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

0-9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Contents:

References ? External links

0-9

802.1x Extensible Authentication Protocol

An advantage of the EAP architecture is its flexibility. EAP is used to select a specific authentication mechanism, typically after the authenticator requests more information in order to determine the method. Rather than requiring the authenticator to be updated to support each new authentication method, EAP permits the use of a backend authentication server, which may implement some or all authentication methods, with the authenticator acting as a pass-through for some or all methods and peers. - (paraphrased and exerpted from the Internet Engineering Task Force's RFC 3748 [1])

802.11b

Channels 1 to 14 (depending on country) in the 2.4 GHz range. Supports transfers up to 11 megabits per second under ideal conditions. Transmission occurs over 20 MHz of bandwidth, but channels are only spaced 5 Mhz apart, so you need to leave gaps. This was ratified by the IEEE in 1999.

802.11a

This is the original 5 GHz standard. It used a different method of transmission known as OFDM allowing it to reach 54 megabits per second under ideal conditions. It requires a radio capable of transmitting in this range. This was ratified by the IEEE in 1999.

802.11g

This 2003 update of the 802.11 standard uses the same channels in 2.4 GHz frequency band of 802.11b, but adopted the OFDM model of 802.11a so it also supports transfers up to 54 megabits per second under ideal conditions. 802.11g equipment can typically operate in 802.11b mode when required to work in 802.11b environments. Like 802.11b, channel spacing is required.

802.11n

This is an extension of both the 2.4GHz and 5 GHz standard that uses newer technologies to increase both speed (up to 600 Mbs) and range. It requires newer equipment and generally have multiple antennas to take advantage of the MIMO features. Unless configured otherwise, the systems will generally fall back to slower speeds to maintain compatibility with 802.11a/b/g clients. One interesting feature of 802.11n is to double the

bandwidth to 40MHz. For general information on using DD-WRT with 802.11n routers, see Wireless-N Configuration. The specification was finalized in 2009.

802.11s

This is a draft of IEEE Standards for Wireless Mesh Networks. See IEEE 802.11s and Status of Project IEEE 802.11s.

A

Access Restrictions

(This entry needs your help.) This mode permits you to restrict access on the basis of time, protocol, or destination. **DOES NOT WORK WITH CLIENT BRIDGE -- USE CLIENT MODE INSTEAD**

Ad hoc

Ad hoc mode, one of the least popular modes, allows the router to connect to other wireless devices that are also available for ad hoc connections. Think of this mode as a Client Mode that doesn't connect to infrastructure networks but rather connects to other ad hoc configured devices. Ad hoc networks lack the central management that is typical of an infrastructure type network. Ad hoc mode doesn't use WDS but it does make use of STP.

Afterburner

Afterburner, also known as SpeedBooster, SuperSpeed, TurboG, 125mbps, HSP125, and G+ is a feature built into some routers that theoretically increase throughput through use of software, or firmware

Main article: Afterburner

Access Point

The default and probably the most common mode. The Access Point mode allows wireless clients to access the Internet, access each other wirelessly, or access other computers that may be connected to the switch with wires. A router in Access Point mode cannot connect wirelessly to other routers, but it can have other routers connected to it wirelessly as clients or repeaters. Access Point is the mode used when configuring a router to act as a repeater.

B

Basic Service Set Identifier

The MAC address of an Access Point.

See Also: Extended Service Set Identifier

Boot Wait

Boot Wait is a feature you will hopefully never need. It introduces a short delay while booting (5 seconds). During this delay, you can initiate the upload of a new firmware image, usually with TFTP or Telnet, providing flash ROM is not completely broken. This is only necessary if the installed firmware will not boot or you cannot use the upload routine in the DD-WRT GUI. The default and recommended setting is "Enable". You can access the Boot Wait setting by going to "Administration" > "Management". For more info, see the topic **Is your router bricked?** in Peackock Thread in the Broadcom Forum.

Border Gateway Protocol

Border Gateway Protocol (BGP) is the core routing protocol of the Internet, generally used by Internet Service Providers to establish routing among each other. It is also used on private networks to "multihome".

Brick

1. Improperly flashing one's WRT54G(S) in a way that renders it unusable
2. To cause to resemble a brick, in mode of operation as well as form
3. To render inert like a rock, or a brick, or ... well you get the general idea

See Also: Recover from a Bad Flash

BSSID

See: Basic Service Set Identifier

C

Captive Portal

A captive portal is a wireless access point which only permits internet access to authenticated users, utilizing either DNS or HTTP spoofing and redirection to divert any user whose MAC address it has not authenticated to a local login page, or a walled garden.

Once you've logged in, the portal will disable the redirection, permitting whatever traffic it allows to pass unmolested to the actual target servers.

Captive portals work well in an environment where the users are utilizing traditional computing devices like laptops, where a web browser is the primary access software; they can cause problems for less capable devices, like dedicated SIP phones, which have no way to access the authentication screens.

CFE

Common Firmware Environment (CFE) is a firmware interface and bootloader developed by Broadcom for 32-bit and 64-bit system-on-a-chip (SOC) systems. It is roughly analogous to the BIOS on the IBM PC platform. (thanks to Wikipedia)

It is part of the flash memory that is not changed when updating the operating firmware in the router and vital for booting the router.

