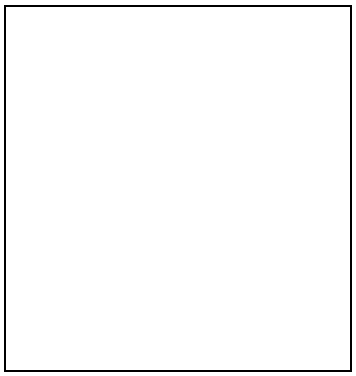
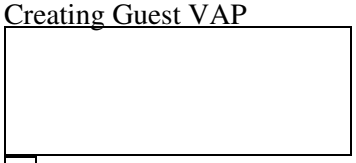
Note: This page must be reevaluated. Please, someone with better expertise should verify that the main dhcp server still works correctly after adding the insulated wlan dhcpd server. Had to hard-reset my router.. main lan/wlan was not assigning any dhcp leases anymore, yet second wlan (guest) had internet working perfectly and good dhcp server. no chance to telnet/ssh... locked out... admin interface not reachable from guest network. Thank you.

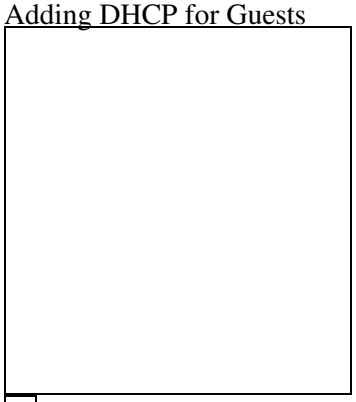
This tutorial is for beginners, and therefore before proceeding make sure you have working reset button and have backed up you configuration (so you can reset your router and restore configuration if you stuck somewhere). This guide will show you the basics of creating and controlling Guest WiFi.



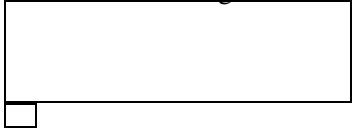
Creating Guest VAP



Adding DHCP for Guests

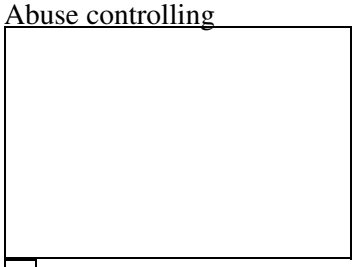


Hardcoded limiting interfaces

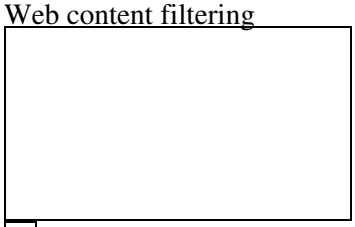


Setting priorities

Abuse controlling



Web content filtering



Content blocked

For that purpose we will first create VAP(Virtual Access point) for Guests .

On **Wireless->Basic Setup** tab click Add on Virtual Interfaces section. **Enable AP isolation** so that guests can not see each others. AP Isolation drops all traffic between clients connected to the VAP. If you want secure Guest WiFI its recommended to enable this feature to help mitigate Wi-Fi snooping attacks.

Set **Network Configuration to Unbridged**, **Enable NAT** (so that guest can have internet). enable **Net isolation** (this option creates a couple of firewall rules that blocks guest to reach your private network). Net isolation works ONLY on unbridged inteface on newer builds, for Broadcom starting from build 23020, for Atheros starting from build 24759 and for Mediatek (Ralink) units starting from build 25934.

AP Isolation = Guests can not hack each other on guest VAP,

Net isolation = Guests can not hack your private LAN+WLAN

Enable Forced DNS Redirection and enter the OpenDNS server IP (208.67.222.222) in the Optional DNS target field. This will prevent users from using their own DNS servers (and hence get around content filtering) by intercepting DNS queries and forcing them to use the DNS servers you specify. Enter the IP Address and Subnet Mask of yours newly created interface (ath0.1) 172.16.1.1./255.255.255.0 Click Save and Apply. Wait about 30 sec. for interface ath0.1 to be created. Note: You still wont be able to connect to this Guest VAP. You must enable DHCP for the clients.

Next step is to **enable DHCPd** for the guest wifi. Go to **Setup->Networking** and on DHCPd section add

another dhcp server for the guest network (click add then choose ath0.1 from drop down menu). select starting IP for guests, max number of IPs and leasetime. Again click Save and Apply. Wait about 30 sec. and try to connect to Guest WiFi. You should be able to browse Internet and shouldn't be able to reach your private network or see other clients on network discovery.

Now, lets do some **bandwidth limiting**. You can put your private network on Maximum and Guest to bulk. The bulk class is only allocated remaining bandwidth when the remaining classes are idle. If the pipe is full of traffic from other classes, Bulk will only be allocated 1% of total set limit. So, basically your guests will not affect your private speed. Or you can set hardcoded limits with manual entering.

With **interface limiting** both bridged & unbridged, offers ability to rate or priority limit services or ports/port ranges. This can be exceptionally useful to control bandwidth hogs, regulate hotspots, etc. with an interface limit, a guest user can change their ip address & mac address as much as they want trying to get around qos, abusive users can't bypass ur rules without switching off the interface.

example such as:

vlan1 512/512 0 ssl manual

^this means all traffic on vlan1 interface (lan ports for some routers, others use eth) is not limited or shaped & goes "up to" global limits, except ssl traffic, being limited to 512kbps both up & down (64KB/s). multiple entries are possible exampled below.

ath0 512/512 0 ssl manual

ath0 2048/512 0 http manual

ath0 512/512 0 ftp manual

^with this, the same applies to what said above, just for the ath0 wireless interface & only the listed services are rate limited. u can also do priority limits, but rate limiting & prioritizing the same service is not supported, one or the other.

You can use Access Restrictions to block torrents and some VPNs. Determined user is very hard to block because nowdays you have free SSTP VPN services etc. On cheap routers you can not run Proxy, Squid etc so this is all we have...

To do some net abuse filtering we will use OpenDNS.

What is OpenDNS?

OpenDNS is a free DNS (Domain Name Server) service which makes internet browsing safer and allegedly faster. By simply using their DNS servers instead of your ISP's you are automatically protected from their list of Phishing websites. However, in order to restrict a variety of adult website content you will need to create a free account with them, register your IP address and select the categories you want restricted (i.e. sexuality, nude, pornography, lingerie, grotesque, etc...). Since most of us have DHCP assigned WAN IP addresses that change periodically we need to instruct our router to tell OpenDNS what our new IP address is when it

changes. See DNS-O-MATIC

Reboot router, clear browser cache, and manually set public dns server in your PC NIC adapter to try to avoid restrictions...