The D-STAR Gateway - Configuration & Operation

Summary

In this final lesson, the student learns about the steps necessary to create the gateway and connect it to the D-STAR system. As with the previous lesson, this is not intended to be a step-by-step set of instructions. The details of configuration will be found in the operating manuals for the various pieces of equipment and software.

Basic Requirements

The D-STAR gateway must be assigned a fixed or **static IP address** and be provided with a broadband Internet connection, such as those provided by a DSL or cable connection. Whether your Internet connection router is a standalone device or included in a broadband gateway modem-router, it will need to provide or implement the following:

Class "A" internal *subnet* (LAN) 10.0.0.1 / 255.0.0.0M
Port forwarding
Setting a fixed IP address, such as for **PPPoE** for WAN

Note also that Icom's gateway software is a proprietary, licensed vendor product, and can not be copied, shared or re-distributed. It is not part of the open D-STAR protocol.

If you are unfamiliar with the Linux operating system or with basic computer networking, it is strongly recommended that you obtain assistance before attempting to install or configure D-STAR gateway systems. For all of the following instructions and when editing or entering data, pay particularly close attention to detail. The syntax of the information is very important--errors will likely cause the software to fail or operate improperly. **Bold** text indicates a file name.

Gateway Router

The gateway router--the interface between the gateway server and the Internet--must be configured to support the server software as follows:

1. Make sure the router's "local IP" settings are set as follows:

   Local IP address: 10.0.0.1
   Subnet mask: 255.0.0.0

2. Set the router to forward the following ports:

   Data sync: 20005, Protocol - TCP, IP Address - 10.0.0.2
   Voice RX: 40000, Protocol - UDP, IP Address - 10.0.0.2
   Data RX: 40001, Protocol - TCP, IP Address - 10.0.0.2
   SSH: 222, Protocol - TCP, IP Address - 10.0.0.2
   Monitor: 3306, Protocol - TCP & UDP, IP Address - 10.0.0.2

Figure 9-1 shows the port forwarding configuration screen for the Linksys WRV54G router as an example. The router is then ready to support the gateway.