ClickJacking

Clickjacking occurs when a user a user accidently clicks on a invisible link which leads the person to a malicious site without their knowledge. This is possible due to the design feature in HTML which lets websites embed content from other sites. This means that every website is vulnerable.

"See Also:" How to prevent ClickJacking

Chillispot

Chillispot can be used for hotspot management. It requires a separate web server to host the redirect URL and a separate radius server (these may be installed on the same machine, of course).

You can also use a hosted Chillispot portal like http://worldspot.net which is free. It replaces both your radius server and your web server, and brings powerful features. You simply register there and create your hotspot. Then you can get the Chillispot configuration settings to enter in the steps below, and you can get your hotspot working in some minutes.

Main Article: Chillispot

Client

Think of work. Clients would be "regular" employees, and a server would be a supervisor. Clients perform lower level tasks (printers, workstations, etc.) while the server performs higher level tasks like delegating (print jobs, ip addressing, Domain name resolution). So think of if you were at work and need 5,000 nails, 2 hammers, 50 2x4's, and 2 carpenters to make something. You do not have the resources to obtain this (client), so you ask your supervisor (server), and the supervisor has the power to get these resources for you to finish your job.

Clients are end devices. Workstations, printers, pda's, cellphones, and most other end devices are clients. Servers are designed and configured to perform tasks that multiple clients need.

Client Bridge Mode

Client Bridge Mode is much like Client Mode except the WLAN and the LAN are on the same subnet. Consequently, NAT is no longer used and services (such as DHCP) that are running on the original network will work seamlessly on the bridged network. Just as in Client Mode, a router in Client Bridge Mode will not accept wireless clients and it will not broadcast beacons. (Note: A technical problem exists in client bridge mode. It appears that this mode is not a fully transparent bridge mode as MAC addresses of packets that pass through the Client Bridged router from behind the client bridged router are rewritten to use the MAC address of the client bridged router. (Sorry, I couldn't think of a more confusing way to write it.) If you really need transparent bridging, consider using WDS bridging instead.)

See Also: Wireless Bridge

Client Isolation Mode

Limits the clients to communicate only with the AP and not with other wireless clients (usually set on hotspots).

Client Mode

Client mode (also referred to as 'AP Client' mode) allows the router to connect to other access points as a client. In a nutshell, this turns the WLAN portion of your router into the WAN. In this mode, the router will no longer function as an access point (doesn't allow clients), therefore, you will need wires to use the router and to configure it. The router won't even be visible to your wireless configuration software or Wi-Fi sniffer software such as Netstumbler, since it no longer broadcasts beacons. In client mode, the WLAN and the LAN will not be bridged, thus they will be on two different subnets. Port forwarding (from the WLAN to the LAN) will be necessary for FTP servers, VNC servers, etc. that are located behind the client mode router to function properly. For this reason, most users chose to use client bridge mode instead of client mode.

See Also: Client Mode Wireless

Connection Watchdog

This is a feature found in most DD-WRT versions, which hopefully you won't need. When configured the router will ping one (or more) other computers and if it can not reach them it will automatically reboot it's self. This provides a crude way to work around situations where the router becomes wedged.

cPanel

cPanel is a Web Hosting Control Panel used to control different aspects of a hosting account. It can also be defined a Graphical interface to manage your hosting account. It is available for both Windows and Linux Server.

"Also see:"How to install cPanel on Linux Server

Cron

Normally called crontab, the cron subsystem is a type of scheduler for Unix/Linux that runs given commands at designated times. The default and the recommended setting is "enabled" since processes such as "Watchdog Scheduler" depend on it. You can access the Cron setting at "Administration" > "Management".

D

Daemon

In Unix/Linux, a daemon (or dæmon) is a background process. Typically, daemons have names that end with the letter "d". For example, syslogd is the daemon which handles the system log. Another example is sshd, which handles incoming SSH connections.

Demilitarized Zone

A DMZ host is generally one selected device or computer on the network where all incoming traffic without a designated destination defined by PAT or port forwarding, is forwarded to. Using a DMZ host is a lot like turning off the firewall capabilities inside your router and letting the DMZ host device handle all uninvited incoming traffic. For this reason, having a computer as a designated DMZ host can be a security hazard. DMZ is disabled by default in DD-WRT firmware. You can change DMZ settings by going to "NAT / QoS" (or "Applications & Gaming") -> "DMZ".

Domain Name

A domain name is a human-readable label for an IP address on a computer or device; it is translated into an IP address (usually) by recursively querying DNS servers starting at the root of the Domain Name System.

Domain Name System

DNS converts human readable domain names into a format the computer and network can understand (IP addresses), and vice versa.

DNS Forwarder

Will forward any DNS request, to a DNS server of your choice (i.e. your ISP's); useful, for configuration/speed issues. Also known as a "recursive server".

DNS Server

DNS servers are the servers responsible for resolving names to IP addresses. When you point your browser to yahoo.com, a DNS Server has to resolve yahoo.com, (that is, look up the corresponding IP address) before the page is actually retrieved, since computers and networking equipment communicate using IP addresses instead of domain names. DNS servers are built into routers, but they are only a local caching server that works in tandem with your LAN's DNS server(s) and/or your ISP's DNS servers.

