



MAC Address Filtering Setup

(3G17Wn)

MAC Address Filtering

MAC address filtering refers to the process of allowing (or denying) access to your wireless network based on the hardware address of the device attempting to connect.*

This Wireless MAC address is usually printed on the underside of the device you are attempting to allow (or deny) access to.



Ensure you are making any MAC address filtering configuration changes from an ethernet connected computer.

If you are not able to do this, remember to add the MAC address of the computer you are making the configuration changes from to the allowed access list.

You will lock yourself out of the wireless network if you do not and an ethernet connection will be required.

* - If supported by your model of modem / router.

Enabling MAC Address Filtering

This guide will take you through the process of enabling MAC address filtering.

1. To find the MAC address of your computer's wireless network card select **Start > All Programs > Accessories > Command Prompt**.
2. Type "**ipconfig /all**" (not including the quotation marks) and press enter.

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\TechSupport>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : techsupport-laptop
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Unknown
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . . :
    Description . . . . . : Broadcom NetLink (TM) Gigabit Ethernet
    Physical Address. . . . . : 00-0F-B0-FA-92-57
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 192.168.20.100
    Subnet Mask . . . . . : 255.255.255.0
    IP Address. . . . . : fe80::20f:b0ff:fefa:9257%4
    Default Gateway . . . . . : 192.168.20.1
    DHCP Server . . . . . : 192.168.20.1
    DNS Servers . . . . . : 192.168.20.1
                            192.168.20.1
                            fec0:0:0:ffff::1%2
                            fec0:0:0:ffff::2%2
                            fec0:0:0:ffff::3%2
    Lease Obtained. . . . . : Thursday, 4 November 2010 1:39:24 p.m.
    Lease Expires . . . . . : Friday, 5 November 2010 1:39:24 p.m.

Ethernet adapter Wireless Network Connection:

    Connection-specific DNS Suffix . . :
    Description . . . . . : Broadcom 802.11b/g WLAN
    Physical Address. . . . . : 00-14-A5-7A-63-EE
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 192.168.20.101
    Subnet Mask . . . . . : 255.255.255.0
    IP Address. . . . . : fe80::214:a5ff:fe7a:63ee%7
    Default Gateway . . . . . : 192.168.20.1
    DHCP Server . . . . . : 192.168.20.1
    DNS Servers . . . . . : 192.168.20.1
                            192.168.20.1
                            fec0:0:0:ffff::1%1
                            fec0:0:0:ffff::2%1
                            fec0:0:0:ffff::3%1
    Lease Obtained. . . . . : Thursday, 4 November 2010 1:42:14 p.m.
    Lease Expires . . . . . : Friday, 5 November 2010 1:42:14 p.m.

