English • Deutsch • Español • Français • Italiano • ??? • Polski • Português • ??????? • Svenska • ???(????)? • ???(??)? •

Contents

Important Note

It Seems that no firmware including ChilliSpot after DD-WRT V24 SP2 SVN 15506 works due to a compilator syntax bug. If you need to use ChilliSpot and if your device support it you should try a firmware release between SVN 14896 and SVN 15506

Brief introduction

Executive summary

ChilliSpot (chilli, chillispot) is a way to

- Easily make the wireless or LAN-connected computers display a "landing page" on users' browsers.
- Redirection occurs on the first Web page, and until the user clicks through (I Agree/Login).
- Optionally earn revenue from your hotspot.
- Provide a Wi-Fi usage agreement, advertising or other neighbourhood or commercial activities.
- Proactive overuse prevention:
- Limit the bandwidth, up and down, hotspot-connected laptops or desktops can use.
- Limit the number of times within a given period hotspot users can log in.
- Other fine-grained limitations.

ChilliSpot can be used for single router, or extended with the use of external services to cover an entire metropolitan area.

Technical description

ChilliSpot is an open source Captive Portal wireless or local area network (LAN) access point controller. It is used for authenticating users. It supports Web-based login, which is today's standard for public hotspots. Authentication, Authorization and Accounting (AAA) is handled by an on-line provider, or a local radius service you provide.

ChilliSpot cannot work alone and needs two (2) additional services, provided externally:

- A Web Portal to which users are redirected. This portal can provide any mean of access control service such as user login, on-line billing, etc...
- A Radius service for authentication and accounting. Most of the time, the Radius server and the Web server will be tightly integrated to offer advanced services.
- There are several on-line providers (ChilliSpot Service Provider, CSP) that have the additional services needed to make ChilliSpot work: See Captive Portal#Provider
- The advantage of a CSP is your ChilliSpot hotspot can operational within minutes.

Chillispot.info Web site is only a copy of the original chillispot.org Web site, without any development. DD-WRT uses an older version of ChilliSpot. ChilliSpot development continued, and it is possible to load the latest release of ChilliSpot into DD-WRT. (more later, in an update to this DD-WRT Wiki article)

Also, CoovaChilli is another entire firmware distribution, based on OpenWRT. It includes the most recent version of ChilliSpot, **but requires changing your router flash and learning a completely new way of setting up the router, especially problematic if you use your router for anything other than just a ChilliSpot portal.** Since this is the DD-WRT Wiki, and not the OpenWRT Wiki, we are not going to cover CoovaChilli here.

Terms and definitions

- DD-WRT device: Your DD-WRT-flashed device!
- ChilliSpot Account: Your [free] account on WorldSpot.net or [[Captive Portal|another online provider of ChilliSpot services[[.

- ChilliSpot Service Provider (CSP): An on-line (Internet-based) provider of the necessary back-end services for the DD-WRT device running ChilliSpot. The major contributor to this Wiki and other authors use Worldspot.net, but other CSP's are available. If you have good success and are familiar with Wiki-editing and Chilli, please update this Wiki with your preferred provider. A list of CSP's is at the bottom.