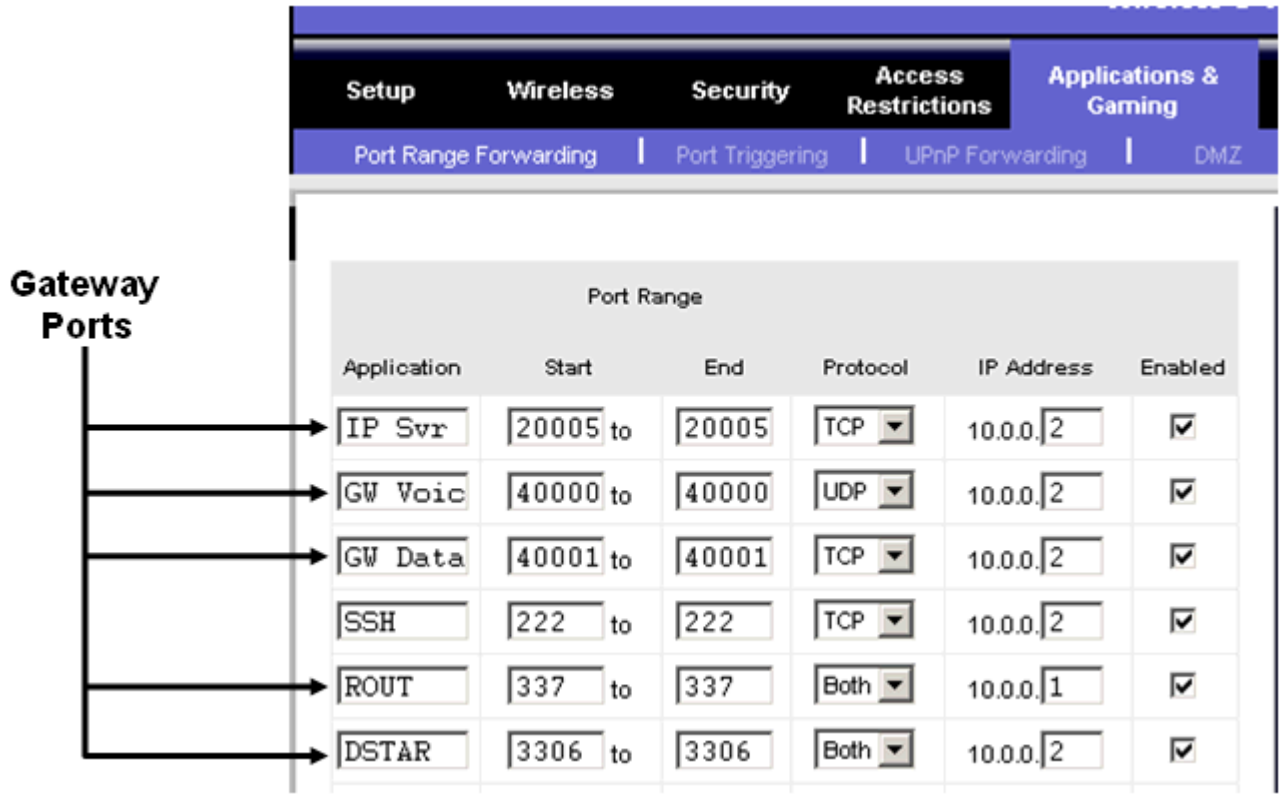

Figure 9-1

Gateway Server Configuration

The gateway software is hosted by a Linux®-based PC. All of the following instructions are based on the Fedora™ Core 3 or Fedora Core 4 version of Linux. The PC on which the gateway server and gateway software will run must meet the following minimum requirements:

Linux OS (recommend Fedora Core 3 or 4)
Pentium-grade 2.4 GHz or faster CPU
At least 512MB RAM
2 LAN cards (NIC from Intel recommended)
At least 10 Gb hard drive free space

Ethernet Port Configuration

The host PC must have two Ethernet ports, eth0 and eth1. Eth0 is configured as a LAN port and will be connected to the router. Eth1 is configured to connect to the ID-RP2C controller. Both ports will have static IP addresses. In the "Ethernet Port" configuration screen set up Eth0 and Eth1 as follows:

Eth0
Select "Statically Set IP Address"
Address: 10.0.0.2
Subnet Mask: 255.0.0.0
Default Gateway Address: 10.0.0.1

Select "static IP" for eth1 as well and enter the proper settings.

Eth1
Select "Statically Set IP Address"

Address: 172.16.0.20
Subnet Mask: 255.0.0.0
Default Gateway Address: none

The gateway server must be physically located at the repeater. The segment of the LAN that connects the controller to the gateway (Eth1 - 172.16.0.20) is very sensitive to latency!

Network Configuration

In the "Network Configuration" configuration screen, the **DNS** server's address should be set to 127.0.0.1.

D-STAR Gateway Database

You will need to create the local database used to maintain connections with other repeaters and services on the D-STAR network. This requires the following steps:

1. Add the information shown in the configuration guide to the **named.conf** file as shown in the gateway software manual.
2. Create a folder named "dsipsvd" in the /var directory.
3. Create the local database, named **dstar.local.db** in the /var/named/chroot/var/named/ directory. The database file should contain the information shown in the configuration guide--syntax is critical. Errors in the "named" service configuration is a common cause for the gateway to not operate properly.
4. Re-start the Linux "named" service.
5. From the Edit Runlevel menu, select Runlevel 3
6. Click "named" and then Restart
7. From the Edit Runlevel menu, select Runlevel 5
8. Click "named" and then Restart

Use a terminal window to test the router and verify that the correct IP address has been entered by entering "dig router.dstar.local" In the "ANSWER SECTION" you should see the router's IP address - 10.0.0.1.

Trust Servers

A trust server, USRoot, is provided as a service to the D-STAR community by K5TIT in Dallas TX. You can use your own private trust server to create your own D-STAR network or you can link to the USRoot trust server in Dallas, if desired. Any PC running the D-STAR gateway software can be configured to be a trust server to create your own private network.

Gateway Software

Installation

The D-STAR gateway software is supplied as a self-extracting file. Be sure to extract the program to the "dstar" folder in the "root" directory.

Configuration

Once the software has been installed, open the file **dsipsvd.conf** to set up the following pieces of information:

TRUST_SERVER - the IP address of the trust server you have chosen

ZR_CALLSIGN - the call sign of the zone repeater (the repeater with the D-STAR gateway for your zone)

IPSV_ADDR - the IP address of the gateway server

DNS_ZONE_FILE_PATH - the location of the **dstar.local.db** file

NAMED_PID_FILE - the location of the **named.pid** file

Next, acquire the **MAC address** of the Eth0 port by typing the command "arp" in a terminal window. Look for the line that shows Eth0 connected to an IP address of 10.0.0.1. Record the MAC address on that line. That is the MAC address of the NIC card of the Eth0 port.

