your network number into the "network_number" field and click "Download Config". Make note of the filename for later.

2. Connect to device and upload file

Next, plug in the device to power by connecting an Ethernet patch cable from the device to the POE injector. Plug the other end of the POE injector to your computer's Ethernet port or USB-to-Ethernet adapter.

What if I cannot use Ethernet with my computer?

If your computer does not have Ethernet and you do not have an adapter, plug in the device to a LAN port on your home router.

If you are using the WinBox method, no changes to the procedure are needed.

If you are using the Terminal method, find the IP address of the device in your router's settings, and use that instead of 192.168.88.1. No need to change your computer's IP settings.

There are two methods you can use to upload the file to the device.

WinBox (Windows and Mac)

Download the WinBox utility from the [MikroTik website](#) for Windows, or from [Joshaven Potter's website](#) for Mac.

Open the utility and click the "Neighbors" tab on the lower-half of the screen, and click "Refresh".

Double-click on the **MAC Address** (important!) that appears in the list. When the MAC Address populates into the "Connect To" box, hit "Connect".

You will get a prompt saying "RouterOS Default Configuration". Hit OK to dismiss.

On the left sidebar, click "Files". Open a File Explorer or Finder window alongside winbox and drop the configuration file you downloaded earlier into the "flash" folder. You should see the uploaded file have `flash/` before the filename (important! if it doesn't have flash before it, make sure you drop the file onto the flash folder and try again).

On the left sidebar, click "System", then "Reset Configuration". Check the "No Default Configuration" box, and click the down arrow next to "Run After Reset" to select the file you uploaded. Finally, hit "Reset Configuration" and you will be disconnected. After a couple of minutes, the LED next to the person icon on the device will turn on, indicating that the configuration has been applied.

Terminal

First, disable any other interfaces such as WiFi you may have on your system other than the Ethernet interface connected to the device. Then, you will have to change your IP address to `192.168.88.5` (this process will vary depending on your operating system).

Open your terminal or command prompt and navigate to the directory where your configuration file is saved. Enter the following command into the terminal, replacing [CONFIG FILE] with the name of the downloaded file from earlier:

```
scp -o StrictHostKeyChecking=no [CONFIG FILE] admin@192.168.88.1: flash/
```

After the file transfers, then enter the following command into the terminal to reset the device with the new configuration, replacing [CONFIG FILE] with the name of the downloaded file from earlier:

```
ssh -o StrictHostKeyChecking=no admin@192.168.88.1 /system reset-configuration no-defaults=yes  
run-after-reset=flash/[CONFIG FILE]
```

The device will reboot in the background. After a couple of minutes, the LED next to the person icon on the device will turn on, indicating that the configuration has been applied.

3. Configure the link

Depending on your use case, you will connect to the antenna differently based on the configuration you selected above.

Plug SXTsq into port 5 of an OmniTik

Disconnect the device from the POE injector and plug the device into Port 5 of the OmniTik on the roof. Then, connect your computer to the OmniTik's WiFi or use Ethernet (if you modified your Ethernet adapter to use a static IP, change it to DHCP). Find the Gateway IP from the interface (this process will vary depending on your operating system) and enter it into your browser.

Log into the OmniTik. On the left sidebar, click "Bridge". Click on the "Filters" tab, and disable the first item on the list, so you will be able to access the device locally (important: when you are done, come back here to reenabling the filter!). On the left sidebar, click "IP", then "DHCP Server". Click on the "Leases" tab, where you will see a device with the hostname containing "sxt". Type this IP address into a new tab on your browser.

Plug SXTsq directly into indoor home router

Ensure your computer is plugged directly into the SXT's POE injector via Ethernet (if you modified your Ethernet adapter to use a static IP, change it to DHCP). At this point, you will need your device to be outdoors to perform the alignment, so a battery pack is recommended to power the device outside.

Find the Gateway IP from the interface (this process will vary depending on your operating system) and enter it into your browser.

Log into the SXT. On the left sidebar, click "Wireless". Click the item named wlan1.

If you already know what node to connect to

If you already know what node you are connecting to (if you only have the install number, see above to convert the install number to its network number), scroll down to "SSID" and replace the `xxxx` with the network number of the node you are connecting to. Scroll down to Description and do the same, then scroll to the top and click "Apply".