Prerequisites

- **A DD-WRT-Compatible device programmed with a distribution of DD-WRT containing Chilli.** Highly recommend build 13064 (10/10/09) or the latest BETA. See general flashing instructions elsewhere in the DD-WRT Wiki.
- **For those using a CSP (ChilliSpot Service Provider, see above), the DD-WRT device *must* already have Internet access.**
    - ♦ Check that a wireless laptop is connected through the DD-WRT device and receiving Web pages.
- Important: For easy setup within the scope of this wiki article, Internet should come from the WAN (Internet) port of the router (normal router mode), not from the LAN port (router in AP-only mode).
- **If you are adding the DD-WRT device to an existing private subnet to introduce ChilliSpot services**, and your existing network has a subnet of 192.168.1.X, there is a conflict with the DD-WRT device default LAN subnet. For the specific issue, you must change the DD-WRT LAN IP address to another subnet, like 192.168.2.x.
    - ♦ If you chain your hotspot off your existing LAN, so the ChilliSpot users are a separate, private subnet of your existing LAN, the DD-WRT WAN interface is facing the LAN. It is recommended that you open management interfaces on DD-WRT to the WAN-side so you can control the DD-WRT telnet/ssh/Web interface from your existing network.
- Create a ChilliSpot Account on a CSP.
    - ♦ After signing up, the CSP should show you a convenient customized screen-image displaying the entries for the DD-WRT device.
- **An Ethernet cable** to connect your laptop LAN port to a LAN port on the DD-WRT device.
- **The DD-WRT device's Web Management Interface must work.** You should be able to connect to at http://192.168.x.1/, or whatever LAN IP you have set your DD-WRT device. Later, for memory consumption and performance of the DD-WRT device, the Web Manager's service can be disabled and run only when needed.
- Set-up your DD-WRT device's Wireless LAN, but disable encryption for the Wi-Fi for now. This greatly simplifies resolving issues.
- The simplest instructions here assume your DD-WRT device currently provides your clients a single private subnet. If this sounds technical, it is the default setup of DD-WRT. By factory setup, a DD-WRT device uses 192.168.1.1 as a LAN IP, and all clients are assigned an address automatically of 192.168.1.x. While other configurations are possible, the easiest examples used here assume your DD-WRT device is using the default settings.
- http://192.168.1.1: The assumed LAN IP address of your DD-WRT device's Web Management. If you have changed this number, use the new number.
- **Experts**: When using ChilliSpot *without* using a CSP, you must provide your own **Web Server** to host the redirect Web site and a **Radius Server** for accounting. The Web Server and Radius Server may be installed on the same machine, but generally not the DD-WRT device. Installation and Set-up of ChilliSpot without a CSP is beyond the scope of this Wiki article.
- (old) **V23SP2 Introduces the option of Enabling "Separation of Wifi from the LAN Bridge": having ChilliSpot control only wireless clients.** The existing DD-WRT device settings are only used for the LAN. Clients behave as if the Wi-Fi and LAN connections are separate networks completely.

Most guides including the WorldSpot.net guide, assume this 'Separate Wi-Fi' configuration is Enabled.
However, new configurations are available with this option:

- If you have Secondary Access Points specifically to increase the Wi-Fi coverage, and these SAP's are physically wired into the LAN ports, then **on the main ChilliSpot'ed DD-WRT device, you do not want to 'Separate Wifi from the LAN Bridge'.** Configurations A or B is recommended.
- If you have "public-access terminals" that are wired LAN computers, such as at a library, connected to the DD-WRT device, and you want these clients to now be directed to the ChilliSpot Authentication Splash Page, you also do not want to "Separate Wifi from the LAN Bridge". Configuration A is recommended.
- If you want to maintain a single, homogeneous network [all Internet-connected devices shares the same private subnet], of wireless and wired clients, **and your wired clients have been made secure from wireless attacks** [outside of the scope of this guide], then you do not want to "Separate Wifi from the LAN Bridge". Configuration B is recommended.

Additional prerequisites for older firmware

- Highly-recommended to have firmware build 14929 as the running firmware.
- Firmware V23xx: If you haven't reset to factory settings after installation, do it, then reboot once more.

  Anyone familiar with the V23-series firmware, please change the above point if this is only needed on specific revisions

- Resetting to factory defaults is NOT needed for V24Final and later.

Configuration

After carefully following the above sections:

Three (3) options:

- New Hotspot Introduction: Hang a new DD-WRT device with Chilli, off an existing LAN. Existing LAN is left completely alone. If you have a DHCP server or some custom corporate setup and you don't want to change or alter it, this is the best way.
- One (1) network: Put both the wireless local area network (WLAN) and LAN clients on the Chillspot. This is good for people who want to switch entirely over to ChilliSpot on their LAN and WLAN.
- Two (2) networks: Keep the existing LAN clients on normal services while splitting off the WLAN clients to chilli. This is okay if you already have a DD-WRT box managing services, and you only want the WLAN clients to go to the ChilliSpot portal page.

Configuration A: Add new Chilli-powered hotspot to existing non-DD-WRT subnet

Add chilli hotspot services to an existing network.

The existing network is not changed at all.

All existing clients operate as before.

A connection from the existing network is plugged into the WAN port on the DD-WRT device. Besides changing the DD-WRT device to allow WAN access to SSHd and the Web interface, the steps are nearly identical to "One Network Subnet". New library access terminals, for instance, can be connected to the LAN ports on the DD-WRT device.

Configuration B: One network subnet, move all clients to ChilliSpot

Keep your pre-Chilli setup throughout. Move all clients to Chilli. The LAN ports and Wi-Fi are bridged together and are seen as a single network managed by ChilliSpot.

