

The Integration of Amateur Radio and 802.11

Amateur Radio and 802.11 wireless networking – a good fit for emergency message delivery.

Roderick D. Mitchell, KL1Y

Integrating two distinct and otherwise autonomous systems can provide rewarding results. There has been a lot of discussion about the use of commercial wireless protocols in the Amateur Radio community. These protocols, defined in the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standards, specify several wireless bands and modulation schemes for local and wide area networks. There are many possibilities with great potential for using available low-cost high-speed devices. Recently I had an opportunity to integrate Amateur Radio and 802.11. The goal was to choose a project that was viable, worth while and feasible in regards to time constraints. I chose the *Winlink 2000* Paalink network. Paalink is a component of the *Winlink 2000* messaging system. The Paalink network allowed me to integrate a wireless local area network (WLAN) using 802.11b/g, a Paalink e-mail server and an Amateur Radio system into a single network. Each of the integrated devices contains protocols and/or technologies that allow it to interconnect with other systems and devices in the network. Protocols are rules that define how communications devices communicate in a network.

PO Box 35053
Fort Wainwright, AK 99703
kl1y@arrl.net

The integration of various systems to form a single diverse system is critical today. Budget cuts that result in equipment and personnel shortages plague many organizations. The ability to integrate non-profit organizations and leverage their experience is critical. Amateur Radio Operators provide non-profit services to the community. Now Amateur Radio's ability to support government and non-governmental efforts during a disaster has expanded. This added capability is due to the integration of current automation and networking technologies with Amateur Radios. Several Amateur Radio Operators (Vic Poor, W5SMM, and Rick Muething, KN6KB) have worked very hard to develop the Paalink messaging software that allow Amateur Radio to integrate seamlessly with modern networking equipment and e-mail clients such as *Microsoft Outlook*, *Netscape* and *Outlook Express*.

Table 1
Application Level Protocol Port Assignments

Protocol	Port
http	80
SMTP	25
POP3	110
TCP	8000

The following sections describe the technical details of the system that integrates Amateur Radio and 802.11. This project supports the implementation goals of high speed multimedia (HSMM) through the use of 802.11. This integrated network easily integrates with the Amateur Radio Internet (Hinternet).

Integrated Technologies Explained

The core technologies that form the nucleus of this Hinternet project are radio frequency (RF), IEEE standards, communications protocols and communications applications and software.

Each of the core technologies has a place in the Open Systems Interconnection (OSI) model. OSI is a model for understanding and developing computer-to-computer communications.¹ The OSI model consists of seven layers: physical, data link, network, transport, session, presentation and application. See Table 1. The following section describes the integrated technologies of this project, their protocols and their place in the OSI model.

OSI Model View of Integrated Technologies

The physical layer of the OSI model converts the ones and zeros to electrical signals

¹Notes appear on page 32.

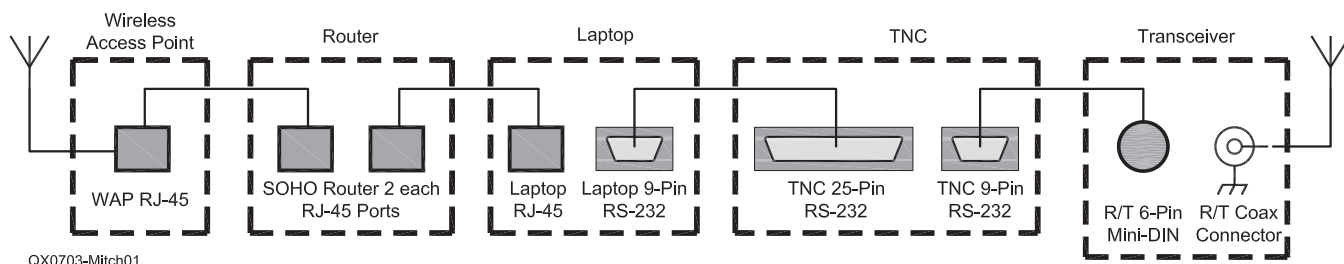


Figure 1 — Wiring diagram of integrated Amateur Radio and 802.11 network.

for transmission between devices.² The data link layer provides an error detection function. The network layer provides logical addressing and routing of information on the network. On the transport layer, error correcting techniques are employed.³ The session layer allows provisions for data exchange between applications as explained by Tuma and Fajfar. Tuma and Fajfar explained the presentation layer as the layer that ensures that applications can communicate with each other when the applications use different formats. The application layer is where application protocols reside in the OSI model.

The following sections describe functions of the specific protocols and technologies used in this project. The descriptions are based on the protocol or technologies function in the OSI model. Table 1 provides a quick view of the communications technologies used and their place in the OSI model. Figures 3 through 6 show the elements of the system.

Physical Layer

IEEE 802.11 at the Physical Layer

An 802.11b/g wireless access point (WAP) provides LAN connectivity to wireless clients equipped with 802.11b/g wireless network interface cards (NICs). A high gain omni-

directional antenna is used for transmission and reception of signals. 802.11 is a member of the IEEE 802 family, a series of specifications for local area network (LAN) technologies. Figure 1 is a wire diagram. The diagram shows the physical connectivity of the integrated circuit. Figure 2 depicts interconnections from a three dimensional perspective.

IEEE 802.3u at the Physical Layer

IEEE 802.3u is the standard also known as Fast Ethernet. This project uses an SMC small office/home office (SOHO) router. The router provides connectivity at the physical layer between the computer and WAP via IEEE 802.3u interfaces.

Amateur Radio at the Physical Layer

The backbone (wide area network connectivity) of the network is dependent upon Amateur Radio at the physical Layer. Amateur Radio is used to move the data from the local area network (LAN) to the Internet or other areas outside the LAN. Amateur Radio technologies and protocols used at this layer include: radio frequency (RF), frequency modulation (FM), TNCs and the AX.25 packet protocol.