DNSmasq

DNSmasq is a piece of software often bundled into versions of DD-WRT. The name is, presumably, meant to suggest that it does DNS masquerading. DNSmasq provides DNS service to your LAN and like most DNS servers it will look to an up stream DNS servers to resolve questions you ask it. Optionally you can can configure it so it can answer a few DNS queries for a few local machines.

Dynamic DNS (DDNS)

Dynamic DNS is a generic term for a service that is hosted outside of your network to provide valid DNS responses to the Internet at large for your computer, hosted on a consumer IP connection with a dynamic IP address. Dynamic DNS servers are located on server computers with static IP addresses, as all DNS servers must be.

In order to take advantage of this service, devices (such as routers or computers) will require a client "updater" software to be installed to pass authentication and account information, and the network's current Internet IP address, in a timed manner.

Many users want to be able to connect to another network (such as their home or office network) from another location but aren't able to connect unless they know the Internet IP address of that network. Because most ISPs provide IP addresses through DHCP (or charge extra for a static IP address) your IP address may change on occasion. Dynamic DNS is a system that allows you to assign a domain name to your network's Internet IP address. Your Dynamic DNS updater software client will take care of passing the correct Internet IP address to centralized DNS servers on the Internet and will make sure it stays updated. So next time you want to connect to that network using VPN or Remote Access software you'll be able to use a domain name instead of trying to remember the IP address.

Dynamic DNS services (such as www.dyndns.com) will help you choose from a list of available domain names.

Main article: Dynamic DNS

Dynamic Host Configuration Protocol

DHCP is a set of rules used by a communications device (such as a computer, router or networking adapter) to allow client devices to request and obtain an Internet address from a server which has a list of addresses available for assignment. DHCP is also used to pass on DNS Server and Gateway information to DHCP clients. WRT devices generally include DHCP servers in their software suite.

E

Ethernet

Ethernet is a large and diverse family of frame-based computer networking technologies for Local Area Networks.

Extended Service Set Identifier

A wireless device may broadcast a name (for example: dd-wrt, default, linksys, home, my-wireless, cafe-wireless) at regular intervals. The user interface for selecting a network on each user's machine will enumerate the names of the devices it can hear. Formally this name is known as the extended service set identifier, usually written ESSID, but sometimes as SSID. As a rule you can only have one ESSID per access point. Wireless devices can disable the broadcast of their name while still accepting connections. This hides them but only from unsophisticated users.

See Also: Basic Service Set Identifier

E-commerce

Its a short form for Electronic Commerce. The name says it all, it consists of the buying and selling of products or services over electronic systems such as the Internet and other computer networks.

F

Fast Framing

Firewall

Software or hardware that limits network activity. There are different ways firewalls work. They could block port access, block ip addresses, mac addresses, or filter websites.

See also - Why Firewall

Firmware

This is just software but it runs on your hardware. It's usually delivered as a binary ROM image that has to be copied down onto your hardware (WRT54G) over a cable. The cable is usually an ethernet patch lead but could be a JTAG serial cable or doe some devices an RS232 cable. In the good old days we would burn an EPROM or flash chip in a programmer and then insert the chip physically into a socket. Hence the term firmware being software you can touch in the form of a chip.

FreeRADIUS Server

FreeRADIUS is the most widely deployed RADIUS server in the world, and can be used to authenticate WLAN clients using WPA/WPA2 Enterprise, which is more secure than WPA/WPA2 Personal (pre-shared key or PSK), since each client is uniquely authorized and encrypted.

FTP

FTP (File Transfer Protocol) is a standard network protocol used to transfer files from one host to another host over a TCP-based network, including the Internet, PCs and routers.

G

Gateway

Setting the operating mode to "gateway" allows your router to route packets between the LAN/WLAN and the Internet (through the WAN port). This is the default setting and the most common setting when the router is hosting the network's Internet connection through the WAN port

H

Host

Host is a generic term used when referring to a computer or device that is hosting a specific service or acting as some type of server. For example, if you have a mesh network in place, the "host" router would probably be the one hosting the Internet connection

Host Name

The hostname is unique name for any device on a network. It helps humans because names are easier to remember than numbers. "Router" is easier to remember than 192.168.1.1. Eash device on the network needs to have a unique name.

Hotspot

A location where wireless internet has been provided for people to use. An example of this would be to switch on your laptop in a cafe and associate with the ESSID available there, perhaps CAFE-HOTSPOT. Attempting to view a web site would show the Hotspot landing page (a 'Captive Portal' where you could press a button for free access or create an account and pay by card. This depends on the operator of the Hotspot. Once in, you can simply use the Internet normally

Hotzone

A large Hotspot, perhaps covering a whole town

HTTP Redirect

This option enables an HTTP redirector for proxy usage

Main article: HTTPRedirect

I

IEEE

Institute of Electrical and Electronics Engineers — a professional organization for electrical and electronics engineers hosting a number of special interest societies and standards committees. The IEEE is responsible for creation of standards such as IEEE 802.11.