> Also known as, "Separate WLAN from LAN" - Disable.

It is strongly recommended that before doing this, you should access DD-WRT's Web interface from the WAN port. If you have a configuration problem with ChilliSpot, you will still be able to access the configuration interface.

This setup is mandatory if you want to use the WDS feature (Wi-Fi repeaters to extend the Wi-Fi range)

ChilliSpot has its own DHCP Server. **If "Separate Wi-Fi from LAN Bridge" is disabled, the DD-WRT device's normal DHCP Server must be off.**

Your existing LAN subnet was 192.168.1.x and your DD-WRT device LAN IP was 192.168.1.1. You have a conflict, as DD-WRT's WAN will be your LAN. So you must change DD-WRT's LAN IP to another subnet.

1. From the DD-WRT Web Setup page, change the DD-WRT device LAN IP to another subnet, such as 192.168.2.1 & press Apply.
2. Reconfigure your LAN client with 192.168.2.10, and reconnect to the Administration Web Site of the DD-WRT device on 192.168.2.1.
3. From the Setup (Main page) of the Web Interface, turn off the DD-WRT DHCP Server.

   Now, clients are **temporarily** no longer receiving a DHCP assignment. After enabling and configuration of ChilliSpot (covered later), ChilliSpot will create a virtual LAN interface at 192.168.1.1 and provides DHCP Services again on 192.168.1.x for all your Wireless and Wired clients.

   Enable ChilliSpot options:

1. 1. With build 13064/v24: Services, Hotspot - ChilliSpot section. or
   2. With v23xx: Administration, Hotspot - ChilliSpot section.
2. **DHCP Interface**: select "LAN" this is the bridge between your LAN ports and the wifi.
3. Fill in the information provided by the CSP
4. Enable ChilliSpot
5. Continue on to the next section, "ChilliSpot setup, detailed options".

Configuration C: Existing DD-WRT router, ChilliSpot manages only Wi-Fi clients. The existing LAN, after some interruptions, operates as before (same IPs, DHCP services)

Two Networks, Wi-Fi separated from LAN. Existing DD-WRT device as a Router, adding ChilliSpot duties

> Example: the existing DD-WRT set-up uses 192.168.1.0/24 as the IP range and the DD-WRT device is at 192.168.1.1. Substitute your own numbers if there is a difference.

1. "Separate Wi-Fi from the LAN Bridge" ? ENABLE
2. Enable ChilliSpot
3. For build 13064 (10/10/09), **DHCP Interface** - leave at LAN. Older builds may have to select WLAN.

> The previous three steps create a configuration called "Bridge Separation". It makes ChilliSpot control only your DD-WRT device's wireless/Wi-Fi. The LAN continues to function without being diverted to ChilliSpot, just as before. Your LAN ports are also inaccessible by the Wi-Fi-connected computers.

Configuration D: Extend the network to regular neighbours and momentary roaming users (draft)

The actual instructions presented have not been polished in their formatting and presentation. And some additional testing is required (2011-12-06... having a bit of difficulty getting it working properly)

A DD-WRT box performs two functions ? both an access point (AP), and a ChilliSpot in this example.

Like the other examples above and by the main author of this wiki, Configuration D is written and done with actual hardware and a successful, stable setup, running DD-WRT, in this case WHR-HP-G54 Buffalo-brand routers. For this case, there is a 50/10 backhaul (megabits) over VDSL2, a main wired LAN and a/n 5ghz separate wireless provided directly from the VDSL2 box (not DD-WRT). The particular model of DD-WRT-enabled box could not handle that level of traffic due to hardware limitations. A dedicated VDSL2 Fritzbox 7570 handles DSL conversion, connection to internal servers, and telephone devices. The DD-WRT box functions as a passthrough device to provide wide-coverage signal for regular neighbours who need more than what ChilliSpot provides, and casual users who only need to operate as clients, to check email for instance. Heavy wireless traffic goes directly through an 802.11a/n 5ghz signal provided directly from the Fritzbox 7570. This solution is an excellent way to provide secondary services to widespread users. A dedicated, modern DD-WRT box could potentially provide all network services and main routing functions, however, in this case a good quality router is rented directly from the telephone company and does the job.

All existing clients operate as before.

