

Internet Radio Linking Project (IRLP) and Emergency Management Application

By Stephen B. Hajducek, N2CKH
AERIALS, Inc.
U.S. Post Office Box 8
Morganville, New Jersey 07751-0008
<http://www.qsl.net/aerials>

Edits by Nate Duehr, WY0X
IRLP List Moderator/IRLP Volunteer
nate@natetech.com

PURPOSE:

The purpose of this paper is to describe the Internet Radio Linking Project (IRLP) and provide a prospective of the potential applications of IRLP by Government and other Emergency Communications planners utilizing the Amateur Radio Service. This paper shall also describe in detail how IRLP works and will identify the advantages and disadvantages of using IRLP in Emergency Communications.

OVERVIEW:

Whenever natural catastrophes, acts of terrorism, or other emergencies occur, the Amateur Radio Service has proven itself a tested and organized nationwide network of trained radio communications volunteer technicians and operators. As part of its Federal Communications Commission (FCC) charter, the Amateur Radio Service provides Emergency Communications (via both informal and formal groups) to coordinate communications during emergencies Nationwide. The Amateur Radio Service is comprised of volunteers who have earned their licenses from the Federal Communications Commission (FCC) and operate according to FCC rules¹. The Amateur Radio Service has provided Emergency Communications during many major crises dating back to 1913 in keeping with its basis and purpose². Amateur Radio operators still "get the word out" after major storms, floods and other natural disasters. Most recently they provided communication services to relief agencies, including the American Red Cross, after the tragic September 11, 2001 terrorist attacks on both the World Trade Center in New York City and the Pentagon in Washington D.C.

Licensed Amateur Radio Operators, or "hams", are involved with various State Office's of Emergency Management throughout the country. Hams also operate at the National level through the Radio Amateur Civil Emergency Service (RACES), which is coordinated through the Federal Emergency Management Agency (FEMA), and through the Amateur Radio Emergency Service (ARES), which is coordinated through the American Radio Relay League (ARRL) and its field volunteers. Many national organizations³ have formal agreements with the Amateur Radio Emergency Service (ARES) and other Amateur Radio groups. In areas that are prone to tornado and hurricane emergencies, many hams support SKYWARN, operating under authority the National Weather Service (NWS).

The purpose of all Emergency Communications is to protect life and property in emergency situations by coordinating response activities of volunteers to requests from municipal, state and federal agencies who have requested assistance to ensure optimum use of the communications resources available. The planning and training of these volunteer entities involves preparations for communications to carry out actions to be taken to mitigate, prepare for, respond to, and recover from the effects of an emergency. The required communications planning must take into account an all hazards approach to Emergency Management and cover natural disasters, technological disasters, and national security crises. As the world is ever changing, the scope of Emergency Communications and the Amateur Radio Service has been influenced by technological advancements, natural and man made disasters and world politics. Emergency Communications services are needed for many hazards, most of which require communications from the field with low power hand held radios. Reliable, quality communications is key and wide area communications is often needed to coordinate with between various local, state and federal agencies as well as volunteer organizations. Amateur Radio can fill the interoperability gap between agencies with dissimilar radio systems and assist with interagency coordination in large-scale disasters.

With the advent of IRLP and its rapid spread across North America and beyond, the possible application of IRLP for on-demand linked communications circuits that can be configured for the geographical communications needs of the emergency situation at hand is a potentially huge very significant advantage to Emergency Communications Managers. Emergency Management officials should view IRLP as simply another communications tool that has become available to them with both strengths and weaknesses as applied to Emergency Communications. It is these strengths and weaknesses of IRLP that need to be identified and understood for the proper integration of IRLP into Emergency Management communications plans at all levels.

IRLP DESCRIPTION:

The IRLP system uses Linux-based software and radio interface hardware to link radios via standard "Internet" TCP/IP data connections. The hardware interface DTMF control board is the brainchild of David Cameron, (Canadian Amateur Callsign: VE7LTD) from Vancouver, British Columbia, Canada. Information on the International IRLP network can be found at <http://www.irlp.net> and maps of IRLP nodes are at <http://www.ipass.net/~jimprice/irlp/>, which shows cities and frequencies in use and is updated with new cities and frequencies almost on a daily basis.

David set out in 1997 to design a better way to use Internet technology to perform radio linking, while improving usability, user control, and sound quality over other systems that had been developed before IRLP. The final IRLP product was a combination of custom hardware and software that creates a seamless radio link between two or more remote sites on the Internet. The product works so well that many people have reported that users of the system find it hard to believe that they are talking through a link utilizing the Internet. Previous technology did not have the sound quality or active control of the radios in the link, making it less transparent to the end-user, and more difficult to operate.

The IRLP system is an open, growing cooperative effort that runs on a large distributed network of dedicated PC based IRLP nodes running the Linux Operating System. Many of the "central" servers are located in donated co-location facilities, which are hardened against power and network losses, however individual nodes can continue to operate without interaction with these servers, even if they are unavailable. Local IRLP radio system nodes can dynamically link to other nodes around the world through the use of IRLP Servers and IRLP Reflectors.

The heart of the IRLP is its Amateur Radio network of independently owned and maintained nodes, linking more than 465 sites around the world that offers excellent voice communications with the full-dynamic-range digital telephone-quality audio. The IRLP is used to link Frequency Modulation (FM) based VHF and UHF simplex radios and repeater systems separated by long distances without the use of leased phone lines, RF links or satellites. A statistical analysis⁵ was performed on 10 May 2002 when 438 nodes existed, based on the data contained at the on line status page information from <http://www.irlp.net> which provides an excellent example of the growth of the IRLP on all seven continents.

IRLP uses Voice-Over-IP software and the Internet to link a radio site to one or many radios sites one a worldwide basis. The system uses its own inexpensive interface board and software suite, which makes interfacing a radio system simple and cost effective. IRLP is an open system to the extent that node owners can modify the IRLP script files and even integrate additional programs and scripting files to augment the IRLP feature set on their node for added capabilities.

An IRLP node is the point of egress into the IRLP network for each radio end of the connection. Each IRLP node having at least one radio point of access, some IRLP nodes are tied into RF linked repeater systems allowing multiple radio points of access and even wider area geographical coverage than a stand-alone repeater or simplex radio. An IRLP node can be connected on demand by DTMF (also known as AT&T's TouchTone™) signaling in a one-to-one configuration to any other node in the IRLP network. In addition, there are numerous (10 at last count) IRLP Reflectors in the network that can provide a one-to-many, multiple node, conference-call-style connection.

During normal operation, a group of redundant IRLP master servers keeps all nodes updated with the latest software and back-end configuration and connection data. An IRLP server handles the connections being made by IRLP nodes, IRLP software updates (including the hosts file) as well as the Echo Reflector, which is used for node testing. However, if these servers are unavailable, individual IRLP nodes can continue to operate normally.

An IRLP Reflector acts as a centralized connection point to bridge an unlimited number of IRLP nodes together, think of this as a conference call. An IRLP Reflector is simply a Linux server that is not connected to any radio but rather permits an IRLP node to be connected by streaming received audio back to all connected nodes.

IRLP CHARACTERISTICS:

IRLP differs a bit from conventional FM Simplex, Repeater and RF Linked Repeater use. The IRLP provides a much wider coverage area (international in fact) than most RF based linking systems and there is additional timing delays required for a transmitted signal to propagate from the intercept point to the retransmission across the network of interconnected nodes. In addition, aside from the local gateway egress into the IRLP, stations cannot just drop down to the input frequency to hear a station not making it in to the system well unless it is a local station, however this is true for any wide area repeater linking scheme, and operators are able to quickly grasp the concepts by listening to the frequency and can start using the system with no training whatsoever.

IRLP is very similar to other linked repeater systems. The main difference is that the link is achieved via the Internet utilizing VoIP verses a leased telephone line or a RF link via UHF radio, Microwave or Satellite. In Reflector operation, a team of IRLP Reflector operators can monitor the system remotely and remove any node from the system real-time if their node is causing other

nodes to have communication difficulty for any reason, including hardware/equipment failure, misconfiguration, or radio interference. An IRLP control operator on a reflector can immediately take down any node that is Pulsing or otherwise hanging up the network

IRLP is accessed via simple DTMF commands provided from the digit keypad on most Amateur Radio equipment. Radio Amateurs have been using DTMF control for years to make autopatch phone calls and to control repeater functions and remote devices. DTMF control feels natural to operators, and is as simple as dialing your home telephone.

To connect to an IRLP node/reflector the IRLP port must be active, some systems require that this port be activated by a system Control Operator. Many systems change the courtesy tone or provide a message alerting users to the fact the IRLP port is active if the system does not always have the IRLP port active. To initiate a call to another node or Reflector, with the IRLP port active, the system user would enter a short series of digits (usually four) that relate to the node number they wish to "call". A full listing of active nodes and their status is available at <http://status.irlp.net>. The system responds with recorded voice prompts for connection information, including errors or other information the operator might need. Please note that some nodes require a prefix code as they may be club sponsored and view IRLP access just as autopatch access, club membership being required. However, unless it is a closed repeater, all hams are usually welcome to join the IRLP activity when a system is linked.

Once the local repeater or simplex node is connected to the IRLP network, you can commence with a normal radio communication (QSO) as you would with any local amateur. However, be sure to leave a few seconds between key ups to allow for Internet time delays and other nodes to disconnect from the IRLP. When you push your Push-To-Talk (PTT) button you are actually keying ALL repeaters connected to the network as well as the local system. This could be only one Repeater in a Point-to-Point Connection or many repeaters virtually all over the world when connected to an IRLP Reflector. Due to there being link radios and other small delays inherent in such a wide-area linked radio system, it is courteous to leave a one-second pause between transmissions. Also operators should key down their microphones and pause briefly before speaking to ensure that all the links in the network have gone active before they start their transmission. When a person comes back to you WAIT for 3-4 seconds before responding, this allows others to join in the QSO (communications in progress) and more importantly, allows node control ops to disconnect from the IRLP Network. Only one node can "talk" at a time, so pauses are important for nodes that would like to disconnect from a Reflector system since many nodes cannot receive and transmit at the same time

IRLP GUIDELINES AND USEAGE INFORMATION:

(For those emergency managers or hams in an area already served by IRLP, these guidelines will be useful to you.)

The most important guideline to remember is leaving a pause after pressing the PTT button as well as between transmissions. Just as with any linking system, the IRLP is subject to some audio delays. These delays are caused by the amount of time digital information can take to be compressed and travel across the Internet between the nodes. So the first thing to remember is to slow down and be patient. When in a conversation, remember to leave a second of dead air before speaking. Due to the timing issues with the system some nodes may require a longer period. By leaving a pause between transmissions you:

- Allow users on other nodes a chance to check in.
- Allow other nodes time to send touch-tone commands to drop their node.