Interface

a network adapter

See Also: http:/http://www.dd-wrt.com/wiki.openwrt.org/OpenWrtDocs/NetworkInterfaces

IPv6

Internet Protocol version 6 — an extension of Internet Protocol version 4 (IPv4). IPv4 uses an address space of 32 bits, allowing it to support 2^{32} (about 4.3×10^{9}) addresses. IPv6 uses an address space of 128 bits, allowing it to support 2^{128} addresses; this is approximately 5×10^{28} addresses for each of the roughly 6.5×10^{9} people alive today.

ISP

Acronym for Internet Service Provider

Internet Service Provider

An *Internet service provider* (abbr. *ISP*, also called *Internet access provider* or *IAP*) is a business or organization that sells to consumers access to the Internet and related services.

J

Journalling Flash File System (JFFS)

Taken from http://www.dd-wrt.comhttp://www.dd-wrt.com/wiki/index.php/Jffs

The Journalling Flash File System (JFFS) allows you to have a writable Linux File System on a DD-WRT enabled router. It is used to store user programs like Ipkg and data into otherwise inaccessible flash memory. This allows you to save custom configuration files, host custom Web pages stored on the router and many other things not capable without JFFS.

JTAG

A JTAG cable is a cable that hooks up to a JTAG interface, such as those on Linksys routers. It allows you to communicate with the router using your computer's parallel port. In many cases, a JTAG cable is an invaluable component used to debrick a partially or completely bricked (but not dead) router.

See Also: Recovery by JTAG cable

K

K24 K26

Used in reference to DD-WRT builds that are implemented with either Version 2.4 or 2.6 of the Linux Kernel. See the Peacock Thread in the Broadcom forum for more information.

Kaid

The Kai console daemon (kaid) is a service that provides tunneling for console games that do not have an inherent connection to the Internet. Although the label refers to XBOX, the daemon works well with PS2, and Gamecube consoles as well. It also allows the new Sony Playstation Portable (PSP) to go online with some of their multiplayer wireless games.

Kismet

Kismet is a layer 2 wireless network detector, sniffer, and intrusion detection software that runs on Linux.

See Also: Kismet Server/Drone

L

Local Area Network

A Local Area Network, or LAN, is your router's switch ports and your router's wireless interface. Most references in the forums and the Wiki are using the term LAN in this manner, although you may need to adjust your thinking according to the context it's used it. For example, the LAN on a WRT in Client mode is only the wired switch ports, because the wireless portion is acting a WAN interface.

Loopback

Loopback is a problem that occurs when multiple routes exist to the same destination. This can happen when a router is connected to an ad hoc network or is configured to function in a mesh network with several WDS-enabled routers. See STP

M

MAC Address

Media Access Control
A MAC address is a unique identifier attached to a network interface. It is stored in hexadecimal and usually appears in the following format: 00:00:00:00:00:00 or 00-00-00-00-00-00.

The first half of the MAC address is the Vendor ID which can be used to determine the Manufacturer of the device.

MAC Filtering

A method of filtering which devices can or cannot connect to a WRT by storing corresponding MAC addresses. MAC filtering is generally only performed on the wireless interface of a WRT.

MAC Number

Migration Authorisation Code number. Not to be confused with MAC Address. This is the number your ADSL ISP gives you when you want to switch to another ISP without a long wait whilst the phone company sends out engineers to move the wires. As you can imagine, this number can be held to ransom until you pay the old ISP bill, which is, of course, a contravention of the Ofcom guidelines

mBSSID

Multiple BSSID - to support a different MAC address for each SSID. Note: Some older devices don't support mBSSID but rather just mSSID (multiple network names, each having the same MAC).

Mesh Network

Taken directly from: http://en.wikipedia.orghttp://www.dd-wrt.com/wiki/Mesh_network Mesh networking is a way to route data, voice and instructions between nodes. It allows for continuous connections and reconfiguration around broken or blocked paths by ?hopping? from node to node until the destination is reached. A mesh network whose nodes are all connected to each other is a fully connected network. Mesh networks differ from other networks in that the component parts can all connect to each other via multiple hops, and they generally are not mobile. Mesh networks can be seen as one type of ad hoc network. Mobile ad-hoc networking (MANet), and mesh networking are therefore closely related, but mobile ad hoc networks also have to deal with the problems introduced by the mobility of the nodes.

Mesh networks are self-healing: the network can still operate even when a node breaks down or a connection goes bad. As a result, a very reliable network is formed. This concept is applicable to wireless networks, wired networks, and software interaction.

N

N Connector

This is the "good old" and "pro" type of antenna cabling connectors used for economical cabling and third-party high-gain antennas, RG-213 or LMR-400 cabling, cable television, and military uses ;). Converters can be used between these and RP-TNC and RP-SMA connections. Has nothing specifically to do with wireless N.

See also: Connector Photos Wikipedia

Network Address Translation

NAT (Network Address Translation) is the translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside. Typically, a company maps its local inside network addresses to one or more global outside IP addresses and unmaps the global IP addresses on incoming packets back into local IP addresses. This helps ensure security since each outgoing or incoming request must go through a translation process that also offers the opportunity to qualify or authenticate the request or match it to a previous request. NAT also conserves on the number of global IP addresses that a company needs and it lets the company use a single IP address in its communication with the world.