The desire is to have an added, encrypted WLAN signal, and add Chilli also as a second WLAN signal. Only some of the *possible* reasons for the configuration are:

1. Allow casual roaming users 15 minutes of access AND
2. Introduece the policy of the encrypted WLAN with the Chilli splash page WHILE
3. Having local, non-roaming users, approach the hotspot operator physically and hand over donations to

access the primary direct-to-backhaul, encrypted WLAN signal:

1. Locals like cash and no specific logins.
2. UPNP and port forwarding available: UPNP is blocked by Chilli (currently)
3. Burst access: No limitation to bandwidth. Operator must trust each user to not hog bandwidth.
    1. Collect the emails of every user and all MAC addresses. If one is hogging bandwidth uncontrollably, email the other users and change the encrypted SSID password.
4. More private: Encryption WPA2-AES for local regulars.

4. You may have your own reasons!

Hardware

WHR-HP-G54

DDNS: opendns.com (restricts, *e.g.*, pornosurfing through Chilli), provides dynamic DNS services more reliable than dyndns imho
DD-WRT Build: 14929

The rest of this Configuration D text is a DRAFT format. There are some persistent issues yet. As more practical experience is gained and more time is possible to edit this, the text will be "dressed up". For now, it is raw text.

Latest tip: Hook the backhaul (local LAN) cable into a LAN port, and patch over to the WAN port. This has not been verified ? and it seems the source is the need to be able to configure chilli to pull network from the LAN instead of the WAN interface.

```
These are the direct notes for setting up a chilli router with a private,
encrypted wlan cloud as an alternate. The chilli cloud gets 15 minute
access per day per client. Visit worldspot.net and set up your account.
access points and profiles there before doing any of the following.
```

Please note, if the upstream Internet has "died" for any reason, it can take the hotspot *five (5) minutes* to get a new upstream Internet address. If you have not waited *five (5) minutes*, please do so now.

If you have performed a complete reset on the router, OK, otherwise push and hold the button for 30 seconds or perform a Factory Reset from the Web interface, then:

Use a LAN cable, not wireless, when doing any of this! Plug into a LAN port on the DD-WRT box. If your main LAN Ethernet IP address is not already 192.168.1.x, must manually add an IP to your LAN card to be something like 192.168.1.5, temporarily to be able to connect. Leave your existing IP, as we are going to use that also, later.

Presumptions: your local LAN operates on 192.168.2.x with 192.168.2.8 as the main router for LAN-->ISP. Alternate these for your specific setup. Usually I set the main LAN to be something other than 192.168.0.x or 192.168.1.x as it seems almost all new or reset router devices have that as a default IP, and I don't want them to conflict with the main LAN. I also like to make the main router something other than x.x.x.1.

If your main LAN is 192.168.1.x and your main router is 192.168.1.1, DO NOT plug your main LAN into the DD-WRT box at all; only plug your laptop into the ports on the DD-WRT box as indicated until you have decided on substitutes for the DD-WRT box IPs.

Plug in your LAN cable from the laptop into a LAN port on the DD-WRT box.

Start, Run... http://192.168.1.1 or open the address in the Firefox browser.

IMPORTANT: Leave all settings alone unless they are specifically mentioned below.

Main DD-WRT box page: Make your new login and password. For now, use "root" and a password of your choosing.

Setup, Basic

Connection type: Static IP (this points to the private LAN main router) WLAN IP 192.168.2.1, SUB 255.255.255.0, GW 192.168.2.8 (IP of main VDSL2 router) & DNS1 of 192.168.2.8, DNS2 4.2.2.4 (or other suitable secondary DNS)

Router name: Chillibrains or something useful to help you remember Host Name: chillibrains Domain: local

Network setup

Router IP: 192.168.1.1 (this is the default IP, and for LAN-port access. It must be a different subnet than the WAN IP above! And different than the ChilliSpot subnet!) (for now, we will continue to use 192.168.1.1... later-on change this if you wish)

DHCP Server: Disable (chilli has its own dhcp module)

Time settings

Server IP: 192.168.2.5 (local server IP) or 0.pool.ntp.org

Click SAVE, wait a second. Do not apply or reboot yet.