IRLP Do's and Don'ts:

- DO pause between transmissions to allow for control codes and to let others in.
- DO hold your microphone PTT for about 1 second before talking to allow all systems time to rise.
- DON'T rag-chew on the local repeater while connected to the IRLP, especially a reflector without someone over the IRLP being a party to the conversation.
- DO pause for 15 seconds when connecting to a reflector to see if other stations are already talking.
- DO identify before sending DTMF command tones to make sure your signal is good enough that you can reliably bring down any connection that you initiate.
- DON'T discuss IRLP link connect/disconnect codes on the air, especially on an IRLP reflector. Please refer people who want information to contact the IRLP Node owner(s) as some club's only allow member access to IRLP just like autopatch on a club system it is a privilege that comes with club membership and they consider it sensitive information.

Making a direct connection:

Note, an IRLP node, depending on how it is sponsored, may require additional code prefixes to access the IRLP and possibly permission or membership in a club to make use of the particular node in question, it is best to inquire with the sponsor as to their rules of access.

As this paper is being written the IRLP is growing rapidly and a few changes are planned to address the growth in IRLP nodes. At present, the standard IRLP node ID is three digits with a suffix digit to make or break the connection as detailed below. However, in the near future the IRLP system will change over to a 4 digit ID for each node. It will at first simply mean adding a zero to all existing three-digit node ID codes. For example, node 728 will become node 7280. When this takes place, there will be no new node ID issued that end in a one (1) for ninety days, however 2-9 will be issued. Also, when the IRLP moves to a 4 digit node ID the standard disconnect code will be "73" to terminate the connection.

The following shall detail how to connection and disconnect using the current 3 digit node ID system.

1. Initiating an IRLP connection is very similar to using an autopatch. First of all, LISTEN on the repeater before transmitting and then ask if the repeater is currently in use. Assuming all is clear and the IRLP link on the node is enabled, identify yourself and say what you are doing. Example: "N2CKH accessing node 728".

Then enter the node ID number plus the standard ON code ("0") for a total of "7280" for node 728 and release your PTT (Remember Standard On code = 0 and OFF code = 1). When the connection is completed the voice ID of the destination node will be transmitted back to you as well as your node's voice ID to the other repeater. NOTE: If the your repeater or the destination repeater is already connected, a message will play to tell you so. After entering codes to bring up a connection you should hear a carrier as the repeater waits for the connection to be established. This can take a few seconds of dead-air so don't be concerned.

2. After hearing the voice ID confirming the connection is established, be sure to listen at least 15 seconds as a conversation may already be in progress. The voice ID of your node is longer than the voice ID of their node, and the connection is not made until the ID is fully played. Their computer may be slower, and hence take longer to process the connection than yours.

3. When you hear the confirmation ID always WAIT at least 15 seconds before transmitting as a QSO (communications) could be in progress. Press and hold the microphone PTT and wait for a second before announcing your presence. Are you calling someone specifically or just looking for a QSO (contact) with another ham in that city?

4. If no response is heard, announce your call and your intent to drop the link and then touch tone in the OFF code. It is not a good idea to transmit touch-tone commands without first giving your call-sign. Not only is this courteous it may be a regulatory issue in the country to which you connected.

Connecting to a reflector:

Reflectors are set up to only allow ONE person to talk at any given time. The reflector will NOT mix audio but instead will allow the first person that transmits to continue talking until they are finished. So there is no point in trying to talk overtop of another node, as you will not be heard. Keep this in mind while using reflectors that due to the delay in the system, you should always leave about 2 seconds between transmissions to ensure that any priority traffic has the chance to talk. Also, if you are not getting through, don't continue to try every transmission, but instead try to wait for a natural break in the conversation. It is the custom that when you "sign on" to an IRLP reflector that you give your geographic location or node you are coming in on.

As above, listen to the local machine and then announce your intention to connect to another node before keying the link on command. After hearing the voice ID confirming the connection is established, be sure to listen at least 15 seconds as you are most likely now connected with many repeaters and a QSO (communications) could be in progress. The voice ID of your node is longer than the voice ID of their node, and the connection is not made until the ID is fully played. Their computer may be slower, and hence take longer to process the connection than yours.

If after 15 seconds you hear nothing, identify yourself and indicate you are listening to the Reflector from "City and State". With the world-wide IRLP activity the repeater now has world wide coverage thus the suggestion to better detail your QTH. Don't be in a hurry to hear someone come back to you. You may have to do a bit of pleading from time to time to un-lodge someone from whatever they are currently doing.

By default, connections to the reflectors DO NOT time out with no activity so it is not unusual for repeaters with minimal traffic to stay connected to the Reflector for extended periods of time. Optionally, node operators may invoke the reflector timeout option on their node. In the case a greeting will precede the timeout saying, "Activity time out ... Reflector two, link off"

Out of courtesy to other node listeners, please do not engage in a prolonged rag-chew on the Reflector.

Error Messages:

From time-to-time you may receive error messages when attempting to connect with a node or reflector. The most common ones are:

- "The node you are calling is not responding, please try again later" This is caused by a loss of Internet connectivity to one end of the call attempt.
- "BEEP Error- The call attempt has timed out, the connection has been lost" This error occurs when a node is OFF-LINE or there is a software error. Some nodes such as in the UK use dial-up connections and then, only for short periods. Also there may be temporary net or node problems.
- "The Connection Has Been Lost" If the Internet connection drops, this error message will be heard.

PHASES OF EMERGENCY MANAGEMENT:

There are four phases of Emergency Management as detailed below, it is the Preparedness, Response and Recovery phases where Emergency Communications and IRLP comes into play.

1. Mitigation: Mitigation activities are those that eliminate or reduce the probability of a disaster occurrence. Also included are those long-term activities that lessen the undesirable effects of unavoidable hazards. Some examples include the establishment of building codes, flood plain management, insurance, elevating buildings, and public education programs.
2. Preparedness: Preparedness activities serve to develop the response capabilities needed in the event of an emergency. Planning, exercising, training and developing public information programs and warning systems are among the activities conducted under this phase.
3. Response: Response activities include direction and control, warning, evacuation and emergency services and are designed to address immediate and short-term effects of the onset of an emergency or disaster. They help to reduce casualties and damage and to speed recovery.
4. Recovery: Recovery includes both short term and long term activities. Short term operations seek to restore critical services to the community and provide for the basic needs of the public. Long term recovery focuses on restoring the community to its normal, or improved state of affairs. The recovery period is also an opportune time to institute mitigation measures, particularly those related to the recent emergency. Examples of recovery actions would be temporary housing and food, restoration of non-vital government services, and reconstruction of damaged areas.

EMERGENCY COMMUNICATIONS AND IRLP:

Entities which make use of the Amateur Radio Service for Emergency Communications need to understand the application and limitations of the IRLP. As the IRLP is a relatively new means of Amateur Radio communications, its impact on Emergency Communications has not yet been felt, however its potential in this regard is huge. To properly utilize the IRLP, it must be used in wide area training drills and not just during emergency situations.

There are any number of different situations and circumstances that might be confronted during an emergency situation. An emergency communications unit should be organized and trained as much as possible to utilize all communications resources to respond to all conceivable scenarios.

Local ARES and RACES operations currently make use of nets on HF, VHF and UHF (simplex and repeaters) using voice, Radio Teletype (RTTY), Packet Radio or other modes such as APRS depending on need and the resources available. These bands and modes are commonly used in daily Amateur Radio operations and are well understood. This wide range of frequencies and modes denotes that flexibility is the keynote. Speaking of APRS, Bob Bruninga, WB4APR, the developer of APRS, has refocused his Automated Voice Relay System (AVRS)⁶ concept for APRS to adapt it for use via IRLP.

However, IRLP is relatively new and not yet widely available, thus most Radio Amateurs have no experience and little understanding of its application to date. OEM planners especially need to be educated on IRLP and understand the application and benefits of IRLP as well as the potential problems in the application of IRLP to both planned training and actual emergency communications. Those in the Federal Government and U.S. Military that may intercommunicate with the Amateur Radio Service must also investigate the Computer Security aspects of the IRLP with respect to direct government interface. It is also possible that IRLP Reflectors and Nodes may be directly hosted behind MILNET firewalls for a national Emergency Communications Network operated by the Military Affiliate Radio System (MARS).

IRLP AND OEM NET APPLICATION:

Local nets which cover small areas such as a community, city, suburban metropolitan area or up to a county usually operate by VHF (typically 2-meter FM) at times and on days that are most convenient to their members. Local nets are intended mainly for local delivery of traffic, inasmuch as such delivery could ordinarily be affected conveniently by telephone. Some local nets operate on a daily basis to provide outlets for locally-originated (i.e. ARRL National Traffic System (NTS)) traffic and to route the incoming traffic as closely as possible to its actual destination before delivery, a matter of practice in a procedure that might be required in an emergency.

At the Statewide and National level, nets usually operate using a combination of RF, Telephone and Satellite linked VHF and UHF repeater systems or High Frequency (HF) Single Sideband (SSB) circuits on frequencies within or adjacent to the Amateur Radio 75/80m and 40m bands to provide an adequate coverage area with minimum propagation effects. However, atmospheric noise on the radio bands, especially during summer months as well as adjacent frequency interference makes the use of HF much more challenging for good quality communications.

Most local nets and even some section nets in smaller sections use repeaters to excellent effect. The average coverage on VHF can be extended tenfold or more using a strategically located repeater, and this can achieve a local coverage area wide enough to encompass many of the smaller sections. Since propagation conditions on HF frequencies are erratic, more use of VHF and repeaters is recommended at local levels. Some nets move from repeater to repeater and alternate with use of simplex for training to be prepared for real life scenarios when a repeater is not available due to system failures attributed to parameters of the current emergency situation such as power failure, downed antenna etc.

In these normal scenarios operators are trained to make use of techniques such as listening to the transmitting stations signal on the input of a repeater system when the station is not putting a good signal into the repeater receiver, aside from a local gateway into the IRLP, this technique cannot be used with IRLP or any linked system unless the station is monitored locally on his/her point of egress into the RF link being received.

HOW DOES IRLP WORK:

The IRLP is a system that runs under Linux, which is a combination of custom executable program utilities and scripting files. The entire system operation is controlled by the action of ANY DTMF sequence passed through the node processed by the custom IRLP DTMF decoder utility which then causes a branch in a script file to call other utilities or script files written to perform specific IRLP functions or custom functions developed by the IRLP user community at large or perhaps only found on a particular node. In this manner, the IRLP is an open platform for future enhancement. Although IRLP is ready to go out of the box, IRLP permits a lot of node customization and experimentation because IRLP is a script driven, open source linking package, it permits node owners to customize the features of their nodes. The changing of IRLP configuration variables in script files and the addition of custom scripts written by the IRLP user community provides for many automated processes, you can use your IRLP machine to play brag messages, bulletins. Two of the custom features that has been added which is very popular is a script which performs an FTP of the weekly Amateur Radio Newslines and ARRL News audio files for later local broadcast on a node by the node owner determined schedule to plan when the node is NOT connected in an IRLP session.