Network Time Protocol

Network Time Protocol (NTP) is used for automatic updating of time & date. The router will connect to an NTP server to update the time & date.

Some Firmware version have the server address embedded; some do not. For the firmware that need an NTP server address to be entered, you can find one here:

http://support.ntp.org/bin/view/Servers/NTPPoolServers

Neutered

In the world of DD-WRT and Linksys routers, a neutered router is a WRT54G v5 thru v8.2 and some other WRT54G2 series routers that have reduced RAM and reduced flash memory (typically 8/2), in comparison to other supported devices, thus the name neutered.

NEWD

A term that refers to the wireless driver used in various DD-WRT builds. See NEWD or VINT.

NoCat

NoCat originally started as a community-supported 802.11b wireless network in Sonoma County, CA and has grown into several projects whose purpose is to encourage the building of wireless community networks.

NoCatAuth is the original "catch and release" wireless captive portal implementation. It provides a simple splash screen web page for clients on the network, as well as a variety of authenticated modes.

Also see: http://nocat.net/

Noise Reference

Noise reference is just for calculating signal/noise ratio (SNR) in AP mode.

Source: A posting by BrainSlayer on the Google-cached LinksysInfo forums

ntop Remote Statistic

ntop is a network traffic probe that shows the network usage, similar to what the popular top Unix command does. ntop is based on libpcap and it has been written in a portable way in order to virtually run on every Unix platform and on Win32 as well.

ntop users can use a a web browser (e.g. netscape) to navigate through ntop (that acts as a web server) traffic information and get a dump of the network status. In the latter case, ntop can be seen as a simple RMON-like

agent with an embedded web interface. The use of:

```
* a web interface
* limited configuration and administration via the web interface
* reduced CPU and memory usage (they vary according to network size and traffic)
```

make ntop easy to use and suitable for monitoring various kind of networks.

What ntop can do for me?

```
* Sort network traffic according to many protocols
* Show network traffic sorted according to various criteria
* Display traffic statistics
* Store on disk persistent traffic statistics in RRD format
* Identify the indentity (e.g. email address) of computer users
* Passively (i.e. withou sending probe packets) identify the host OS
* Show IP traffic distribution among the various protocols
* Analyse IP traffic and sort it according to the source/destination
* Display IP Traffic Subnet matrix (who's talking to who?)
* Report IP protocol usage sorted by protocol type
* Act as a NetFlow/sFlow collector for flows generated by routers (e.g. Cisco and Juniper) or
* Produce RMON-like network traffic statistics
```

NVRAM

Non-Volatile Random Access Memory; a flash memory chip where the router's firmware is stored. Unlike Dynamic RAM (ie. SDRAM/DDR SDRAM), Non-Volatile RAM can hold data for a long period of time even after power is lost.

Note: "nvram" is also used to refer to the portion of flash memory where the firmware's configuration settings are stored. Do not be confused. If someone ever tells you to erase nvram, they probably just mean bring dd-wrt back to default settings (see Hard reset or 30/30/30). To erase the entire NVRAM chip with JTAG would actually require you to reload the unit from scratch (including the bootloader).

O

OLSR(d)

OLSRd The daemon that implements OLSR

OLSR (Optimized Link State Routing Protocol) is an IP routing protocol optimized for mobile ad-hoc networks, which can also be used on other wireless ad-hoc networks. OLSR is a proactive link-state routing protocol, which uses hello and topology control (TC) messages to discover and then disseminate link state information throughout the mobile ad-hoc network. Individual nodes use this topology information to compute next hop destinations for all nodes in the network using shortest hop forwarding paths. (Thanks to Wikipedia)

OpenVPN

OpenVPN is an open source VPN solution. Unlike most VPN systems, OpenVPN uses SSL/TLS to manage and encrypt the connection's data stream. This makes the solution very conducive to modern networking environments, as the connections can be easily used with NAT (the connections are simple, single port UDP or TCP).

Open Shortest Path First

One of several router protocols known as IGPs, (Interior Gateway Protocol). Using OSPF, a host that obtains a change to a routing table or detects a change in the network will immediately multicast the information to all other hosts in the network so that all will have the same routing table information. This method is more efficient than RIP (Routing Information Protocol) which sends the entire routing table to a neighboring host every 30 seconds. OSPF also uses more advanced algorithms to determine the shortest path, where RIP1 and RIP2 simply use hop counts. If your router is acting as a repeater, OSPF is the recommended protocol to use unless your network has other devices that only support RIP2.

P

Port Forwarding

Port Forwarding is necessary to allow computers outside of the LAN to access services that may be hosted by one or more computers inside the LAN. Since there is a shortage of public IP addresses in IPv4, the issue was conquered using NAT. While NAT isn't all bad (it adds security) it does introduce some complications when a computer inside an LAN is hosting a public service such as a web server, ftp server, or e-mail server. Port forwarding was designed to take care of this problem. Port forwarding can be configured in DD-WRT by going to "Applications & Gaming" > "Port Forwarding". You can also forward ranges of ports instead of single ports by going to "Applications & Gaming" > "Port Range Forwarding". Routers can be configured to listen on one port but forward to a different port. While it isn't foolproof, this can add a measure of security by using obscure ports to listen instead of the default ports that attackers expect you to host common services on.