Setup, DDNS

(we are using DNSOMATIC, part of opendns) DDNS Service: Custom DYNDNS Server: updates.dnsomatic.com / or for DynDns.org members.dyndns.org User Name: your username Password: your password Host Name: all.dnsomatic.com / or for Dyndns.org yourdomainname.dyndns.org URL: /nic/update? Additional DDNS options: [none for dnsomatic] / or for Dyndns.org try: --dyndns_system dyndns@dyndns.org --ip_server_name ip1.dynupdate.no-ip.com:8245 / (DynDNS service has had a problem with a non-reachable (down) checkip.dyndns.org)

Click SAVE, wait a second. Then click: MAC Address Clone: (optional) 12:34:xx or your chosen MAC 12:34:xx or your chosen MAC (Here we are only changing the first two number sets for setup.)

Click SAVE, wait.

Wireless, Basic Settings

Wireless Network Name (SSID): PrivatWLAN (Or your wireless cloud name for private LAN access.) Wireless Channel: 13 Sensitivity Range: 0 (suggested) (optional G-only) (This affects BOTH WLAN clouds)

Click SAVE, wait a bit. Click Add interface: 15minWLAN AP isolation Enabled Network configuration (leave at) bridged.

SAVE

Wireless security

WPA2 Personal (WPA2-AES) for the primary WLAN NO SECURITY for the secondary (chilli) wlan. SAVE

Back to: Setup, networking Create bridge (ADD), Bridge 0 name br1, SAVE IP Address 192.168.181.0/255.255.255.0 SAVE Assign to bridge> Assignment 0: br0 interface eth1 Assignment 1: br1 interface wl0.1 You might have to toy with saving the settings a few times to get all the correct bridges to appear. SAVE

Wireless, advanced settings

[note these settings are specific to your radio. add or change as necessary] Wireless TX power will be at 28, I set to 251 and later the startup commands set higher. (Only the WHR-HP-G54 with hardware mods.) You can turn off Wireless GUI access for security if you like... Shortslot override Short Preamble Auto Frame burst disable Afterburner disable --- Scroll down to "Wireless Multimedia Support Settings" WMM support. Turn this off. Seems to work poorly with multiple clients connected (on the WHR-HP-G54). Click SAVE, wait a second.

Services, Services

Disable ttraff to save RAM WAN Traffic Counter: Disable Click SAVE, wait.

Services, Hotspot

ChilliSpot: Enable Separate Yes, br1 Primary Radius: radius.worldspot.net Secondary Radius: radius2.worldspot.net "Remote Network": net 192.168.182.0/24 (This is the same thing as the "net" declaration) DNS IP (OpenDNS primary): 208.67.222.222 Redirect URL: https://secure.worldspot.net/wk/Uam (secure is the europe one, secure2 is the north american server.) The above Redirect URL is *CASE SENSITIVE* and must be entered exactly as shown above, in the box). Shared Key yoursharedkeyfrom worldspot Radius NAS ID: yourradiusnasid from worldspot UAM Secret: your UAM secret value from worldspot UAM Any DNS: 0 (leave at default) UAM Allowed: www.paypal.com,www.paypalobjects.com,paypal.112.2o7.net Additional ChilliSpot Options: domain local dns2 208.67.220.220 dynip 192.168.182.128/26 uamallowed 66.211.168.0/24,64.4.241.0/24,216.113.188.0/24 uamallowed 88.221.0.0/16,84.53.0.0/16,67.133.200.0/22,72.246.0.0/15 uamallowed 216.52.17.0/24,70.42.134.0/24,128.242.125.0/24 Click SAVE, wait. (dynip is **not neccessary**, as there are no static IPs in the same subnet as chilli in this tutorial)

Security, Firewall

Uncheck "Filter multicast" and "Filter ident." and "Filter anonymous ping" SAVE, wait.

Access restrictions, WAN access

Status: Enable Policy Name: Block164x Deny (this means Internet access...) *** SCROLL DOWN CLICK "SAVE" *** Save, wait a second... *** scroll back up *** Edit list of clients Enter the IP Range of the clients 192.168.164.2 ? 192.168.164.254 Block access from all IPs of 2 through 254. SAVE, then CLOSE

The goal is to block all computers that are not using ChilliSpot attempting from using the main subnet router directly on 2.x. Chilli blocks unauthorized access on the 182.x range, but not on the upstream WAN side of

2.x / Note: Otherwise, manually-configured wireless clients could potentially use a 2.x address to get online outside of chilli, crowding out other clients. [This theory is still being tested. Your results may vary.] SAVE then CLOSE SAVE

(We perform the next step NOW to make sure the DD-WRT box is accessible from the WAN port)

Administration, Management

Web Access: Uncheck Protocol HTTP (Do not auto-load Web management interface) Disable Info Site Remote access: Web Gui management enable web gui port 80 Telnet enable

CRON (Reboot periodically, 2x a month, at 2 a.m. on the 1st and 15th. addresses leaks.) 0 2 1 * * root /sbin/reboot 0 2 15 * * root /sbin/reboot

IP Filter Settings

4096 TCP Timeout 500 UDP Timeout 90

Click SAVE, then wait.