Open the **dsgwd.conf** file and set up the following pieces of information:

ZR_ADDR - the address of the zone repeater server, set to 172.16.0.10

ZR_CALLSIGN - the call sign of the zone repeater

DNS_MAC - the MAC address of the Ethernet device used to connect to the DNS server.

In the **/etc/syslog.conf** file, add the following lines to set up the D-STAR log files (the first line, beginning with #, is a comment):

```
# for D-STAR
local0.* /var/log/dsgwd.log
local2.* /var/log/dsipsvd.log
```

Make sure to type "local" immediately before the number with no spaces.

Next, modify the startup script **/etc/rc.d/rc.local** to automatically run the D-STAR gateway software by adding this line anywhere in the file:

```
/dstar/exec-mgsv
```

Set the software's default runlevel to "3" by opening the file **/etc/inittab** and changing the line

```
id:#:initdefault:
```

so that the pound sign (#) is replaced by "3".

This completes the configuration of the D-STAR gateway software. Restart the Linux system.

Testing the Gateway

After the system starts, from the SSH Shell, type:

```
ps -ef | grep dstar
```

and you should see at least the following pair of programs running:

/dstar/dsipsvddsipsvd - this is the gateway server
/dstar/dsgwd/dsgwd - this is the gateway itself

Without both programs running, the gateway will not be functional! If the programs are not running, check the log file at:

/var/log

The log files from both programs should be being saved as:

dsipsvd.log
dsgwd.log

D-STAR System Sync

Once your gateway is up and running, it will synchronize itself with the rest of the D-STAR network. The easiest way to see if it synchronized is to look at the **dstar.local.db file**.

Open the file:

/var/named/chroot/var/named/dstar.local.db

If the gateway has been synchronized, you will see a list of other D-STAR gateway servers and their IP addresses as shown in **Figure 9-2**.

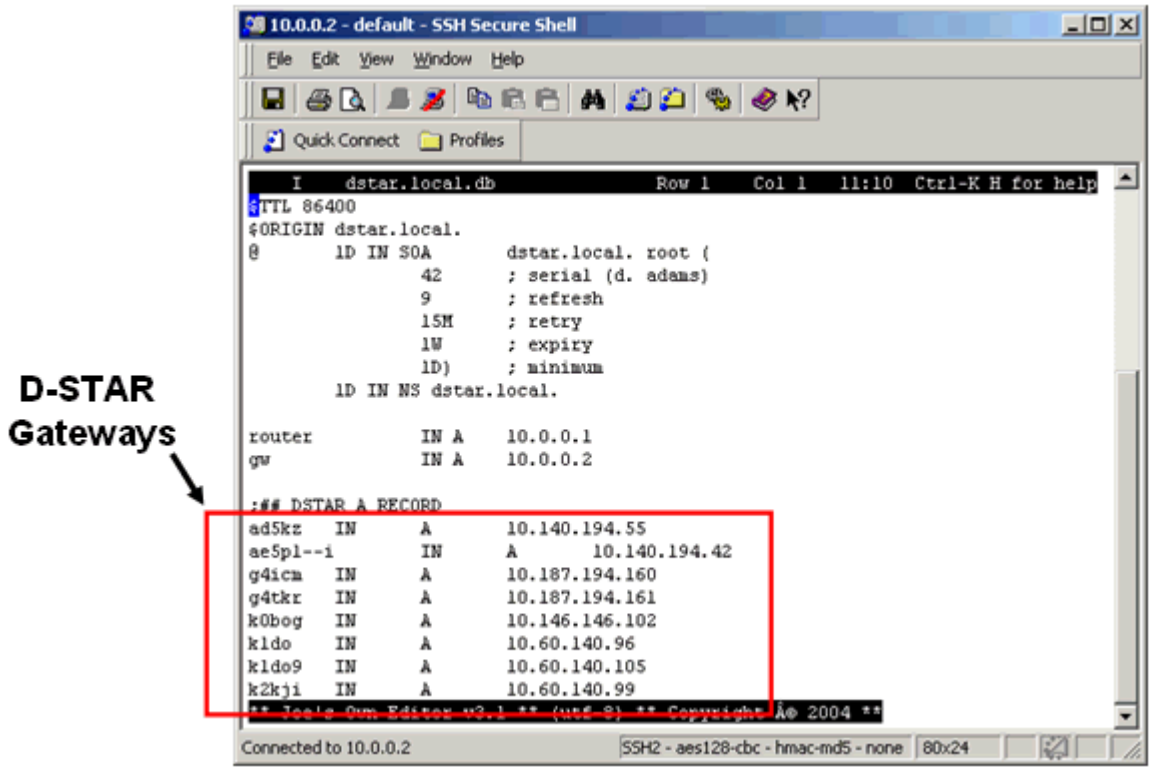

Figure 9-2

The gateway software uses 3 tables:

RIP - Reserved IP addresses
GIP - Gateway IP addresses
MNG - Call sign manage table

The backup tables are stored in the /var/dsipsvd folder. The files being used by the gateway are resident in memory after being downloaded from the trust server. You can "write" the tables to a text file to view, if desired. You can not edit them directly. All files are updated / merged automatically with the trust server and all the other gateways on the network at least once a day.

Adding Users to the D-STAR Network

Any user can operate locally on a D-STAR repeater, with or without their call sign in the registry. Only users that have been added to the gateway registry are allowed to cross the D-STAR gateway and access the D-STAR network. Once a user is added to the D-STAR gateway, they have gateway rights via any D-STAR gateway that is configured to use the same trust server.

Each user call sign is assigned a fixed IP address. The IP addresses are assigned to the gateway server in blocks of 32 and are created by using the "reserve" command. The exact syntax of the "reserve" command is shown in the gateway software manual.

After running the "reserve" command you can view the assigned block of 32 addresses by using the following command

```
cat /tmp/dsipsvd-cmdin
```

Record the range of IP addresses for use in registering new calls.

The exact syntax of the "add user" command is shown in the gateway software manual. Along with the range of IP addresses, the following information is required:

User ID - the users call sign, it must be 8 characters long, add spaces to pad

Area Repeater Call Sign - the system call sign with the letter [A] in the 8th position, use spaces between the call sign and the [A]

Zone Repeater Call Sign - the zone repeater call sign, it must be 8 characters long, add spaces to pad

GW IP Address - the public fixed IP address of the gateway server

Users Assigned IP Address - the address assigned to the user by the local address coordinator (one of the IP addresses recorded earlier)

Alias Name for DNS - the user's call sign, in lower case, padded with spaces at the end if necessary.

The following is an example of a "add user" command to add W7JRL to the N7IH registry. * represents a space in this example:

```
add
W7JRL71*|N7IH9**A|N7IH9***|65.102.167.146|10.140.194.xxx|w7jrl71"
> /tmp/dsipsvd-cmdin
```

Going Live!

Before attempting to go "live" on the D-STAR network you must verify that you are 100% functional on the Icom test system. If you have ANY questions, contact Icom. This will avoid corrupting the network databases that would inconvenience many D-STAR users.

Once operational on the "test" network, you need to "kill & clean" your gateway, change the TRUST_SERVER IP address, and re-boot the gateway PC. Simply re-starting the gateway software will not do the job!

To "clean" your system and start fresh (on the live network), begin by killing all active D-STAR services:

1. Execute a '`ps -ef | grep dstar`' command. This will provide the process numbers for the dsgwd & dsipsvd processes.
2. Execute a '`kill xxx`' command, where 'xxx' is the process number revealed in step one, for each of the two processes.
3. Execute a '`rm /var/dsipsvd/*.*`' command. This should completely clear the /var/dsipsvd directory.
4. Edit the file /var/named/chroot/var/named/dstar.local.db with a text editor and delete any call sign entries after "#DSTAR A RECORD".E
5. Execute a '`cat /etc/dsipsvd.conf`' command, and ensure that your TRUST_SERVER points to the proper server IP for the desired network. Use a text editor to change the TRUST_SERVER IP, if needed.
6. If you are creating or cleaning your own D-STAR network, you can execute the cleanup on the TRUST_SERVER, and have it ready. (Do not perform this step if you are joining an existing D-STAR network.)
7. Execute a '`reboot`' command on your gateway.
8. The gateway will run and download new database files from the TRUST_SERVER, then re-sync with each of the other gateways.

All gateways pointed to the same trust server share the same GIP, RIP and MNG tables. These tables can not be changed or "cleaned-up" independently. Going live requires that all connected gateways to be "killed" and "cleaned" first.

Once all connected gateways are "killed", the trust server files can be edited, but only before any gateway is re-booted. When the gateways are "cleaned" and re-booted, they will download the new GIP, RIP and MNG tables from the TRUST_SERVER.

Click the "Review" button to review the topics covered in this lesson. When you are ready, click "Next" to continue...