Port Triggering

Port triggering is a configuration option on a NAT-enabled router which allows a host machine to dynamically and automatically forward a specific port back to itself. In layman's terms port triggering opens an incoming port when your computer is using a specified outgoing port for specific traffic.

Description

Port triggering is a way to automate port forwarding in which outbound traffic on predetermined ports ("triggering ports") causes inbound traffic to specific incoming ports to be dynamically forwarded to the initiating host while the outbound ports are in use. This allows computers behind a NAT-enabled router on a local network to provide services which would normally require the computer to have a fixed address on the local network. Port triggering triggers an open incoming port when a client on the local network makes an outgoing connection to a predetermined port or port-range on an external server.

Example

As an example of how port triggering operates, when connecting to IRC it's common to authenticate your username with the Ident protocol via port 113.

When connecting to IRC the client computer typically makes an outgoing connection on port 6667 (or any port in the range 6660-7000), causing the IRC server to attempt to verify the username given by making a new connection back to the client computer on port 113. When the computer is behind a NAT the NAT silently drops this connection because it does not know which computer behind the NAT to send the request to connect.

In the case of port triggering, you tell the router that when you make a connection out on any port 6660-7000 then it should allow connections in to that particular computer. This gives it more flexibility than static port forwarding because you do not need to set it up for a specific address on your network. You also gain security in a sense that that port is not left open when not actively in use.

Disadvantages

The disadvantage of port triggering is that it only allows one client on the network to supply a particular service that uses a particular incoming port. Port triggering is unsuitable for putting servers behind a NAT router because it relies on the computer to make an outgoing connection before it can receive incoming ones; servers should use port forwarding.

Point-to-Point Protocol over Ethernet (PPPoE)

PPPoE, **Point-to-Point Protocol over Ethernet**, is a network protocol for encapsulating PPP frames inside Ethernet frames. It is used mainly with ADSL services where individual users connect to the ADSL transceiver (modem) over ethernet. It was developed by UUNET, Redback Networks, and RouterWare and is available as an informational RFC 2516.

Ethernet networks are packet-based and have no concept of a connection or circuit. But using PPPoE, users can virtually "dial" from one machine to another over an ethernet network, establish a point to point connection between them and then transport data packets over the connection.

PPTP

The **Point-to-Point Tunneling Protocol (PPTP)** is a method for implementing virtual private networks. Layer 2 Tunneling Protocol (L2TP) (RFC 2637) or IPSec are the standards-based replacements for PPTP.

Q

QoS

(Quality of Service)
Main article: Quality of Service

R

RADVD

Linux IPv6 Router Advertisement Daemon

The router advertisement daemon (RADVD) is run by Linux or BSD systems acting as IPv6 routers. It sends Router Advertisement messages, specified by RFC 2461, to a local ethernet LAN periodically and when requested by a node sending a Router Solicitation message. These messages are required for IPv6 stateless autoconfiguration.

Also see: Litech's information on RADVD, Linux HQ's information on RADVD

Repeater

While repeater is not a selection in the "Wireless Mode" drop-down menu, it is commonly thought of as a mode that is different from the others listed above. In reality, a router acting as a repeater is configured as an Access Point (AP Mode) and has WDS (Wireless Distribution System) enabled. To use your router as a repeater will also require you to enable and configure WDS in the router you are connecting to (the "host router"). Do not attempt to turn on repeater mode by using the "Site Survey" and then the "Join" button to connect to other routers, as this will actually put your router into Client mode. Also, be aware that using your router as a repeater will reduce the router's wireless throughput since WDS uses wireless bandwidth that would normally be available to wireless clients, to "talk" to other routers. This reduction in wireless bandwidth will probably not be noticeable if the repeater router(s) are used only to share an Internet connection, unless you have more than three routers "daisy-chained" in this manner.

See Also: Linking Routers, Repeating Mode Comparisons

RFlow

The RFlow Collector (download) is a graphical traffic monitoring and management tool.

RIP

(Routing Information Protocol)
RIP1 and RIP2 are both older protocols that are to be used only when an existing network does not have OSPF compliant equipment. In short, RIP2 is slightly more secure and slightly more efficient than RIP1, while OSPF has great advantages over both. It is assumed that RIP2 is in the feature set primarily for backward compatibility reasons.

Router

A router is a device that handles IP addressing. Routers connect LANs and WANs together. Routers link MAC addresses to IP addresses. Interfaces connect to switches in a lan, those switches are connected to

routers to communicate beyond their LAN. The router itself does NOT include the Wireless Access Point (WAP) or 5 port switch that "home routers" include (like my wrt-54gs). Most of these devices are actually "3-in-1" devices (router, switch, WAP).

See Also: WRT

RP-SMA Connector

A *Reverse Polarity SubMiniature version A Connector* is a type of antenna connector used on brands of routers including Buffalo and Asus. Also found on PCI cards.

See also: Connector Photos Wikipedia N Connector

RP-TNC Connector

A *Reverse Polarity Threaded Neill-Concelman Connector* is a type of antenna connector used on Linksys access points. Designed to make it difficult to add high-gain antennas which breach FCC rules!