NAT QoS, QoS

W/VDSL2 50/10: (we split the bandwidth here between internal use and external users. **External users** are DD-WRT box primary WLAN cloud + ChilliSpot users.) 2500 / 25000 SAVE Select: http, click Add Skypeout, Add SkypetoSkype, Add Set http Express, Skypexxx protocols Premium (can add others here like NTP, DNS, RSTP)

Don't be surprised if the router locks out here for a bit. Wait. You may have to reboot it then plug into the WAN port, and communicate with it over the WAN IP. To restart the management Web interface, telnet into it, and run 'httpd' and continue..

Save, wait a second.

Administration, Commands

1. fixes bug with ChilliSpot and MTU

/usr/sbin/iptables -t mangle -A POSTROUTING -p tcp --tcp-flags SYN,RST SYN -m tcpmss --mss 1441:65535 -j TCPMSS --clamp-mss-to-pmtu Save Firewall. ---

Startup

1. enables WOL from Internet
2. ip neigh change 192.168.178.5 lladdr 00:1B:21:02:EE:4F nud permanent dev br0
3. ip neigh add 192.168.178.5 lladdr 00:1B:21:02:EE:4F nud permanent dev br0
4. turns on noack (optional)

wl noack 1

1. increases power to maximum (only on WHR-HP-G54 Buffalo/updated routers with hardware modification)

wl txpwr1 31 Save Startup

ChilliSpot setup: detailed options

- **RADIUS Server 1** As assigned by CSP. the name or IP address of the primary RADIUS server.
- **RADIUS Server 2** As assigned by CSP. the name or IP address of the secondary RADIUS server.
    - ♦ If you have only one Radius Server, leave as 0.0.0.0 or specify the same field value of Radius Server 1.
- **DNS IP** Your Internet provider's 1st DNS Server. This is available on the DD-WRT device Status page.
- **Remote Network** [1] (AD20110108: bug noted, option missing in build 14929)

    ◊ For One Network, change the default to 192.168.1.0/24, or your old subnet.
    ◊ For Two Networks, it's 192.168.182.0/24 here by default.
        - One could choose something else, like 192.168.155.0/24, so long as it is not the existing DD-WRT LAN subnet.

- **Redirect URL** As given by your CSP. The address of the UAM Server, the Web authentication portal.
- **Shared Key** As given by your CSP. It's also called your RADIUS secret password
- **RADIUS NAS ID** As given by your CSP. The RADIUS name of your Hotspot
- **UAM Secret** is a secret password between the Redirect URL and the Hotspot. Given by the CSP.
- **UAM AnyDNS** Allows Clients to use their own DNS servers. Allows ANY traffic through port 53. Only set this to 1 if you know what you are doing, and can reconfigure IPTABLES properly!
- **UAM Allowed** is a list of Web sites that unauthenticated users are allowed to access.
- **MacAUTH** Enabled or Disabled. Allows authentication of clients by their WLAN or LAN card MAC (hardware) address. Not used in this guide.
- **Additional ChilliSpot Options**
    - ♦ If your local domain is 'local', then
      `domain local`
    - ♦ Your provider may offer another, optional setting for domain.
    - ♦ If your second Internet provider's DNS is for example 4.2.2.4, then for redundancy
      `dns2 4.2.2.4`
    - ♦ To tell ChilliSpot to limit DHCP addresses to be part of the entire subnet:

        - `dynip 192.168.1.128/26` [2]
        - Can be most helpful in a 'one network' subnet setup.
        - Allows fixed IP's to exist from 192.168.1.2 through 127 for your existing devices.

- Apply Changes/Save, and if needed, reboot your DD-WRT device.
- Your ChilliSpot Hotspot should work now. If you tested your wireless client device before setting up ChilliSpot, right-click and 'Repair' the Wi-Fi connection in XP to get a new ChilliSpot-provided IP address.

[1] Remote Network is the same as the `net` command, found on the Internet, elsewhere in references to ChilliSpot configuration and chilli.conf. `net` defines the ChilliSpot network. In DD-WRT, the field is called Remote Network, but it is the same setting as `net`.