IRLP software takes the audio from the receiver which is fed into a PC sound card where it is converted into ADPCM digital data the same format used by the phone companies for Long Distance service. The Linux PC then converts this digital information into digital packets each assigned with IP addresses for the destination node. These packets now flow through the internet to the destination Linux PC where the packets are decoded then sent to the sound card and out to the transmitter microphone of the link radio which then transmits the audio out over the local repeater. The transmitter is keyed as soon as these TCP/IP (Internet Protocol) packets start to arrive. As soon as the data stops the link radio automatically un-keys and process reverses.

The IRLP uses a Voice-Over-IP (VoIP) streaming software called Speak Freely. The Speak Freely package is very similar to other VoIP software packages (such as Microsoft NetMeeting and VocalTec Iphone) with one major difference, it runs under Linux. Linux is the operating system of choice for the IRLP system as it allows the best in reliability, programmability, efficiency, and functionality. Most IRLP nodes use RedHat Linux as it is a very stable release and runs very smooth on most any 486 or better computer.

The system starts by receiving audio into a radio that has been modified to interface with a computer (using the IRLP interface board). When a signal is received by the radio, the COS state changes. This change is then sent to the interface board, which tells the computer that the COS line is active. This change is picked up by the IRLP software and the computer starts sending a packet stream containing the audio from the receiver. This audio is picked up by the connected computer(s) and played out the sound card. The IRLP software detects the incoming packets and sends a PTT signal to the link radio. Hence the audio from one end is heard on the other.

The concept of IRLP's use of VoIP is as follows:

The radio received audio is sampled using an analog to digital (A/D) converter. The A/D converter used by IRLP is the input source of a standard PC sound card. This creates a continuous mono 8-bit digital stream of raw audio at 8000Hz (64000 bps). The audio is compress by down sampling the stream and using an 8-bit ULAW algorithm to reduce the size of the stream by a factor of two (32000 bps). It is then split into small chunks or packets. The packets are

transmitted to the remote host using User Datagram Protocol (UDP) stream. The UDP does NOT confirm the reception of packets, so it uses a "fire and forget" method. The packets are received on the remote host. The split packets are then joined back together into an 8-bit ULAW stream. The ULAW stream is then un-compressed back into an 8-bit raw stream of audio. The raw audio stream is then played through a digital to analog (D/A) converter, the sound card in your PC. The control software controls the stream using carrier operated squelch (COS) or continuous tone coded sub-audible squelch signals (CTCSS) to start and stop the stream. When COS is present, the computer detects it through the IRLP interface board.

The PTT is controlled by the buffer which joins the split packets back into the audio stream. The IRLP interface board receives a "transmit" signal from the computer while there are packets in the buffer, and an "unkey" command when the buffer is empty.

The user interfaces to the IRLP computer using DTMF signals sent over the radio. DTMF sequences are IRLP node owner programmable, and can accomplish almost any function imaginable. The DTMF signals are detected on the IRLP interface board and sent directly to the computer in binary, where they are converted into numbers. A custom DTMF software program then runs commands on the computer depending on the code entered. These commands are what start and stop Speak Freely, basically establishing and breaking the link. Just as with any linking system, IRLP is subject to some minor audio delays which are mostly radio related. These delays are caused by the amount of time it takes for numerous radios to decode the Tone Squelch information so the first thing to remember is to slow down and be patient. The overall delay involved with the Internet depends on how far the packets have to travel. When the IRLP nodes are fairly close together, the delay is usually less than 0.20 seconds.

ILRP works as most radio systems work, in half duplex, where one side of the connection at a time is transmitting and the other is receiving. Although most of the IRLP systems running run in half-duplex mode, because they are either running on a simplex frequency or accessing a repeater through a half duplex radio. Some systems are capable of running full-duplex, but there are a few software and hardware limitations which do not allow the system to run full duplex in its current configuration.

Although Speak Freely has the ability to run full-duplex and the IRLP interface board was designed with full duplex operation in mind, it not commonly used. As many IRLP users are interested, the system programmers are taking a further look into full duplex linking in the near future. So as a warning to anybody who may be considering moving to full duplex in the future, PLEASE note you will REQUIRE the following:

1. A Creative Labs Sound Blaster 16, AWE32, or AWE64. (ENSURE THAT THE SB16 you purchase is capable of FULL DUPLEX OPERATION)
2. A full-duplex radio link with or without hang time
3. A licensed OSS sound driver from www.opensound.com

EQUIPMENT CONSIDERATIONS FOR IRLP:

Radio Equipment: For entities considering the sponsorship of an IRLP node, both the nature of emergency communications and the high duty cycle on a busy IRLP Reflector in normal daily operation will require transmitters and amplifiers that are rated for continuous duty cycle operation.

For repeater operation, an IRLP node can either be configured with a direct physical connection to a repeater controller on an open two-way port such as a link radio port or 2nd repeater port. It will NOT work on a control receiver receive only port. Optionally, although with more complication, a link radio system on an auxiliary linking frequency can be used with the IRLP Linux computer off sight from the repeater. In addition, where legally permitted, a remote link radio system using a link radio on the standard repeater input/output frequency pair may be utilized.

For repeater or link radio operation, the radio must have a Carrier Operated Squelch (COS) signal available when a signal is present on the receiver's input. If the link radio is to be connected directly to the input/output frequencies of a repeater, the repeater MUST NOT have any hang time, courtesy tones, CW ID or voice brag messages transmitted over the IRLP. This is the complicated aspect of using a link radio in the input/output of a repeater. To achieve this, the repeater control must be programmed to remove these items and make the CW ID as low as possible or the repeater controller or other method must be employed to drop the repeater transmitter PL or DPL on transmit during periods of ID so that the link radio using PL or DPL encode/decode does not receive the transmissions and relay them over the IRLP.

To assure proper operation of the IRLP reflectors there are certain minimum requirements that connecting nodes must meet. These mandatory requirements are necessary to assure those using the reflector do not receive unintentional interference from improperly adjusted or configured nodes.

No repeater tail or any other signal that may keep your nodes COS high when no input signal is present to the node receiver. This includes attempts to notch or turn down the audio on CW ID that still results in a COS signal being sent to the IRLP network and thus an un-modulated carrier on all connected nodes. No Courtesy tones or CW ID to the IRLP other than the occasional CW ID that is overlaid with a voice transmission due to someone transmitting over their local ID. Besides being annoying, the biggest problem with IDs is that every time they play (in the U.S. at least once every ten minutes when active), they key up every node connected to the reflector at the exclusion of all other signals. Remember, on the IRLP the first signal received blocks all others, unlike repeaters where IDs can mix with signals from other users.

No pulsing of the node. This requirement has ZERO tolerance. Pulsing is the single most important item we must prevent and is also the most common reflector issue. Since it is difficult for an offending node to detect this without being proactive, a node can be pulsing and not know it. A pulsing node is one that sends a COS signal to the IRLP network each time another node stops transmitting. The result is that the pulsing node keys up all connected nodes to the reflector each time the carrier of other nodes drops. If two pulsing nodes are connected to a reflector at the same time, it grinds to a halt as the two pulsing nodes will ping-pong pulse each other making the reflector unusable.

It is recommended that all IRLP nodes run PL (CTCSS) or DPL (DCS) decode in addition to Carrier Operated Squelch (COS). It is NOT recommended to run just decode with the squelch open, as a matter of fact, some receivers standard PL decode will NOT provide the needed COS signal if the squelch is left open in addition to the annoying sound caused on the receiver.

If is also required that all IRLP node receivers filter out the PL tone signal on their receivers so as NOT to pass the sub audible tone onto the IRLP which can cause problems for other node owners. Some radios in use such as GE Master II receivers have standard EIA tone filters built in for this purpose.

Also, repeater Autopatch operation must be disabled for an IRLP connection that is active on a reflector or to any international node outside the U.S. The IRLP is international in scope and autopatches (as well as third party traffic) are illegal in some areas. It is actually best if Autopatch is always disabled when IRLP is active.

Computer Hardware for an IRLP Node: The following is the minimum configuration required for running an IRLP node. It has been the author's experience that used IBM Server PC 325 Dual Pentium Pro systems which are Linux certified and available very cheap make excellent IRLP servers.

1. An Intel processor based, dedicated IBM compatible computer, 486 class or better, running a processor with a minimum 100 Mhz. For a Pentium class processor at least 75Mhz is required. A mouse is not needed. A keyboard and video card/monitor (Mono, EGA, VGA etc.) are required for installation and any access to the machine as required but not for daily operation.
2. Memory of at least 16 MB of RAM with 24 MB recommended.
3. One (1) dedicated hard drive (IDE or SCSI) with at least 800 MB free disk space.
4. One (1) 3 ½ inch 1.44MB compatible floppy disk drive. Needed for install and not thereafter, unless used for backup purposes.
5. One (1) CD ROM drive. Needed for install and not thereafter.
6. One (1) standard parallel port running LPT1 (HEX address 0x378 or 0x379).
7. One (1) ILRP certified sound card such as a genuine Creative Labs ISA SoundBlaster 16 or AWE 32 soundcard (No clones accepted, PCI cards will require additional commercial drivers).
8. One (1) Red Hat Linux supported Ethernet network interface cards.
9. One (1) routable IP address Internet connection and seven (7) ports per IRLP node is required. An IRLP node can exist behind a firewall by making additional configuration settings.
10. A Cable modem, xDSL or ISDN (single dedicated ISDN 64KB channel or undedicated dual channel will work fine) connection with the ability to sustain 80000 bps (8K/sec). A router is not needed, but can be utilized as the network configuration may warrant. For those lucky enough, a drop off a T1 Line would be better.
11. Although a Static IP is desirable, a Dynamic (variable) IP address will work just fine. Static hostnames are beneficial but unnecessary as the IRLP system uses its own Dynamic Name Server

(DNS) to resolve IP addresses. What not having a Static IP address will mean is that should/when the nodes IP address change, until the IRLP DNS can be updated, the node can connect out but no connection to it can be made. If the node in question uses a dynamic IP address, you can register a domain with a company that will point people to a Dynamic IP addresses using a fixed IP address, many require a fee to do so.

Other IRLP Node Hardware:

1. Custom IRLP interface board and LPT to IRLP board cable. This interface board does not need to be installed in the Linux PC, however that is the best place for it and as delivered is configured for PC mounting and D.C. power connectivity.
2. Miscellaneous cables and connectors wired by the node owner to interface to the IRLP interface board and PC Sound Card for connection to repeater controller or link radio or simplex node radio for Ground, Push-to-Talk (PTT), Carrier Operated Squelch (COS), Transmit Audio, Receive Audio.