See also: Connector photos Wikipedia N Connector

Rx

Abbreviation for *receive* or *receiver*

S

Samba

A free software re-implementation of SMB/CIFS networking protocol in Linux and most UNIX-like systems, allowing Microsoft Windows machines to access files and printers on a Linux or UNIX host over a network.

Simple Network Management Protocol

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

Two versions of SNMP exist: SNMP version 1 (SNMPv1) and SNMP version 2 (SNMPv2). Both versions have a number of features in common, but SNMPv2 offers enhancements, such as additional protocol operations. Standardization of yet another version of SNMP — SNMP Version 3 (SNMPv3) — is pending. This chapter provides descriptions of the SNMPv1 and SNMPv2 protocol operations.

SOC

A system on a chip or system on chip (SoC or SOC) is an integrated circuit (IC) that integrates all components of a computer or other electronic system into a single chip. It may contain digital, analog, mixed-signal, and often radio-frequency functions?all on a single chip substrate. A typical application is in the area of embedded systems. (Thanks to Wikipedia)

Source Code

This is the software before cross-compilation into firmware. For firmware this is usually written in C. For DD-WRT the source can be downloaded and cross-compiled on the PC to produce firmware that is ready to be uploaded onto the WRT54G. This is not something most people need to do since the compiled binary firmware is usually available.

Secure Shell

SSH clients can access information and make changes to remote systems that are running an SSH daemon. Telnet or SSH can be used as another method of changing settings on your DD-WRT router, as opposed to the Web Interface. Certain changes to your DD-WRT router can only be done using Telnet or SSH.

Main Article: Telnet/SSH and the Command Line

SIPatH

SIPatH is a configurable, free and RFC3261-compliant SIP proxy. SIPatH features a Status web interface, enables individual VoIP provider settings on each IP phone and internal calls among all registered phones within the local network. Main projects objectives are providing a simple solution of the SIP-over-NAT problem and free PBX-like telephony features. According to the last release notes, other features included:

- NAT-RTP proxying and improved SIP-NAT traversal
- Aliases for registered URIs, configurable at runtime via a web interface
- SIP Messaging: Messages can be sent through the web interface to all registered SIP UAs

The SIPatH project is now being continued by the Boozy version of the router software maintained by Milkfish project.

SSID

See: Extended Service Set Identifier

Static DHCP

An extension of the DHCP protocol enabling the server to issue a specific IP address to a client based on its MAC address. This feature effectively guarantees that the client will receive the same IP every time it requests

a new lease, yet the configuration is dynamic in all other respects.

STP

(*Spanning Tree Protocol*)
STP needs to be enabled to prevent loopbacks on networks where multiple paths to the same point are possible. A mesh network that uses multiple repeaters where repeaters have WDS configured to work with more than one device should enable STP. STP is known to interfere with the router's DHCP client for users who use Comcast Cable as their ISP.

Main article: Spanning Tree Protocol

Syslog

(System logging) Syslog is a messaging standard for logging on a network. This term can be used to describe a library or a client/server protocol. Logging is useful to monitor the health of your network, help diagnose problems, intrusion detection, and intrusion forensics. For an excellent white paper on syslog see this pdf from SANS (http://www.sans.org/rr/whitepapers/logging/1168.php - 560KB).

Main Article: Logging with DD-WRT

T

Telnet

Telnet clients can access information and make changes to remote systems that are running a Telnet daemon. SSH is similar to Telnet and is preferred because Telnet traffic is not encrypted, thus usernames and passwords are passed in plain text and can easily be sniffed by packet sniffing software. Telnet or SSH can be used as another method of changing settings on your DD-WRT router, as opposed to the Web Interface. Certain changes to your DD-WRT router can only be done using Telnet or SSH.

Main Article: Telnet/SSH and the Command Line

TFTP

TFTP (Trivial File Transfer Protocol) is a file transfer protocol notable for its simplicity. It is generally used for automated transfer of configuration or boot files between machines in a local environment. Compared to FTP, TFTP is extremely limited, providing no authentication, and is rarely used interactively by a user. Due to its simple design, TFTP could be implemented using a very small amount of memory. It is therefore useful for booting computers such as routers which may not have any data storage devices. (Thanks to Wikipedia)

Trailed Build

A Trailed build is a build with the router model and version in the file name. These builds are often necessary for the initial installation of DD-WRT onto a router that contains factory firmware. They have the correct header in the file which allows it to be loaded by the factory firmware. See specific router install instructions and the Peacock Thread in the Broadcom Forum for more information.

TTL

Time To Live

The purpose of the TTL is to prevent chaos. TTL prevents a network packet from existing on the internet indefinitely. If a packet has TTL of 64, it will be discarded after 64 hops. Usually, every router that the packet crosses will decrease the TTL field by one.

The TTL is useful in other ways. It can help us to determine the best time to flash DD-WRT on our routers.

When we first power up the router, the bootloader waits for a brief period and opens up TFTP daemon. This daemon, or background service, listens for network packets which would initiate an emergency firmware recovery/upgrade.

A router's bootloader will typically respond to a ping with a reply having a TTL of 100. However, the dd-wrt firmware itself, which is based on the Linux operating system, will respond with a TTL of 64 once it is up and running.