Roughly align the device towards the desired node. If the alignment is sufficient, the status will change from `searching for network` to `connected to ess`, indicating that the connection has been established with the other OmniTik. If the status does not change, verify that the device is aimed towards the other node and that the other node is powered on.

If you do not already know what node to connect to

Look at the [map](#) to determine what might be around. If you see a nearby node, click the node and see above to convert the displayed install number to its network number.

Roughly align the device towards the desired node. To verify that the connection will work, click "Scan..." on the top of the screen. Click "Start", and click "Radio Name" twice to bring all of the NYC Mesh nodes to the top. If your desired node does not appear on the list, verify that the device is aimed towards the other node and that the other node is powered on.

Click "Cancel". Scroll down to "SSID" and replace the `xxxx` with the network number of the node you are connecting to. Scroll down to Description and do the same, then scroll to the top and click "Apply".

4. Align the antenna

Scroll down to "Tx/Rx Signal Strength" and look at the numbers. Align the device to get the values closest to 0. -30s are excellent, -40s are great, -50s are good, -60s are fair, and -70s will be unusable.

Once the device is aligned for best signal, tighten the clamp and secure all cables. Congratulations, the SXT install is complete!

Legacy OSPF configurations

Wirelessly connect SXTsq to OmniTik via WDS

The SXTsq also supports WDS, which allows the device to automatically connect to nearby NYC Mesh OmniTiks. However, if there are multiple OmniTiks in range that have equal-length paths to a supernode, there may be routing issues and performance degradation.

[Plug SXTsq into port 5 of an OmniTik](#)

[Plug SXTsq directly into indoor home router](#)

Wirelessly connect SXTsq to OmniTik

The SXTsq also has a variation of the first configuration that uses OSPF to communicate with the OmniTik, instead of DHCP. This is only needed if the SXTsq needs to be a router instead of a simple bridge.

[Plug SXTsq into port 5 of an OmniTik](#)

LinkNYC Kiosk connection (encrypted)

LinkNYC kiosks have both an unencrypted and encrypted network available. They function similarly and have the same Internet available.

The encrypted version uses a feature marketed as "passpoint" which allows you to roam across an area with a user name and password using [EAP TTLS](#). The encrypted network is more secure because no traffic can be sniffed between the kiosk and your CPE. Another benefit is it skips the captive portal (a webpage that pops up when you connect).

When you login to the LinkNYC unencrypted network, a captive portal prompts you to click a button, and if your device is supported, download a profile and reconnect to the encrypted network. Currently only iPhones are supported with the auto-config feature. However, it's technically possible to connect with any capable device once you have a connection profile. By taking the profile from an iPhone, we can extract the pieces needed to connect a standard antenna such as the sxtsq.

After powering on an sxtsq you should configure it as a CPE with routing, NAT, and DHCP on the internal port.

Then, to configure the radio, apply the following lines on the command line interface (CLI): (This can be performed using the graphical user interface, but it may be faster to paste these lines.)

```
/interface wireless security-profiles
add authentication-types=wpa-eap,wpa2-eap eap-methods=eap-tls-mschapv2 group-
ciphers=tkip,aes-ccm mode=dynamic-keys mschapv2-password=5fs0pxER mschapv2-
username=anonymous@citybridge.com name=linknyc supplicant-identity=anonymous@citybridge.com
tls-mode=dont-verify-certificate unicast-ciphers=tkip,aes-ccm

/interface wireless
set [ find default-name=wlan1 ] band=5ghz-a/n/ac channel-width=20/40/80mhz-Ceee
country="united states2" default-authentication=no disabled=no frequency=auto security-
profile=linknyc ssid="LinkNYC Private" wireless-protocol=802.11

/interface wireless connect-list
add interface=wlan1 security-profile=linknyc ssid="LinkNYC Private" wireless-protocol=802.11
```

Be sure to shutdown the antenna properly the first time to ensure the config is saved. This is not required, but Mikrotik antennas are especially sensitive to being powered off with no proper shutdown.