Operating System for IRLP node:

1. Red Hat Linux 6.2, running a kernel of 2.2.14 (basic Red Hat 6.2 Workstation install) configured for Text Only operation without mouse support.
2. Licensed OSS sound driver may be required if your sound does not work properly. (IRLP assistance in obtaining this will be provided).

Computer Hardware for an IRLP Reflector: A reflector requires only a dedicated Linux computer and an Ethernet Interface card. It does not require any IRLP hardware or radio equipment and it cannot operate on the same machine as an IRLP node. The bandwidth runs 32K per connection, linear equation, plus a tiny bit more for "overhead". The big thing about the connectivity is that it must have good routes to all the other major backbone providers. If there's a bottleneck between say, UUNet and Sprint and you're on Sprint's backbone, you'll have any users that are coming in through UUNet's backbone complaining of packet loss. However, most of the carriers have good interconnectivity these days. The following is the required minimum configuration for running an IRLP reflector.

1. An Intel processor based, dedicated IBM compatible computer, 486 class or better, running a processor with a minimum 100 Mhz. For a Pentium class processor at least 75Mhz is required. A mouse is not needed. A keyboard and video card/monitor (Mono, EGA, VGA etc.) are required for installation and any access to the machine as required but not for daily operation.
2. Memory of at least 16 MB of RAM with 24 MB recommended.
3. One (1) dedicated hard drive (IDE or SCSI) with at least 800 MB free disk space.
4. One (1) 3 ½ inch 1.44MB compatible floppy disk drive. Needed for install and not thereafter, unless used for backup purposes.
5. One (1) CD ROM drive. Needed for install and not thereafter.
6. One (1) Red Hat Linux supported Ethernet Network Interface card.

7. One (1) routable IP address Internet connection and seven (7) ports. An IRLP Reflector can exist behind a firewall by making additional configuration settings.

8. A Cable modem, xDSL or ISDN (single dedicated ISDN 64KB channel or undedicated dual channel will work fine) connection with the ability to sustain 32000 bps (32K/sec) per connection. A router is not needed, but can be utilized as the network configuration may warrant. For those lucky enough, a drop off a T1 Line would be better.

9. A real Static IP address is required for a reflector.

Operating System for IRLP Reflector:

1. Red Hat Linux 6.2, running a kernel of 2.2.14 (basic Red Hat 6.2 Workstation install) configured for Text Only operation without mouse support.

IRLP NODE LINUX SERVER ADMINISTRATION:

The initial install and setup of Linux and the IRLP software with the supplied IRLP package and directions are straight forward and almost fool proof. With the exception of the new IRLP node owner needed to make some decisions as to addressing and user name and password selections, everything else is provided in black and white. In addition, the default configuration settings will allow for basic IRLP operation without further intervention.

However, to get the most from the IRLP system an effort should be made to learn the IRLP system and tweak the default configuration to optimize node operation. The advanced user may want to use their IRLP node for more advanced functions. The simple interface combined with the computer allows several software based functions to be performed by the IRLP node. Almost any feature of a repeater controller besides port linking can be performed in software using your IRLP node. Some which that have been done or are planned to be done are:

- Pre-recorded announcements
- Retrieval by FTP and Playback of Amateur Radio Newslines
- Retrieval by FTP and Playback of ARRL News
- Voice ID system for your local repeater
- Time/Date on demand
- Voicemail message system for your repeater
- Weather alert/Weather forecast
- Interactive and automatic Swap and Shops
- Online DTMF decoder with playback
- DTMF macro playback
- Signal Check voice playback

Administration of an IRLP node will require experience with Linux. It is not possible to administer a Linux-based computer with only a MS-Windows or Apple Mac background without taking the time to learn a number of Linux fundamentals. It is much easier to do serious damage in Linux logged in as the root user than one can do in an MS-Windows environment. Then there is the learning curve regarding the IRLP system files running on Linux to achieve, this is true even of a Linux expert as IRLP is script file driven and those script files require understanding.

An IRLP node is maintained in two ways, via automation provided by the IRLP system daily for certain system files and periodically for new code releases of both IRLP and Linux files and manually by node administrator editing system and IRLP scripting files.

An IRLP node may also be controlled in two ways, either by radio using DTMF signaling or manually by the node owner or administrator via the PC keyboard or via a remote administration session. There are several IRLP specific commands which can be entered from the command line to control a node, many mimic DTMF control functions and others are for both testing and local control as may be needed. A node owner could open a Telnet session or better yet a secure Secure Shell (SSH) session and login remotely to have direct control over their node when out of reliable RF access. The standard installation of Linux includes Telnet support, however SSH must be installed separately as it is data encryption that cannot be exported without a license.

To administer an IRLP server the main concerns are the editing and backup of both system and IRLP Shell Language script files, validating that AutoRPM is properly functioning, AutoRPM will e-mail the root user with information about what it did when it ran as it runs from cron regularly to keep the system updated. Also, properly shutting down the system both automated during power failures, preferably tied into a smart UPS and manually as required comes under the role of system administration. Should there be more than one person performing maintenance and augmentation to the IRLP server, then the Administrator will also need to maintain other users as well and for certain functions may need to share root privileges, however, bear in mind again, it's easy to do serious damage in Linux as user root.

FREQUENCY COORDINATION AND IRLP:

If an IRLP node is hosted on a repeater, then all standard FCC coordinated repeater station⁴ rules regarding frequency coordination apply. Within the U.S. it is highly recommended that a node operator hosts their node on a coordinated repeater, for a listing of frequency coordinators refer to the National Frequency Coordination Council (NFCC) web site at: <http://www.arrl.org/nfcc/>

However, the coordination and use of simplex frequencies for IRLP has been a topic of much discussion due to the interference it can cause for other regular users of simplex frequencies and because two stations might not hear each other but try to work the local node at the same time. As of this writing, there is not any requirement for IRLP simplex node frequency coordination by the FCC within the U.S. Furthermore, to the author's knowledge and no Frequency Coordinator has yet done so.

An IRLP node should not be on a calling frequency like 146.52 nor 446.00 or on any simplex frequency within the planned nodes geographical service area that is already in heavy use by the local Amateur Radio community. Instead, it has been suggested that the IRLP community work out an international "NODE" channel for simplex nodes, just like APRS etc., which would comply with ARRL band plan standards. The segments 145.500-145.800Mhz and 445.000-447.000Mhz would be ideal (except around 446.00). Alternately, less used "Simplex" channels could be used by local option such as 146.49 or 146.58 or the 15khz splinters, if properly coordinated. However, in many densely populated areas one (1) Megahertz split repeaters have been slipped in such as 146.490/147.490Mhz etc. to preclude use of standard 2m simplex as an option.

All linking within the U.S. per the FCC must be at 222Mhz and above and again frequency coordination comes into play.

POSSIBILITY OF IRLP DISRUPTION DUE TO HACKING:

Since IRLP utilizes the Internet, the question of security can be raised regarding an IRLP server, reflector or node being hacked.

The IRLP system runs its own Dynamic Name Server (DNS) to allow ONLY authenticated IRLP nodes to connect to each other, and protects the sites from the rest of the Internet. IRLP is the only Amateur Radio Internet based linking system known to use modern cryptographic authentication. IRLP only allows RF gateways to connect via an IRLP node, there is no PC to IRLP node or PC to PC communications allowed.

All IRLP TCP connections are logged by verified spoof-free corrected IP address. The TCP calls are authenticated using a technology accepted in the industry as "secure", namely Pretty Good Privacy (PGP). A dual challenge/response 512 bit PGP key controlled by the IRLP is used to challenge each connection to authenticate nodes, minimizing the risk of someone coming in the "back door" and tampering with normal operation of the IRLP system. The PGP key is created ONLY by the IRLP Installer and uploaded to the master IRLP server. Only IRLP nodes with valid PGP keys can add their IP to the IRLP IP list. Secure reflectors are firewalled to allow only IP addresses of valid IRLP nodes to communicate, preventing others from listening or talking. The program which decodes the IRLP audio and plays it over the repeater will ONLY allow audio packets to be played by an IP address which is defined when the program is started. This MUST be an IRLP node IP, and this ensures ONLY IRLP nodes can send audio to your IRLP node.

A properly installed and maintained Linux computer is much more secure than an equivalent MS-Windows computer. There are a few services that are problematic, but if they are avoided or kept up to date, the chance of being hacked is minimal. In addition, the IRLP install instructions specifically state to shut down several services as SOON as the Red Hat software is installed as follows:

1. FTP servers - wu-ftpd and others
2. DNS servers - bind
3. RPC (Remote Procedure Call) services (Portmap, rpc.mountd)
4. Network File Systems
5. Samba (MS-Windows/Linux file sharing utility)

IRLP DISRUPTION ATTRIBUTED TO JAMMING OR INTERFERENCE:

Just as in normal RF based simplex or repeater operation, a jammer can transmit a signal or some form of interference can develop on the RF point of egress into an IRLP node and cause interference not only on that node but all nodes (two or more nodes if an IRLP reflector is being utilized) connected.

However, when a reflector is being utilized, an IRLP Control Operator can see what node is hanging open the network and can then disconnect that node from the network. In the case of a node to node contact the problem will either have to be tolerated or the connection will need to be terminated.

As a one-on-one IRLP node-to-node connection does not allow for a third node to be connected no unexpected connections can be made. In addition, a reflector can be configured so that only a specified group of IRLP nodes can connect to the given reflector. These two characteristics of the IRLP infrastructure minimize the potential for jamming.

Note, should a node owner perform the required Full Duplex modification to their IRLP interface board, then a connection can be dropped even though the node to be dropped is currently receiving the transmission of another node. However, making this modification will also allow the modified nodes local transmissions onto the IRLP where normally a local control function can be performed such as just turning off the local repeater controller IRLP port or other needed local signaling while IRLP transmissions are being received.

INTERNET SERVICE DISTURBANCE AND IRLP:

The Internet is the largest worldwide computer network that uses the TCP/IP protocols. The Internet is the world's largest distributed system; it was designed and engineered for redundancy it has an abundance of routes and connections and resilience, it easily recovers from a mishap. The Internet is not a single company or a group of companies, nor even a single network.

The Internet is a worldwide mesh or matrix of hundreds of thousands of networks, owned and operated by hundreds of thousands of people in hundreds of countries, all interconnected by about 8,000 Internet Service Providers (ISP). No single organization controls the Internet; not the U.N.; not the biggest ISPs; and the Internet has long since outgrown control by the U.S. government.