[2] `dynip` configures ChilliSpot to use a limited range of IP's within the `net` parameter, as the client DHCP

pool, instead of using the entire `net` range. In this example, address assignments from 192.168.1.128 to 192.168.1.191 are assigned to clients. IP's from 2 through 127 are left for fixed assignments, and can be further specified by `statip` if DHCP clients come on the network needing a specific address from the ChilliSpot DHCP service.

Tips

If you are not knowledgeable about your LAN security, or have poorly configured insecure XP devices on your LAN, to reduce possible attacks from wireless clients, you can enable the option: "Separate Wi-Fi from the LAN Bridge" (your LAN won't be visible to wireless clients). If you are certain your LAN is configured as secure, which it should be anyway, and you want to have access to your LAN equipment from your Wi-Fi, then leave "Separate..." Disabled.

- ChilliSpot will not start unless it can see the DNS Server specified the ChilliSpot settings.
- Note that after reboot, it can take a certain time before a wireless client receives an IP address. Don't forget to switch back to automatic IP assignment (DHCP) on your client when testing!

Troubleshooting

Your client gets a ChilliSpot IP, but no welcome page, or certain Web sites don't open (MTU Bug)

Maybe you are using a PPPOE modem and you are experiencing the MTU bug?

Add this to your Firewall Commands (Administration tab in the Web Interface, Commands sub-tab): Changes MSS to fit inside ChilliSpot tunnel. Important so some Web sites work properly, otherwise "MTU Bug"

```
/usr/sbin/iptables -t mangle -A POSTROUTING -p tcp --tcp-flags SYN,RST
SYN -m tcpmss --mss 1421:65535 -j TCPMSS --clamp-mss-to-pmtu
```

More information in this forum post

ChilliSpot fails after a while, **memory full on router** on low-RAM units

This is a common problem when the infrequently-used Web Interface (httpd) is left running.

- On a hotspot (DD-WRT device) with 16 (or less) megabytes of RAM, the *chilli* process uses 19%.
- The Web Interface process, httpd, uses 19% also. About 3 megabytes!
- Newer builds of Chilli are supposed to use less RAM, although DD-WRT may not have these yet.
- The Web Interface uses a lot of RAM, and in any case, should not be left running on a production router.

Solution 1: SSHd (run HTTPD only when necessary)

This is most suitable when no secured or direct, wired connection to the hotspot is available. or the hotspot is to be administered over the Internet. In this case, an encrypted tunnel is desired to administer the hotspot.

1. On the hotspot Web onterface, go to "Services, Services, Secure Shell", and turn on SSHd, and turn off Telnet.
2. On "Administration, Management, Web Access", turn off HTTP Access (httpd).
3. Make sure access to the hotspot WAN port is available if your setup is *Configuration A: Hotspot Only.* (See above)
4. Save/Apply/Reboot as needed.

To use the Web Interface:

1. For *Configuration A*, physically plug your laptop into the existing network.
2. For *Configuration B* or *C*, physically plug your laptop into a LAN port on the DD-WRT device.
    1. Open your browser and log in to the ChilliSpot page as if you want to use the Internet, as Chilli's firewall rules will block your client from connecting to the DD-WRT device/hotspot otherwise.
3. Putty (SSH) into the DD-WRT device.
    1. The command may look like "putty 192.168.182.1" or
    2. "putty 192.168.182.1 -P *60000*", where *60000* is the chosen port number, if you changed the SSH port.
4. Enter "httpd". (The command to restart httpd is different on older versions of DD-WRT (v23sp2))
5. Open the Web Interface address on your client's browser.
6. When you are finished, enter "killall httpd".

Solution 2: Telnetd alternate, in place of SSHd. Added: 2009.11.11

Telnetd uses less RAM than SSHd, however it is a completely insecure (clear-text) method to connect to the hotspot.

The solution requires a direct, wired connection to the hotspot for administration.