Therefore, the best time to flash DD-WRT is when TTL equals 100. When the TTL equals 64, it is too late because we are beyond the bootloader's TFTP stage.

Tx

Abbreviation for *transmit* or *transmitter*

U

Universal Plug-n-Play

UPnP (Universal Plug-n-Play) is a Home/SOHO networking standard. It allows for a number of benefits to ease networking setup, such as device discovery and control. In the realm of home/SOHO routers, it is mainly used for automated port forwarding and other simple networking setup.

Connect USB modem to A Game Console

Universal Wireless Repeater

V

VINT

A term that refers to the wireless driver used in various DD-WRT builds. See NEWD or VINT.

VLAN

(*Virtual Local Area Network*)
A VLAN is, in basic terms, a group of physical interfaces on a switch that behave as if they are a separate standalone switch. While using one physical switch, a VLAN allows you to partition it into multiple LANs, each one completely isolated from the others. The switch must support VLAN configurations — most cheap switches don't allow this, but high-end manageable switches do, as does the internal switch on DD-WRT compatible routers.

VoIP

(*Voice over Internet Protocol*)
VoIP is a rather new technology for making phone calls using the Internet. Skype is an example of VoIP, but so is Vonage, which allows you to use a real phone directly plugged into your WRT54G rather than needing to fire up your PC.

VPN

(*Virtual Private Network*)
A VPN allows two LANs together over the Internet using a virtual cable, or VPN. You have PPTP, IPSec, OpenVPN. Mostly DD-WRT is not too good at doing this but will allow these service to operate as a pass-through. Hence the term VPN-Passthrough.

VPN Passthrough

The router allows you to run a VPN service on your network. The VPN version of DD-WRT includes this.

VPN Server

This is where the router actually creates a VPN connection to another VPN server. This is the one you really want for VPN. The VPN version of DD-WRT does not seem to do this.

Virtual Private Server - Future of Web Hosting

W

WAN

See: Wide Area Network

Wardriving

The act of scanning for wireless networks and hotspots whilst traveling. See also Wombling.

WDS

(Wireless Distribution System)
A Wireless Distribution System is a system that enables the interconnection of access points wirelessly. In DD-WRT, WDS allows multiple WRTs to communicate with each other wirelessly without the need for a wired backbone. A WRT communicating in this manner is generally referred to as a repeater.

WDS Bridging

WDS bridging is when you setup a repeater router to "talk" to a main/host router and then disable the Access Point function in the repeater so that it will not accept clients. You'll need to run a short script from the shell to achieve this. A WDS bridge is fully transparent. In this configuration the wireless portion of the repeater WRT has bridged the repeater WRT's LAN interface with another WDS enabled wireless device. WDS bridging is done in access point mode.

Main article: WDS Bridging

Wi-Fi Multimedia Technology

WMM gives priority to audio, video and voice applications in a Wi-Fi network so that other applications and traffic are less likely to slow them. for e.g it help you reduce the delay in Phone conversations. Watching video, you are more likely to see smooth action.

WiFi and Wireless Help

Wi-Fi Protected Access 2

WPA2 is the second generation of WPA security and provides a stronger encryption mechanism through Advanced Encryption Standard (AES), which is a requirement for some government users.

Wide Area Network

Wide area network, also referred to as WAN, deals with connections between remote locations. This term often is equivalent to the wider internet or at least the connection to the internet provided by one's ISP.

WIP

(*Work In Process*)
WIP is seen in the Supported Devices page to indicate that firmware for a particular router is under development, but not yet available.

WISP

Wireless Internet Service Provider — a company using wireless gear such as WRT54G and DD-WRT to deliver broadband Internet into peoples' homes without using their phone line. The advantage of a WISP is that one is not limited by the speed of one's telephone line and perhaps one doesn't even have a telephone line at the service location. Since there is no telephone line, the WISP is not paying fees to the telephone company, so can often provide a better service at the same cost. You could start your own WISP or at least a hotspot with your DD-WRT.

WLAN

(Wireless Local Area Network)
In it's simplest form, the wireless network provided by your wireless router.

WOL

(Wake-On-LAN)
Wake-on-LAN is an Ethernet computer networking standard that allows a shut-down computer to be booted remotely. The network card of the computer that has WOL enabled will listen for a "Magic Packet", then verify the information in that packet and decide whether or not to boot the computer.

Main Article: WOL

Wombling

Also known as Wardriving, wombling is the act of scanning for wireless networks and hotspots whilst traveling. This was traditionally done with a Proxim ORiNOCO PCMCIA card in a laptop with a Pringles can Yagi antenna. We are talking old school. The connection with the Wombles comes from "Orinoco" who is, of course, one of the Wombles from Wimbledon Common. It is often thought that using someone's Internet connection without their permission is illegal. It seems to be a form of trespass, so if you don't look at any local files or break anything then you're probably OK. However if you bring their connection into disrepute or slow it down significantly or look at their personal files then you are clearly a law breaker and could get prosecuted. If they have taken trouble to secure the connection then you should respect that and not break past

the security.

WRT

(Wireless Receiver/Transceiver)

X

Y

Z