Much rerouting in the Internet is dynamic, and happens automatically. Some rerouting isn't automatic. In particular, the biggest ISPs, frequently called backbones, cover vast geographical areas and carry large proportions of the Internet's traffic. A failure in a backbone or in one of the major interconnection points between them can affect many Internet users. And such a problem may take some time to be resolved, as the biggest ISPs often prefer to manually examine changes in major routes before implementing them. However, longstanding observation of the Internet indicates that "some time" is normally at most few hours, even in the face of the biggest problems, however a few hours outage during Emergency Communications would be a major problem depending on the geographic area of the backbone coverage area and the given Emergency geographic area overlap.

The decentralization of the Internet is one of its biggest advantages and one of its most basic features, designed into its protocols from the beginning and tested in practice over many years. If one piece breaks, that doesn't mean the Internet is broken. And decentralization requires cooperation, so the various ISPs and Internet Exchange Points (IXs) and the like are accustomed to cooperating with one another to fix and prevent problems. It is this decentralization and cooperation that has permitted the Internet to grow faster for longer than any other technological phenomenon in history. It is important for you, the user, to understand how decentralization makes the Internet work, so that you will know that the Internet is actually very hard to break.

Thus, should there be a major key outage of Internet service, the rerouting time and extra loads on those paths will likely cause a slowing of the Internet and possible packet loss as well as connectivity problems in certain geographical areas. As the IRLP nodes and reflectors are geographically decentralized as well, in some cases by continents, an alternate independent reflector will most likely be available. However, if a major backbone outage is in the

geographical area of the emergency at hand, many if not all IRLP nodes in the area of the emergency situation may be affected as well.

POWER LINE DISTURBANCE AND IRLP:

Just as in all forms of radio communications, a source of Alternating Current (A.C.) and or Direct Current (D.C.) power is required for the operation of the communications system equipments. Most communications systems can be directly powered from a fixed 13.8 volt or 28 volt D.C. power source, which means in times of A.C. power mains interruption, the communications equipment can work off of battery backup systems that have been kept charged. Some systems are configured to charge from both solar and commercial mains and in the case of a commercial mains outage charge from the solar sub system.

However, with IRLP we need to power the Linux PC server, although a PC is also D.C. powered at the mother board level, a number of different D.C. voltages are required. Thus a PC is usually kept alive in a power outage by an Uninterruptible Power Supply (UPS) or D.C to A.C. Inverter. There are a number of differences between a UPS and an Inverter, both are used to convert D.C. into A.C. to power devices that normally run of A.C., the main difference being that a UPS is self-contained with one or more D.C. battery internally and configured for automatic backup. In addition the UPS provides a much cleaner A.C. power source and provides additional filtering of the commercial A.C. mains when it is not running off the back up batteries.

With respect to Emergency Communications and IRLP, both the local and remote IRLP nodes equipments and any IRLP Reflector being used must remain powered under all circumstances to be of use. This also takes into account the local ISP and all upstream Internet connections as well. Should any point in the IRLP network suffer a loss of power then that network path will not be available, thus alternate IRLP nodes and reflectors need to part of the planning just as alternate repeaters are part of the current planning.

ADVANTAGES OF IRLP IN EMERGENCY COMMUNICATIONS:

The following list of advantages are not provided in any particular order of importance.

- * Wide area on demand communications links from county, state, nationwide as needed to meet the demand of the situation.
- * Wide area training nets
- * Full time Private Emergency Communication nodes using custom access prefixes can be configured.
- * Full time Private Emergency Communication reflectors can be configured.
- * Node blocks/lockouts list can be created to restrict access from undesired node connections.
- * For special circumstances at an ECC where an outside antenna is not feasible and hand held communications are not feasible such as below ground, if Internet connectivity is available an IRLP node can be set up with an indoor antenna or even a dummy load for full wide area access.

* Unlike other wide area linking methodologies, when an IRLP reflector is used, a control operator can detect what node is interfering with communications immediately and disconnect the offending node.

* A node owner can telnet into their node for remote maintenance and control. If they have radio reception of the node for the remote location they can actually perform control operator functions.

DISADVANTAGES OF IRLP IN EMERGENCY COMMUNICATIONS:

The following list of disadvantages are not provided in any particular order of importance.

* Timing delays across the Internet to key all connected repeaters/remote bases of about 2 seconds require a pause after PTT engage before talking. It is also recommended that 2-4 four seconds pause be provided between exchanges to allow other parties to drop their node connection under normal daily operation. This may/may not be of concern in Emergency communications application.

* When a signal at an RF point of egress into the network locks the network open, no signal except a strong enough RF signal on the same point of egress can override the offending signal. This prevents a node from dropping their connection from the offending node under normal circumstances. If a reflector connection, it prevents all node from dropping their connection to the reflector, however a reflector control operator can drop the offending node. In addition, the IRLP interface board can be modified to allow DTMF signaling to drop a node while another node is still transmitting. Also note, most repeater controllers allow DTMF signaling to disable the remote/repeater port that the IRLP hardware is connected to.

* Internet packet loss which sounds similar to FM picket fencing, but much sharper due to the digital brick wall effect on the lost digital data is caused by a poor route through a major backbone provider, say a bottleneck between UUNet and Sprint if you're on Sprint's backbone, you'll have any users that are coming in through UUNet's backbone complaining of packet loss.

* Although it one of the downfalls to the IRLP Reflector is that rarely occurs and is shorted lived, it currently has no ability to limit the input stream. If more than one stream hits the reflector at the same time, both signals will be repeated in a time-share fashion, which makes both streams unreadable. With active Fire Walling, the first signal to reach the reflector will capture the input port and not release it until the stream has ended. This part of the IRLP is still in development.

* For a Dynamic (variable) IP address node, until the IRLP DNS can be updated, the node can connect out but no connection to it can be made. When and if this happens, it is short lived. As the IRLP Server handles the software updates, including the hosts file, on the rare occasions that the IRLP server goes down, the hosts file on each node will not update (which usually happens every few minutes) and any nodes whose IP addresses have changed will not be able to receive calls until the hosts file is updated (you can't find someone if you don't know their address). Nodes with changed IP addresses will be still able to call out to nodes and reflectors whose addresses still match what is listed in the hosts file. If this happens to you and you're having trouble meeting people on skeds, try scheduling to meet them on a quiet reflector.

* Unlike Simplex operation, Repeaters and IRLP nodes have timeouts. Even a Simplex IRLP node will have a timeout as timeout timers are hard coded in the IRLP software and

programmable by the IRLP node owner. The standard Push-to-Talk (link radio RX from IRLP) is set for 5 minutes. The COR (link radio RX locally) is set for 4 minutes. The standard COR Timeout will disable the node, and require the use of the Node enable command. The PTT timeout will drop the node from the connection but will leave the node enabled. This is all subject to configuration, to include overrides on the particular node being used.

OTHER INTERNET LINKING METHODS:

The IRLP as detailed previously was not the first and more than likely will not be the last method developed to utilize the Internet for linking Amateur Radio communications. However, it is one of the two most popular methods at this point in time and in the author's opinion the best to be developed to date and the only system to run under Linux.

The iLINK (<http://www.aacnet.net>) system is the other popular system currently in use, it runs under MS-Windows and it has received more Amateur related media attention as the MS-Windows operating system is more popular with the Amateur Radio community just as it is with the general consumer public. iLINK was released in May of 2001 by Graeme Barnes, M0CSH of Kent, U.K. who felt that Linux and only being able to use radios for communications egress and not a PC was a limitation.

IRLP & iLINK are both simply means of linking Remote Bases and Repeater Systems via the Internet, however IRLP and iLINK have two (2) different philosophies regarding egress into the Amateur Radio spectrum. The following must be taken into account when comparing IRLP and iLINK:

- IRLP is the only system known to use modern cryptographic authentication
- IRLP only allows RF gateways to connect and they authenticate each other using a technology accepted in the industry as "secure", namely PGP
- IRLP uses a 512 bit PGP key challenge on each connection to authenticate nodes, minimizing the risk of someone coming in the "back door" to prevent hackers.
- iLINK allows PC with soundcard microphone and speakers to link into Amateur Radio circuits using Internet (IRLP does **NOT** allow this).
- iLINK allows PC with soundcard microphone and speakers to link to another PC using Internet (IRLP does **NOT** allow this).
- iLINK allows the possibility of unauthenticated users (its security method is looking up call signs on QRZ and QRZ is not a secure means of authentication - ask any security professional) to access the system from a PC into Amateur Radio RF gateways.

Similarities between IRLP and iLINK:

- Both connect Amateur Radio stations around the world via the Internet.
- Both use Voice-over-IP (VoIP) technology.

- Both have security weaknesses of unlicensed users. However with IRLP such unlicensed use is the same as it has always been, a radio must be used illegally by a bandit.

CONCLUSION:

The IRLP provides an additional means of wide area communications in support of Emergency Communications that provides for on-demand linked communications circuits to meet the needs of the emergency situation in effect. The characteristics of FM VHF and UHF radio will provide for the highest quality communications yet available to the Amateur Radio Service Emergency Communications community.

An infrastructure of regional IRLP Nodes and Reflectors specifically in place to support Emergency Communications and the large number of independently owned and operated IRLP nodes which can be pressed into Emergency Communications service will provide for unparalleled battery powered, hand held, low power wide area communications.

The use of IRLP nodes will mandate that sufficient efforts must be undertaken to provide for backup power operation. In addition, the hosting of IRLP reflectors for use in Emergency Communications where the physical server resides outside of the actual geographic area of the user community will likely guarantee that the IRLP reflector server is not subject to Internet service disruption or commercial power line disruption attributed to the situation at hand unless it is a very far geographical ranging scenario.

The use of IRLP will require additional training of personal, however the benefits of IRLP far out weigh the additional training efforts required. The use of IRLP will actually enhance training in a number of ways for emergency communications in that it will allow for wider area training nets.

There are already a number of Amateur Radio Emergency Communications⁷ entities making use of IRLP that have some experience with the mode to the extent that they have even funded, own and operate their own node. These entities are the most valuable starting point in a line of communications for an Emergency Management official to make contact with regarding their experience to date and recommendations as to where and how to get started with IRLP for Emergency Communications.

GLOSSARY

ADPCM: Adaptive Differential Pulse Code Modulation

ADAPTIVE DIFFERENTIAL PULSE CODE MODULATION: A method of encoding sound data files that takes up less storage space than the regular PCM format used by .WAV and .AIFF files. It is a family of speech compression and decompression algorithms. A common implementation takes 16-bit linear PCM samples and converts them to 4-bit samples, yielding a compression rate of 4:1.

AMATEUR RADIO: Amateur Radio is as old as the history of radio itself. In 1912, Congress passed the first laws regulating radio transmissions in the US. By 1914, amateur experimenters were communicating nation-wide, and setting up a system to relay messages from coast to coast.