Create a Point-to-Point link

The following works with two new SXTsq or a reset SXTsq. To reset an SXTsq, hold the reset button for about 5 seconds while the unit is booting and release as soon as green LED starts flashing (to reset RouterOS configuration to defaults). It is recommended to update the firmware of your SXTsq to the latest. The under has been tested with firmware v.6.43.12

One of the SXT will act as an "AP" but can be associated to only one "client". The second SXT will be the "client".

After the configuration there will be no DHCP Server or Client, thus you will need to configure your laptop IP manually in the same network range, for exemple 192.168.88.11

The SXT-AP and SXT-Client port address will be change in order to not interfere with another potential SXT default IP.

- AP will be ether1: 192.168.88.2 and bridge1: 192.168.88.3
- Client will be ether1: 192.168.88.4 and bridge1: 192.168.88.5

Connect to the SXTsq via ethernet and DHCP. You will get a 192.168.88.xxx address

In the terminal

```
ssh -o StrictHostKeyChecking=no admin@192.168.88.1
```

Say 'yes' to the warning and paste this for the SXT-AP-

```
# Feb 25th 2019 for RouterOS 6.43.12
# model = RBSXTsqG-5acD

# SXT PtP / This is the AP

# Set the SXT Identity
/system identity
set name="sxt ptp ap"

#add security profile (to secure wifi connection login) and SSID
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
add authentication-types=wpa-psk,wpa2-psk management-protection=allowed mode=\
dynamic-keys name=sxt-ap supplicant-identity="SXT PtP AP" \
wpa-pre-shared-key=nycmeshnet wpa2-pre-shared-key=nycmeshnet

#set the wireless (wlan1) to USA 2 and the proper band
/interface wireless
set [ find default-name=wlan1 ] band=5ghz-a/n/ac channel-width=\
20/40/80mhz-Ceee country="united states2" disabled=no mode=bridge \
security-profile=sxt-ap ssid=nycmesh-nn-sxtptp

# disable the NAT and disable all the firewall filters
/ip firewall nat
set numbers=0 disabled=yes

/ip firewall filter
set numbers=1 disabled=yes
set numbers=2 disabled=yes
set numbers=3 disabled=yes
set numbers=4 disabled=yes
set numbers=5 disabled=yes
set numbers=6 disabled=yes
set numbers=7 disabled=yes
set numbers=8 disabled=yes
set numbers=9 disabled=yes
set numbers=10 disabled=yes
```



```
# disable the dhcp-client and server
/ip dhcp-client
set [ find interface=wlan1 ] disabled=yes
/ip dhcp-server
set [ find interface=ether1 ] disabled=yes

#add a bridge and add port ether1 and wlan1 (switch)
/interface bridge
add name=bridge1
/interface bridge port
add bridge=bridge1 interface=ether1
add bridge=bridge1 interface=wlan1

#change IP address of the "sxt ptp client" to not mix with potential other SXT default IP
address
/ip address
add address=192.168.88.3/24 interface=bridge1 network=192.168.88.0
set [ find interface=ether1 ] address=192.168.88.2/24
```