1. Bring up the Web Interface of the DD-WRT device.
2. In "Administration, Management, Web Access", turn off HTTP Access (httpd).
3. In "Services, Services, Secure Shell": Turn off SSHd.
4. Scroll down and turn on Telnet (telnetd).
5. **Save changes**

To use the Web Interface:

1. Make sure your workstation or laptop data is secure to the hotspot.
    1. Anyone who can monitor the traffic can see the root password sent to the hotspot
2. From a cmd prompt (Windows) or Linux: "telnet routerip"
3. Enter "httpd" (only current versions of DD-WRT. v23sp2 requires a different command to start HTTPd.)
4. In your browser: http://routerip. Log in.
5. When finished, at the telnet prompt type: "killall httpd" <enter>

Use the "top" command to check memory usage

After using *Solution 2*, here is the "top" output:

```
Mem: 9012K used, 3992K free, 0K shrd, 1136K buff, 2836K cached CPU: 0.1%
usr 2.9% sys 0.0% nic 96.8% idle 0.0% io 0.0% irq 0.0% sirq Load average:
0.72 0.29 0.10 1/22 778
PID PPID USER STAT VSZ %MEM %CPU COMMAND

 417   214 root     R     1184  9.0  0.4 top
 500     1 root     S     2500 19.1  0.2 chilli -c /tmp/chilli.conf
 157     1 root     S     1176  9.0  0.2 telnetd
 210     1 root     S     1660 12.7  0.0 pppd file /tmp/ppp/options.pppoe
 211     1 root     S     1504 11.5  0.0 /tmp/ppp/redial 30
  14     1 root     S     1504 11.5  0.0 watchdog
   1     0 root     S     1468 11.2  0.0 /sbin/init noinitrd
 454     1 root     S     1460 11.1  0.0 process_monitor
 221     1 root     S     1460 11.1  0.0 ttraff
 739     1 root     S     1460 11.1  0.0 wland
 214   157 root     S     1196  9.1  0.0 -sh
 511     1 root     S     1176  9.0  0.0 syslogd -R 192.168.xxx.xxx
 515     1 root     S     1176  9.0  0.0 klogd
 505     1 root     S      820  6.2  0.0 inadyn --input_file /tmp/ddns/inadyn.conf
 756     1 root     S      692  5.3  0.0 igmprt
  10     1 root     SW       0  0.0  0.0 [mtdblockd]
 545   505 root     Z        0  0.0  0.0 [sh]
   2     1 root     SW       0  0.0  0.0 [keventd]
   6     1 root     SW       0  0.0  0.0 [kupdated]
   3     1 root     SWN      0  0.0  0.0 [ksoftirqd_CPU0]
   4     1 root     SW       0  0.0  0.0 [kswapd]
   5     1 root     SW       0  0.0  0.0 [bdflush]
```

DD-WRT Firmware: Administration/Hotspot/ChilliSpot tab does not show

Make sure you are using a package that includes ChilliSpot. ChilliSpot is not in the micro and mini versions of dd-wrt (consult this table).

Connection Failed on v24-SP2 Firmware(from SVN 14896 to SVN 15506)

if your settings seems to be correct but ChilliSpot don't start. It could come from a too long uamallowed list. Don't put more than three doamin name in this field. If you have more domain to add leave the Uamallowed field empty, and add your uamallowed domains in "Additional ChilliSpot Options" field.

Connection Failed on v23 Firmware

If your client does not recieve a ChilliSpot IP address you may have changed the ChilliSpot DHCP Interface. On older versions of DD-WRT Firmware, touching this setting breaks ChilliSpot. A fix is to reset to factory defaults and re-enter all your settings or use newer firmware.

If the UAM Secret you entered in ChilliSpot Settings is incorrect, you will have an authentication failure.

If the RADIUS Shared Secret is incorrect, the login process will hang.

More troubleshooting tips

If it does not work, you must connect with ssh or telnet to your router.

```
login: root
password: <your password>
```

First, check that you have Internet access:

```
ping google.com
```

Worldspot Users: If you don't have any ping return, check the output of "ifconfig" and post it on the WorldSpot forum.

If Internet works from your router, but you don't have ChilliSpot working, check first that the chilli process is launched with

```
ps -ef
```

You should see a "chilli -c /tmp/chilli.conf" process. If not, recheck your ChilliSpot settings. For example, if you put a whitespace in the NAS ID, the chilli process won't launch.

For the FON Hotspot

Please see the FON Hotspot page for a guide and advice on setting up a FON hotspot using DD-WRT and ChilliSpot.

External Links

- www.chillispot.info

Some ChilliSpot Service Providers (CSPs):

- Worldspot.net
- Hotspotsystem.com
- Yzy-oui-fi.com
- Wifigator.com
- EngageHotspots.com
- Signifi.org, India