AMATEUR RADIO EMERGENCY SERVICE: Per the ARRL, Part 97 of the FCC's RULES and REGULATION, which covers the Amateur Radio Service in the U.S., states under "Basis and Purpose" in 97.1 (a) that: "Recognition and enhancement of the value of the amateur service to the public as a voluntary non-commercial communication service, particularly with respect to providing emergency communications." ARES consists of licensed amateurs who have voluntarily registered their qualifications and equipment for communications duty in the public service when disaster strikes. Every licensed amateur, regardless of membership in ARRL or any other local or national organization, is eligible for membership in the ARES. The only qualification, other than the possession of an Amateur Radio license, is a sincere desire to serve. Because ARES is an amateur service, only amateurs are eligible for membership. The possession of emergency-powered equipment is desirable, but is not a requirement for membership". Part 97 of the FCC's RULES and REGULATION, which covers the Amateur Radio Service in the U.S., states under "Basis and Purpose" in 97.1 (a) that: "Recognition and enhancement of the value of the amateur service to the public as a voluntary non-commercial communication service, particularly with respect to providing emergency communications."

AMATEUR RADIO OPERATOR: A licensed operator within the Amateur Radio Service.

AMATEUR RADIO SERVICE: Per the FCC, "The amateur and amateur-satellite services are for qualified persons of any age who are interested in radio technique solely with a personal aim and without pecuniary interest. These services present an opportunity for self-training, intercommunication, and technical investigations". Per the International Telecommunication Union (ITU), "A voluntary noncommercial communication service, particularly with respect to providing emergency communications. A radio communication service for the purpose of self-training, intercommunication and technical investigations carried out by amateurs, that is, by duly authorized persons interested in radio technique solely with a personal aim and without pecuniary interest".

AMATEUR STATION: Per in 47 C.F.R. § 97.3(a)(5): A station in an amateur radio service consisting of the apparatus necessary for carrying on radio communication.

AMERICAN RADIO RELAY LEAGUE: The American Radio Relay League is the principal representative of the Amateur Radio Service in the USA, serving members by protecting and enhancing spectrum access and providing a natural resource to the public. Amateur Radio is as old as the history of radio itself. In 1912, Congress passed the first laws regulating radio

transmissions in the US. By 1914, amateur experimenters were communicating nation-wide, and setting up a system to relay messages from coast to coast which is how the American Radio Relay League or ARRL, for short come into existence.

APRS: Amateur Packet/Position Reporting System

AMATEUR PACKET/POSITION REPORTING SYSTEM: A means of transmitting GPS referenced location telemetry over Packet radio so that a suitably equipped computer can display your location on a map. This is particularly useful mode in Emergency Communications when there is a need to know all stations locations. Textual data and Weather information can also be transmitted.

ARES: Abbreviation for Amateur Radio Emergency Service

ARRL: Abbreviation for American Radio Relay League

AUTOPATCH: A semi-automatic means of affecting a telephone interconnect using a repeater station.

CABLE MODEM: A cable modem is a device that enables a PC interface to a local cable TV provider 75 ohm coaxial line to receive data at about 1.5 Mbps. This data rate far exceeds that of the prevalent 28.8 and 56 Kbps telephone modems and the up to 128 Kbps of Integrated Services Digital Network (ISDN) and is about the data rate available to subscribers of Digital Subscriber Line (DSL) telephone service. A cable modem has two connections: one to the 75 ohm coaxial cable other to a PC. Although a cable modem provides for modulation between analog and digital signals, it is a much more complex device than a telephone modem. Typically, the cable modem attaches to a standard 10BASE-T Ethernet Network Interface card in the PC using CAT-5 cable or to the PC Universal Serial Bus (USB) port using a standard USB port cable.

All of the cable modems attached to a cable TV company coaxial cable line communicate with a Cable Modem Termination System (CMTS) at the local cable TV company office. All cable modems can receive from and send signals only to the CMTS, but not to other cable modems on the line. Some services have the upstream signals returned by telephone rather than cable, in which case the cable modem is known as a telco-return cable modem.

The actual bandwidth for Internet service over a cable TV line is up to 27 Mbps on the download path to the subscriber with about 2.5 Mbps of bandwidth for interactive responses in the other direction. However, since the local provider may not be connected to the Internet on a line faster than a T-carrier system at 1.5 Mbps, a more likely data rate will be close to 1.5 Mbps.

CLOSED REPEATER: An Amateur Radio Service repeater station that restricts access to the repeater station to specific licensed Amateur Radio operators.

CONTINUOUS TONE CODED SQUELCH SYSTEM: A set of standard sub-audible frequencies present as a continuous fixed frequency audio tone used to activate a receiver. The frequency range of 67 Hz to 255 Hz is used. These tones are called sub-audible because communications receivers use 300 Hz to 3000 Hz for voice communications

COORDINATED STATION: Per 47 C.F.R. § 97.3(a)(20): A station that operates according to recommended transmit/receive channels and associated operating and technical parameters.

COURTESY TONE: One or a series of audible tones to indicate that the previous transmission has completed that the repeater time-out timer has reset and that it is now ok for the next transmission to begin.

CTCSS: Continuous Tone Coded Squelch System

CW ID: Continuous Wave (International Morse Code) identification used to automatically send out the station ID periodically to identify the owner of the transmitting repeater station to satisfy the requirements of the FCC for automatic station identification.

DCS: Digital Coded Squelch

DIGITAL CODED SQUELCH: Similar to CTCSS except a continuous sub-audible digital code is substituted for the continuous fixed frequency audio tone.

DIGITAL PRIVATE LINE: Similar to Private Line except a continuous sub-audible digital code is substituted for the continuous fixed frequency audio tone.

DIGITAL SUBSCRIBER LOOP: A family of technologies generically referred to as DSL, or xDSL, capable of transforming ordinary phone lines (also known as "twisted copper pairs") into high-speed digital lines at speeds up to 1.2Mbps, capable of supporting advanced services such as fast Internet access and video-on-demand. ADSL (Asymmetric Digital Subscriber Line), HDSL (High data rate Digital Subscriber Line) and VDSL (Very high data rate Digital Subscriber Line) are all variants of xDSL. DSL is limited by availability and distance from telephone Central Offices (COs).

DNS: Dynamic Name Server

DPL: Digital Private Line

DSL: Digital Subscriber Loop

DTMF: Dual-Tone Multifrequency

DUAL-TONE MULTIFREQUENCY: A signaling and control system used originated by the telephone industry for touch-tone telephones. DTMF assigns a specific set of frequencies, or tone pairs, to each key pressed on a DTMF keypad.

DYNAMIC IP ADDRESS: A Dynamic IP address is one that is temporarily assigned to a user by their Internet service provider every time the connect. This cuts down on the number of IP addresses large consumer provider's need because not all of their customers are using the service at any given time. It also cuts down on bandwidth usage by preventing consumers from hosting servers. Note: Recently a number of companies have started to offer services aimed at updating DNS for dynamically connected clients.

DYNAMIC NAME SERVER: Service that provides domain name resolution. A DNS Server is any piece of software that serves as a name server, a resolver, or both.

EMERGENCY COMMUNICATIONS:

EMERGENCY MANAGEMENT: Organized analysis, planning, decision making and assignment of available resources to mitigate (lessen effect and/or prevention of disasters), preparation for, response to and recovery from the effects of ALL hazards. Main goal of EM is to save lives, prevent injuries and protect property and the environment if an emergency occurs.

ETHERNET: The most popular LAN technology in use today. An Ethernet specification commonly defined by the Institute of Electrical and Electronic Engineers (IEEE). The 802.3 specification covers rules for configuring Ethernet LANs, the types of media that can be used, and how the elements of the network should interact.

FCC: Federal Communications Commission

FEDERAL COMMUNICATIONS COMMISSION: Per the FCC, The Federal Communications Commission (FCC) is an independent United States government agency, directly responsible to Congress. The FCC was established by the Communications Act of 1934 and is charged with regulating interstate and international communications by radio, television, wire, satellite and cable. The FCC's jurisdiction covers the 50 states, the District of Columbia, and U.S. possessions. The Commission's jurisdiction over interference matters is set forth in Section 302(a) of the Communications Act of 1934, as amended, 47 U.S.C. § 302(a). It is clear from the report of the Joint Committee of Conference, H.R. Report No. 765 97th Cong., 2nd Sess., that the congress intended that the Commission have exclusive jurisdiction over interference to home electronic equipment.

FEMA: Federal Emergency Management Agency

FEDERAL EMERGENCY MANAGEMENT AGENCY: A federal agency that coordinates communications, resources and training nationwide for disasters.

FM: Abbreviation for Frequency Modulation

FREQUENCY COORDINATOR: Per 47 C.F.R. § 97.3(a): An entity, recognized in a local or regional area by amateur operators whose stations are eligible to be auxiliary or repeater stations, that recommends transmit/receive channels and associated operating and technical parameters for such stations in order to avoid or minimize potential interference.

FREQUENCY MODULATION: Per Federal Standard 1037C, Frequency Modulation is where the instantaneous frequency of a sine wave carrier is caused to depart from the center frequency by an amount proportional to the instantaneous value of the modulating signal.

FTP: File Transfer Protocol

FILE TRANSFER PROTOCOL: A standard Internet protocol, is the simplest way to exchange files between computers on the Internet that uses the Internet's TCP/IP protocols.

HANG TIMES: The time a repeater controller is programmed for to keep the repeater in transmit before dropping after a user releases the PTT on their transmitter.

HF: Abbreviation for High Frequency

HIGH FREQUENCY: Per Federal Standard 1037C, frequencies from 3 MHz to 30 MHz

INTERNET EXCHANGE POINT: A public Internet peering point

INTERNET RADIO LINKING PROJECT: The aim of this project is to link radio systems separated by long distance without the use of expensive leased lines, satellites, or controllers. The IRLP uses Voice-Over-IP software and the power of the Internet to link your radio site to the world. The system uses its own custom interface board and software suite which makes interfacing your radio system to the world simple and cost effective. The IRLP runs a large network of dedicated servers and nodes to offer the very best in voice communications. The heart of the IRLP is its Amateur Radio network which reaches hundreds of towns and cities across North America, linking them all with a full dynamic range, telephone quality sound.

IONOSPHERE: Per Federal Standard 1037C, that part of the atmosphere, extending from about 70 to 500 kilometers, in which ions and free electrons exist in sufficient quantities to reflect and/or refract electromagnetic waves

Integrated Services Digital Network: A telecommunications standard for digital transmission of voice, video and data. Ordinary phone lines are used to transmit digital instead of analog signals, allowing data to be transmitted at a much faster rate than with a traditional modem.

INTERNET PROTOCOL ADDRESS: This address is a unique string of numbers that identifies a computer on the Internet. These numbers are usually shown in groups separated by periods, like this: 123.123.23.2. All resources on the Internet must have an IP address--or else they're not on the Internet at all.