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Connection-specific DNS Suffix . . :
```

- Find and record the **physical address** of your wireless network card on your computer. This is the **MAC address** of the wireless network card. Also note the IP address of your wireless network card. It is best practice to make sure your IP address has been statically assigned so that the IP address does not change on restarting either the pc or the router. To set a static IP address please see <http://www.netcomm.com.au/support/frequently-asked-questions/networking-setting-a-static-ip-address>

The recommended IP address details are:

IP address : 192.168.20.101
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.20.1
Preferred DNS: 192.168.20.1
Alternate DNS: 4.2.2.2

- Navigate to <http://192.168.20.1> in a web browser using admin as the default username and password.
- Select **Firewall > MAC / IP / Port filtering**.

The screenshot shows the NetComm 3G17Wn - 3G 3-Port 11n Wi-Fi Router's web interface. The page title is "Firewall > MAC/IP/Port filtering". The "MAC/IP/Port Filtering Settings" section includes a description: "This page allows you to setup MAC, IP and port filtering rules to protect your network from malicious activity. The filtering rules can be used to either allow or block certain users and/or ports from accessing the Internet." Under "Basic Settings", "MAC/IP/Port Filtering" is set to "Enable" and "Default Policy" is set to "Dropped". There are "Apply" and "Reset" buttons. The "MAC/IP/Port Filter Settings" section contains the following fields: "MAC address" (00:14:A5:7A:63:EE), "Dest IP Address" (192.168.20.101), "Source IP Address" (202.121.232.4), "Protocol" (None), "Dest Port Range" (empty), "Source Port Range" (empty), "Action" (Accept), and "Comment" (empty). A note states "(The maximum rule count is 32.)". At the bottom, there are "Apply" and "Reset" buttons and a section for "Current MAC/IP/Port filtering rules in system:".

6. Set **MAC / IP / Port filtering** to enable and change the **Default Policy** to suit – either to accept or deny data packets that do not match the filtering rule you are to create.
7. Enter the **MAC address** of your wireless network card. Enter a colon ":" between each set of two characters as per the example above.
8. Enter the **Destination IP address**, the IP address of the wireless network card of your pc or other wireless network device.
9. Enter the **Source IP address**, the WAN or external IP address from where the data packets originate. If you are unsure of this address enter 0.0.0.0 which represents any IP address.
10. Press **Apply**. The example below highlights the completed rule.

Firewall > MAC/IP/Port filtering

MAC/IP/Port Filtering Settings

This page allows you to setup MAC, IP and port filtering rules to protect your network from malicious activity. The filtering rules can be used to either allow or block certain users and/or ports from accessing the Internet.

Basic Settings

MAC/IP/Port Filtering Disable ▾

Default Policy – The packet that don't match with any rules would be: Dropped. ▾

MAC/IP/Port Filter Settings

MAC address

Dest IP Address

Source IP Address

Protocol None ▾

Dest Port Range -

Source Port Range -

Action Accept ▾

Comment

(The maximum rule count is 32.)

Current MAC/IP/Port filtering rules in system:

No.	MAC address	Dest IP Address	Source IP Address	Protocol	Dest Port Range	Source Port Range	Action	Comment	Pkt Cnt
<input type="checkbox"/>	00:14:A5:7A:63:EE	192.168.20.101	202.121.232.4	-	-	-	Accept		-
Others would be dropped									-

Port Filtering

In addition to Mac / IP filtering the 3G17Wn has the option of port filtering, to allow or deny data packets throughput across designated ports.

The example below highlights an example of port filtering for port 80 (http traffic).

Firewall > MAC/IP/Port filtering

MAC/IP/Port Filtering Settings

This page allows you to setup MAC, IP and port filtering rules to protect your network from malicious activity. The filtering rules can be used to either allow or block certain users and/or ports from accessing the Internet.

Basic Settings

MAC/IP/Port Filtering ▾

Default Policy – The packet that don't match with any rules would be: ▾

MAC/IP/Port Filter Settings

MAC address

Dest IP Address

Source IP Address

Protocol ▾

Dest Port Range -

Source Port Range -

Action ▾

Comment

(The maximum rule count is 32.)

Current MAC/IP/Port filtering rules in system:

No.	MAC address	Dest IP Address	Source IP Address	Protocol	Dest Port Range	Source Port Range	Action	Comment	Pkt Cnt
<input type="checkbox"/>	00:14:A5:7A:63:EE	192.168.20.101	202.121.232.4	-	-	-	Accept		
Others would be dropped									-

If you wish to allow or deny traffic across a range of ports enter the start port and then the end port in both the Destination Port Range and the Source Port Range. In addition you will need to enter the MAC address, Destination IP address and Source IP address in the same way as Mac filtering. The example below highlights a completed port filter rule.

Current MAC/IP/Port filtering rules in system:

No.	MAC address	Dest IP Address	Source IP Address	Protocol	Dest Port Range	Source Port Range	Action	Comment	Pkt Cnt
<input type="checkbox"/>	00:14:A5:7A:83:EE	192.168.20.101	202.121.232.4	-	-	-	Accept		-
<input type="checkbox"/>	00:14:A5:7A:83:EE	192.168.20.101	202.121.232.4	TCP	80 - 80	80 - 80	Accept		-
Others would be dropped									-

You will then need to repeat this process for any subsequent devices you want to allow to access your wireless network.