Say 'yes' to the warning and paste this for the SXT-Client-

```
# Feb 25th 2019 for RouterOS 6.43.12
# model = RBSXTsqG-5acD

# SXT PtP / This is the Client

# Set the SXT Identity
/system identity
set name="sxt ptp client"

#add security profile (to secure wifi connection login)
/interface wireless security-profiles
set [ find default=yes ] authentication-types=wpa-psk,wpa2-psk group-ciphers=\
tkip,aes-ccm mode=dynamic-keys supplicant-identity=MikroTik \
unicast-ciphers=tkip,aes-ccm wpa-pre-shared-key=nycmeshnet \
wpa2-pre-shared-key=nycmeshnet
/interface wireless security-profiles
add authentication-types=wpa-psk,wpa2-psk group-ciphers=tkip,aes-ccm \
management-protection=allowed mode=dynamic-keys name=sxt-ap \
```

```
supplicant-identity="sxt ptp client" unicast-ciphers=tkip,aes-ccm \
wpa-pre-shared-key=nycmeshnet wpa2-pre-shared-key=nycmeshnet

#set the wireless (wlan1) to USA 2 and the proper band.
/interface wireless
set [ find default-name=wlan1 ] band=5ghz-a/n/ac channel-width=\
20/40/80mhz-Ceee country="united states2" disabled=no frequency=auto \
mode=station-bridge security-profile=sxt-ap ssid=nycmesh-nn-sxtptp

/interface wireless connect-list
add interface=wlan1 security-profile=sxt-ap ssid=nycmesh-nn-sxptp

# disable the NAT and disable all the firewall filters
/ip firewall nat
set numbers=0 disabled=yes

/ip firewall filter
set numbers=1 disabled=yes
set numbers=2 disabled=yes
set numbers=3 disabled=yes
set numbers=4 disabled=yes
set numbers=5 disabled=yes
set numbers=6 disabled=yes
set numbers=7 disabled=yes
set numbers=8 disabled=yes
set numbers=9 disabled=yes
set numbers=10 disabled=yes

# disable the dhcp-client and server
/ip dhcp-client
set [ find interface=wlan1 ] disabled=yes
/ip dhcp-server
set [ find interface=ether1 ] disabled=yes

#add a bridge and add port ether1 and wlan1 (switch)
/interface bridge
add name=bridge1
/interface bridge port
add bridge=bridge1 interface=ether1
```

```
add bridge=bridge1 interface=wlan1
```

```
#change IP address of the "sxt ptp client" to not mix with potential other SXT default IP  
address
```

```
/ip address
```

```
add address=192.168.88.5/24 interface=bridge1 network=192.168.88.0
```

```
set [ find interface=ether1] address=192.168.88.4/24
```

Legacy Client Node

Set your computer to connect using DHCP ("automatic" on PC)

Connect via ethernet and you will get an address like 192.168.88.xxx

Reset

press the reset button WHILE powering on the unit by plugging in the POE cable.

Once one of the LEDs begins to flash white/blue (about 5 seconds), release reset button while it's flashing. After one minute the device will be ready

Connect to GUI

open your browser and connect to <http://192.168.88.1/>

default username: admin

default password: (leave empty)

Click the button that says "Webfig" in the top right

Name the device

system > identity

"n--". So if your network id is 1000, your device name could be: n1000-sxt-0

Set a password

System > password

IMPORTANT: You must use a unique and strong (at least 8 characters, the longer the better) password to ensure the security of your device!

IP > Services

- Disable telnet
- Disable ftp
- Consider disabling the api and winbox services if you will not be using them.

Other security precautions to consider https://wiki.mikrotik.com/wiki/Manual:Securing_Your_Router

IP > firewall

Find and disable this input rule:

;;; defconf: drop all not coming from LAN

Bridge

- add new
set Protocol Mode to "none"
- hit apply and OK

IP > DHCP Server

disable by clicking the small [D] button

IP > DHCP Client

- change Interface to bridge1
- hit apply and OK

Wireless > security profiles (tab)

add new

name: nycmeshnet

uncheck wpa psk

leave wpa2 psk checked

write in wpa2 Pre-Shared-Key field: nycmeshnet

apply and ok

Wireless > wlan1

Set mode to station-bridge

Set SSID of the hub you want to connect to e.g. nycmesh-xxx

Set channel width to 20/40/80MHz XXXX

Set frequency to auto

Set security profile to nycmeshnet

(below only if you have SXT international version)

Click Advanced Mode button at top

Scroll down and set country drop down to united states

When all settings are correct and the station connects the status should change from "searching for network" to "connected to ess".

Bridge > Ports

Add new, set interface to ether1, set bridge to bridge1

Add new, set interface to wlan1, set bridge to bridge1

IP > Addresses

- Add new, set address to 192.168.88.1/24 set interface to bridge1
- Delete entry 192.168.88.1/24 on interface ether1

Change your computer network settings back to automatic or DHCP

(Note you must be connected to the access point to proceed beyond this point)

Access GUI via routable IP address

Use the name you used for your device, plus the name of the access point to generate the correct URL. For example if your network id is 1000 and the hub id is 500, the URL would be:

`http://n1000-sxt-0.n500.mesh/`

Update (2 step process)

1. system > packages

- enable ipv6
- update / reboot

2. system > routerboard > update
Reboot

Revision #8

Created 9 December 2023 04:39:35 by Willard Nilges

Updated 13 July 2024 22:00:23 by James