IP ADDRESS: Internet Protocol Address

IRLP: Internet Radio Linking Project

IRLP ECHO REFLECTOR: A special IRLP reflector running on an IRLP Server that is for use in the initial setup and subsequent testing of the audio of an IRLP node. The Echo Reflector will simply record ten seconds of transmission and plays back whatever it recorded for ten seconds.

IRLP NODE: A single IRLP Linux server connected to a simplex radio or repeater.

IRLP NODE ID: IRLP nodes and reflectors are currently assigned a three digit numerical ID code which will support up to a total of 999 nodes.

IRLP SERVER: Handles the connections being made by IRLP nodes, IRLP software updates (including the hosts file) as well as the Echo Reflector which is used for node testing

IRLP REFLECTOR: A reflector can be seen as a digital repeater of sorts, it acts as a centralized connection point to bridge an almost unlimited number of IRLP nodes together. An IRLP Reflector is simply a Linux server that is not physically connected to any radio equipments but rather permits an IRLP node to be connected by streaming received audio back to all connected nodes. It takes one digital bit stream in, and repeats that bit stream to all other connected sites making a digital "partyline".

ISDN: Integrated Services Digital Network

ISP: Internet Service Provider

INTEGRATED SERVICES DIGITAL NETWORK: Commonly called ISDN, is a set of communications standards allowing a single wire or optical fiber cable to carry voice, digital network services and video as an integrated digital network in which the same time-division switches and digital transmission paths are used to establish connections for different services. ISDN offers transfer speeds of 64 Kbps on one of two channels or 128 Kbps when both channels are combined.

INTERNET: This worldwide network is comprised of thousands of interconnected computer networks, and reaches millions of people in many different countries. The Internet was originally developed for the United States military, and then became used for government, academic and commercial research and communications. The Internet is made up of large backbone networks (such as MILNET, NSFNET, and CREN), and smaller networks that link to them. The U.S. National Science Foundation maintains a major part of the backbone (NSFNET). The Internet functions as a gateway for electronic mail between various networks and online services. The World Wide Web facility on the Internet makes possible almost instantaneous exchange of information by linking documents around the world. Internet computers use the TCP/IP (Transmission Control Protocol/Internet Protocol). There are over six million hosts on the Internet: mainframes, minicomputers or workstations that support the Internet Protocol. The Internet is connected to computer networks worldwide that use various message formats and protocols; gateways convert these formats between networks so that the Internet functions as one big network. The Internet sometimes appears to be amorphous and unregulated, but there are several administrative bodies: the Internet Architecture Board, which oversees technology and standards; the Internet Assigned Numbers Authority, which assigns numbers for ports and sockets, etc.; InterNIC, which assigns Internet addresses; the Internet Engineering and Planning Group, Internet Engineering Steering Group, and the Internet Society.

INTERNET SERVICE PROVIDER: A company that provides Internet service. The Internet is centered around thousands of ISPs.

IX: Internet Exchange Point

LINUX: Linux (often pronounced LIH-nuhks with a short "i") is a UNIX-like operating system (<http://www.linux.org/>) that was designed to provide personal computer users a free or very low-cost operating system comparable to traditional and usually more expensive UNIX systems. Linux has a reputation as a very efficient and fast-performing system. Linux's kernel (the central part of the operating system) Linux is an operating system that was initially created as a hobby by a young student, Linus Torvalds, at the University of Helsinki in Finland. Linus had an interest in Minix, a small UNIX system, and decided to develop a system that exceeded the Minix standards. He began his work in 1991 when he released version 0.02 and worked steadily until 1994 when version 1.0 of the Linux Kernel was released. To complete the operating system, Torvalds and other team members made use of system components developed by members of the Free Software Foundation for the GNU project. Linux is a remarkably complete operating system, including a graphical user interface, an X Window System, TCP/IP, the Emacs editor, and other components usually found in a comprehensive UNIX system. Although copyrights are held by various creators of Linux's components, Linux is distributed using the Free Software Foundation's copyleft stipulations that mean any modified version that is redistributed must in turn be freely available. Linux is distributed commercially by a number of companies such as Red Hat. Unlike Windows and other proprietary systems, Linux is publicly open and extendible by contributors. Because it conforms to the Portable Operating System Interface standard user and programming interfaces, developers can write programs that can be ported to other operating systems. Linux

comes in versions for all the major microprocessor platforms including the Intel, PowerPC, Sparc, and Alpha platforms. It's also available on IBM's S/390.

LOS: Line of Sight.

MARS: Military Affiliate Radio System

MF: Abbreviation for Medium Frequency

MILNET: The original Advanced Research Projects Agency Network (ARPANET) was formed in by the U.S. Military. In 1984, the original network split into two networks: the ARPANET and the MILNET. The days of having just one or two networks are long gone. Today, the Internet is an international collection of thousands of networks interconnected with the TCP/IP protocols. Users of any one of these networks can use the network services provided by TCP/IP to reach any of the other networks. For example, in addition to the MILNET, in the United States there are the National Science Foundation Network (NSFNET), the Energy Science Network (ESnet), and the NASA Science Internet (NSI).

MEDIUM FREQUENCY: Per Federal Standard 1037C, Frequencies from 300kHz to 3000 kHz.

MILITARY AFFILIATE RADIO SYSTEM: MARS is a program conducted by the Army, Navy/Marine Corp and Air Force originally established on 26 November 1948 in which U.S. licensed Amateur Radio stations and operators participate and contribute to the mission of providing auxiliary communications on a local, national and international basis as an adjunct to normal military communications.

NETWORK INTERFACE CARD: The physical connection from the computer to the network is made by putting a Network Interface Card inside the computer and connecting it to the shared cable.

NWS: National Weather Service

NATIONAL WEATHER SERVICE:

OEM: Office Of Emergency Management

OFFICE OF EMERGENCY MANAGEMENT: The office or department in a city, town or county that coordinates disaster planning and resources.

OPEN REPATER: An open repeater is a system that does not limit access to specific Amateur Radio operators, rather the system owner/sponsors welcome the use of the system by all licensed Amateur Radio operators.

OPERATING SYSTEM: The main control program of a computer that schedules tasks, manages storage, and handles communication with peripherals. Its main part, called the kernel, is always present. The operating system presents a basic user interface when no applications are open, and all applications must communicate with the operating system.

PACKET LOSS: A measure of measurement packets sent to a destination that do not elicit corresponding return packets; those missing packets are lost packets. Specifically regarding

IRLP, packet loss is a loss of signal intelligence from the transmission which on the receiving end leaves a gap in stream what was transmitted.

PACKET RADIO: Packet radio provides for the exchange messages, bulletins, live chat using the keyboard and file exchange via Radio. In a number of areas there are large TCP/IP systems which can be used much more like the Internet.

PGP: Pretty Good Privacy

PL: Private Line

PRETTY GOOD PRIVACY: Pretty Good Privacy is a flavor of algorithmic encryption that uses two cipher keys, one public and one private. Anyone can use a public key to send a scrambled message to the receiving party. The private key is then used only by the receiving party to unscramble incoming messages. The two-key system was developed by RSA Data Security, Inc. and PGP is the most popular type of two-key encryption available for public, non-commercial use.

PRIVATE LINE: Motorola's trademarked name for CTCSS

PULSEBACK: A signal on the IRLP network caused by a digital packet(s) being sent from a node without a valid COS signal. Pulsebacks' are most often caused by hang time settings on a repeater. They can also be caused by the receiver sending a COS signal to the IRLP board after the radio has just unkeyed, thus a Pulseback occurred. The packet that is then sent out causes the connected node (or several connected nodes during a reflector connection) to also key and unkey.

RACES: Abbreviation for Radio Amateur Civil Emergency Service

RADIO AMATEUR CIVIL EMERGENCY SERVICE: Per the ARRL, RACES, administered by local, county and state emergency management agencies, and supported by the Federal Emergency Management Agency (FEMA) of the United States government, is a part of the Amateur Radio Service that provides radio communications for civil-preparedness purposes *only*, during periods of local, regional or national civil emergencies. These emergencies are not limited to war-related activities, but can include natural disasters such as fires, floods and earthquakes. As defined in the rules, RACES is a radio communication service, conducted by volunteer licensed amateurs, designed to provide emergency communications to local or state civil-preparedness agencies. It is important to note that RACES operation is authorized by emergency management officials only, and this operation is strictly limited to official civil-preparedness activity in the event of an emergency-communications situation. Per Civil Preparedness Guide Federal Emergency Management Agency Washington, D.C. 20472, CPG 1-15, a. RACES is an organization of amateur radio operators who volunteer to provide radio communications for State and local governments in times of emergency. Created in 1952 primarily to serve in civil defense emergencies, RACES provides essential communications and warning links to supplement State and local government assets during emergencies. b. RACES is a special part of the amateur operation sponsored by the Federal Emergency Management Agency (FEMA). RACES provides emergency communications for civil preparedness purposes only. RACES is conducted by amateurs using their primary station licenses or by existing RACES stations. In the event that the President invokes the War Emergency powers, amateurs officially enrolled in the local civil preparedness group would become limited to certain frequencies, while all other amateur operations would be silenced.

RADIO TELETYPE: A 5-unit, start-stop, International Telegraph Alphabet No. 2, code defined in International Telegraph and Telephone Consultative Committee Recommendation F.1, Division C commonly known as Baudot.

REMOTE SITE: A radio communications location which is part of the communications system that is geographically located from the main radio equipment site.

REPEATER: Per 47 C.F.R. § 97.3(a)(35): An amateur station that automatically retransmits the signals of other stations.

REPEATER STATION: A device or combination of devices, in Fixed locations for receiving radio signals from a Base, Mobile or Portable station and automatically transmitting corresponding radio signals which have been amplified, reshaped, or both for the purpose of extending communication range

RF LINK: A radio communications circuit using directional antenna and low power transmitters on specific linking sub bands used to connect to geographical isolated communications systems for either the one-way or two way communications between the sites in question.

ROUTER: A router is a device or, in some cases, software in a computer, that determines the next network point to which a packet should be forwarded toward its destination. The router is connected to at least two networks and decides which way to send each information packet based on its current understanding of the state of the networks it is connected to. A router is located at any gateway (where one network meets another), including each Internet point-of-presence. A router is often included as part of a network switch.

RTTY: Radio Teletype

SECURE SHELL: Secure Shell (SSH), sometimes known as Secure Socket Shell, was developed by SSH Communications Security Ltd. Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another with secure access. It is widely used by network administrators to control Web and other kinds of servers remotely. It provides strong authentication and secure communications over insecure channels. It is a replacement for rlogin, rsh, rcp, and rdist. SSH protects a network from attacks such as IP spoofing, IP source routing, and DNS spoofing. An attacker who has managed to take over a network can only force SSH to disconnect. He or she cannot play back the traffic or hijack the connection when encryption is enabled. When using SSH's slogin (instead of rlogin) the entire login session, including transmission of password, is encrypted; therefore it is almost impossible for an outsider to collect passwords. SSH is available for Linux, MS-Windows, Unix, Macintosh, and IBM OS/2. SSH commands are encrypted and secure in several ways. Both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted. SSH uses RSA public key cryptography for both connection and authentication. Encryption algorithms include Blowfish, DES, and IDEA with IDEA is the default.

SKYWARN: SKYWARN, in cooperation with NOAA's National Weather Service regional offices, provide a system of reporting weather conditions that may become a hazard to persons and property over a widespread area. Amateur Radio Skywatch, supported by radio enthusiasts, are trained in recognition of real-time severe weather conditions. They train in sufficient reporting procedures and provide reports from widespread locations.

SKYWAVE: Per Federal Standard 1037C, a radio wave that travels upward from the antenna.
Note: A sky wave may be reflected to Earth by the ionosphere.

SSH: Secure Shell

STATION: Per 47 C.F.R. § 2.1(c): One or more transmitters or receivers or a combination of transmitters and receivers, including the accessory equipment, necessary at one location for carrying on a radio communication service, or the radio astronomy service.

STATIC IP ADDRESS: A static IP Address is an IP address assigned by a service provider that never changes. This requires that the service provider keep at least one IP address per customer. Because their IP address remains fixed, static IP addresses can be used for hosting name servers.

T1 LINE: The T-carrier system, introduced by the Bell System in the U.S. in the 1960s, was the first successful system that supported digitized voice transmission. The original transmission rate (1.544 Mbps) in the T-1 line is in common use today in Internet service provider (ISP) connections to the Internet. Another level, the T-3 line, providing 44.736 Mbps, is also commonly used by Internet service providers. Another commonly installed service is a fractional T-1, which is the rental of some portion of the 24 channels in a T-1 line, with the other channels going unused.

TCP/IP: Transmission Control Protocol/Internet Protocol

TELNET: Telnet is the way you can access someone else's computer, assuming they have given you permission. (Such a computer is frequently called a host computer.) More technically, Telnet is a user command and an underlying TCP/IP protocol for accessing remote computers. On the Web, HTTP and FTP protocols allow you to request specific files from remote computers, but not to actually be logged on as a user of that computer. With Telnet, you log on as a regular user with whatever privileges you may have been granted to the specific application and data on that computer.

TRANSMISSION CONTROL PROTOCOL/INTERNET PROTOCOL: The basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an Intranet or an Extranet). When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from also has a copy of TCP/IP. TCP/IP is a two-layer program. The higher layer, Transmission Control Protocol, manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol, handles the address part of each packet so that it gets to the right destination. Each gateway computer on the network checks this address to see where to forward the message. Even though some packets from the same message are routed differently than others, they'll be reassembled at the destination. TCP/IP uses the client/server model of communication in which a computer user (a client) requests and is provided a service (such as sending a Web page) by another computer (a server) in the network. TCP/IP communication is primarily point-to-point, meaning each communication is from one point (or host computer) in the network to another point or host computer. TCP/IP and the higher-level applications that use it are collectively said to be "stateless" because each client request is considered a new request unrelated to any previous one (unlike ordinary phone conversations that require a dedicated connection for the call duration). Being stateless frees network paths so that everyone can use

them continuously. (Note that the TCP layer itself is not stateless as far as any one message is concerned. Its connection remains in place until all packets in a message have been received.)

TIME OUT TIMER: A timer that when exceeded will shut off the transmitter. Per FFC Part 97 requirements can be set to a maximum of 3 minutes for repeater stations.

USB: Universal Serial Bus

UHF: Abbreviation for Ultra High Frequency

ULTRA HIGH FREQUENCY: Per Federal Standard 1037C, frequencies from 300 MHz to 3000 MHz.

UNIVERSAL SERIAL BUS: USB (Universal Serial Bus) is a plug-and-play interface between a computer and add-on devices (such as audio players, joysticks, keyboards, telephones, scanners, and printers). With USB, a new device can be added to your computer without having to add an adapter card or even having to turn the computer off. The USB peripheral bus standard was developed by Compaq, IBM, DEC, Intel, Microsoft, NEC, and Northern Telecom and the technology is available without charge for all computer and device vendors. USB supports a data speed of 12 megabits per second. This speed will accommodate a wide range of devices, including MPEG video devices, data gloves, and digitizers. It is anticipated that USB will easily accommodate plug-in telephones that use ISDN and digital PBX. Since October, 1996, the Windows operating systems have been equipped with USB drivers or special software designed to work with specific I/O device types. USB is integrated into Windows 98 and later versions. Today, most new computers and peripheral devices are equipped with USB. Most cable modems now available offer either an Ethernet CAT-5 or USB port interface.

VHF: Abbreviation for Very High Frequency

VERY HIGH FREQUENCY: Per Federal Standard 1037C, frequencies from 30 MHz to 300 MHz

VOICE ID: A programmed synthesized male or female voice or a recording of a human voice which is used to identify the repeater station.

REFERENCES

1. 47 C.F.R. Part 97

Code of Federal Regulations, Title 47, Telecommunications, Federal Communications Commission, Part 97, Amateur Radio Service, Rules and Regulations.

2. FCC Part 97.1 Basis and Purpose

97.1. Basis and purpose. The rules and regulations in this part are designed to provide an amateur radio service having a fundamental purpose as expressed in the following principles:

- a) Recognition and enhancement of the value of the amateur service to the public as a voluntary noncommercial communication service, particularly with respect to providing emergency communications.
- b) Continuation and extension of the amateur's proven ability to contribute to the advancement of the radio art.
- c) Encouragement and improvement of the amateur service through rules which provide for advancing skills in both the communication and technical phases of the art.
- d) Expansion of the existing reservoir within the amateur radio service of trained operators, technicians, and electronics experts.

3. ARRL Amateur Radio Emergency Service (ARES) agreements with National Emergency Management Groups.

The Amateur Radio Service has in place agreements with National Emergency Management Groups that serve most communities within the United States:

Memorandum of Understanding Between the National Weather Service and the American Radio Relay League, Inc. (since 1986);

Statement of Understanding between the American Radio Relay League, Inc. and the American National Red Cross (since 1940, updated 1994);

Memorandum of Understanding Between the Federal Emergency Management Agency and the American Radio Relay League, Inc. (since 1984);

Memorandum of Understanding Between the American Radio Relay League, Inc. and the National Communications System (since 1983);

Memorandum of Understanding Between the Associated Public Safety Communications Officers, Inc. and the American Radio Relay League, Inc. (since 1984).

4. FCC Part 97.205 Repeater Station

1. Any amateur station licensed to a holder of a Technician, General, Advanced or Amateur Extra Class operator license may be a repeater. A holder of a Technician, General, Advanced or Amateur Extra Class operator license may be the control operator of a repeater, subject to the privileges of the class of operator license held.

- a) A repeater may receive and retransmit only on the 10 m and shorter wavelength frequency bands except the 28.0-29.5 MHz, 50.0-51.0 MHz, 144.0-144.5 MHz, 145.5-146.0 MHz, 222.00-222.15 MHz, 431.0-433.0 MHz and 435.0-438.0 MHz segments.
- b) Where the transmissions of a repeater cause harmful interference to another repeater, the two station licensees are equally and fully responsible for resolving the interference unless the operation of one station is recommended by a frequency coordinator and the operation of the other station is not. In that case, the licensee of the non-coordinated repeater has primary responsibility to resolve the interference.
- c) A repeater may be automatically controlled.
- d) Ancillary functions of a repeater that are available to users on the input channel are not considered remotely controlled functions of the station. Limiting the use of a repeater to only certain user stations is permissible.
- e) [Reserved]

The control operator of a repeater that retransmits inadvertently communications that violate the rules in this Part is not accountable for the violative communications.

5. IRLP statistical analysis as of 10 May 2002.

Number of nodes: 438

Number of countries on IRLP: 15

Country with largest number of nodes: U.S.

List of continents with IRLP nodes: 7

Africa
Antarctica
Asia
Australia
Europe
North America
South America

List of countries on IRLP: 15

Country	Number of Nodes
Antarctica	1
Australia	29 + 1 Reflector
Barbados	1
Canada	130 + 5 Reflector
Dominica	2
Ecuador	1
England	14
Japan	1
Netherlands	1
New Zealand	3
Scotland	2
South Africa	2
Sweden	1
Trinidad and Tobago	3
United States of America	230 + 4 Reflector

Number of U.S. states on IRLP: 36

State with largest number of nodes:

California

List of U.S. states on IRLP:

State	Number of Nodes

Alabama	3
Alaska	5
Arizona	10
California	56
Colorado	5 + 1 Reflector
Connecticut	1
District of Columbia	1
Florida	13
Georgia	7
Hawaii	8
Idaho	5
Illinois	10
Indiana	6
Iowa	1
Kentucky	1
Massachusetts	3
Maryland	1
Michigan	4
Missouri	4
Montana	2
Nebraska	1
New Hampshire	3
New Jersey	7
Nevada	6 + 1 Reflector
New York	15
North Carolina	5 + 1 Reflector
Ohio	5
Oklahoma	1
Oregon	4
Pennsylvania	10 + 1 Reflector
South Carolina	4
Tennessee	4
Texas	5
Utah	5
Washington	6
Wisconsin	3

Number of reflectors on IRLP: 10

Number of countries with reflectors: 3

List of continents with reflectors: 2

Australia
North America

List of countries with reflectors:

Country	Number of reflectors
Australia	1
Canada	5

United States of America	3
--------------------------	---

Number of U.S. states with reflectors: 3

List of states with reflectors:

Colorado
North Carolina
Pennsylvania

6. Automatic Voice Relay System (AVRS) Draft by Bob Bruniga, WD4APR

Draft paper (<http://web.usna.navy.mil/~bruninga/avrs/AVRS.doc>) to integrate APRS into IRLP. AVRS is a "Voice" addition to APRS. Just like APRS now provides mobile-to-mobile worldwide Text Message capability via the Internet APRServe system, integrating voice to this using an Internet connection of local repeaters via IRLP on-demand-access with the APRS text messaging capability would then allow switching back and forth from Text to Voice as needed. Text messages can confirm the other person is on the air, AVRS then lets them open a voice link to that same area.

7. A few Emergency Management organizations that already have experience using the Internet and IRLP.

- a. Emergency Amateurs Responding To Help (E.A.R.T.H.) <http://www.qsl.net/earth/> in Texas
- b. Finger Lakes Law Enforcement Amateur Radio Emergency Service (FLARES) in Rochester, N.Y. <http://www.flares.monroe.edu/>
- c. Chesterfield RACES Mobile Services in Chesterfield, Va. <http://www.ke4eue.org/>