AX.25 at the Physical Layer

The Amateur Radio packet protocol

AX.25 operates at the physical layer for connectivity between two terminals. AX.25 assumes that both ends of the link are of the same class.⁴ This class distinction is in regards to data terminal equipment (DTE) and the data communications equipment (DCE). With AX.25 there is no DTE and DCE. Connectivity between the computer and TNC is over serial cable using an RS-232 serial cable.

RS-232 at the Physical Layer

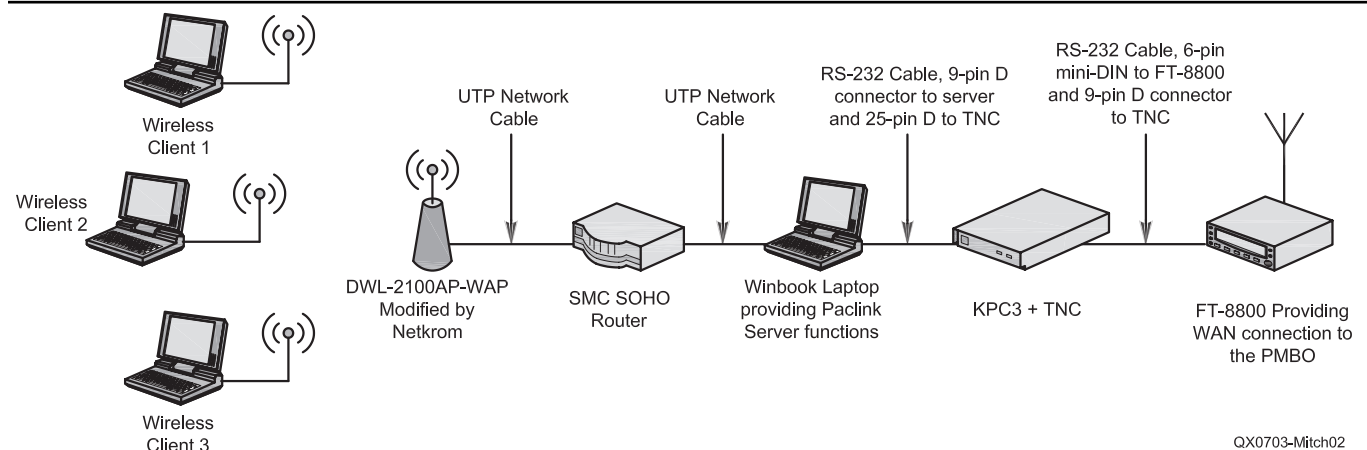
This network uses RS-232 connectivity between the computer and TNC and between the TNC and radio. RS-232 is a set of standards that specify three types of interfaces: electrical, functional and mechanical.⁵ The computer to TNC connection is a 9-pin D shape connector on the computer side and 25-pin D shape connector on the TNC side. The radio to TNC pin out for the 9-pin RS-232 connection and the 25-pin pin out are available at the Kantronics Web site: www.kantronics.com/documents/kpc3ppinout.pdf.

Coaxial Cable at the Physical Layer

Coaxial cable is used between the transceiver and the antenna. RG-8/U is used for this application. Some versions of RG-8/U have relatively low loss. We selected one that had a loss of approximately 1.8 dB per

Table 2
OSI Reference Model with Technologies Used in the Integrated Amateur Radio and 802.11 Networks

OSI Layer	Protocol or Technology
Application Layer (7)	SMTP, POP3, DHCP
Presentation Layer (6)	B2F
Session Layer (5)	TCP/IP (Sockets)
Transport Layer (4)	TCP, SMTP (Port 25), POP3 (Port 110), HTTP (Port 80)
Network Layer (3)	IP and Router
Data-Link Layer (2)	802.11, 802.3u, AX.25, KISS, Switch
Physical Layer (1)	AX.25, RF, RS-232, IEEE 802.3u, IEEE 802.11, Coaxial Cable (RG-8/U), UTP Cable



QX0703-Mitch02

Figure 2 — Interconnections of integrated network.

100 feet over 144 to 148 MHz. With our 50 feet, power loss is about 0.7 dB.⁶

UTP Cable at the Physical Layer

Unshielded twisted pair (UTP) cabling is used to interconnect the router, WAP and server. UTP is less expensive than its shielded (STP) counterpart. STP provides the best immunity to stray RF interference. The short lengths of UTP have proved reliable in this project. The UTP cable consists of four insulated pairs of wire. Wires 1, 2, 3 and 6 are used for transmission and reception of signals.

Data Link Layer

Network Switch at the Data Link Layer

Switches are connectivity devices that make efficient use of bandwidth. Switches allow devices to establish a direct connection to another port on the switch. This is in contrast to hubs that broadcast data to all ports. The switch in this network implementation provides connectivity for the WAP and server. Other LAN computers or, a printer, may be attached to the switch as the need arises. The switch interprets media access control (MAC) address information to determine where to forward packets it receives.⁷ The MAC address is a special address that is burned on the NIC during the manufacturing process. Each MAC address is unique. The switch, dynamic host control protocol (DHCP) server and router are all integrated in the SMC router housing.

IEEE 802.11 at the Data Link Layer

The definition of 802.11 functions at the MAC sublayer of layer 2 of the OSI model stated that "802.11 allows for mobile network access; in accomplishing this goal a number of additional features were incorporated into the MAC."⁸ As a result the 802.11 MAC may seem baroquely complex compared to other 802 MAC specifications".

IEEE 802.11 is not a far departure from other 802 standards. 802.11 adopted Ethernet-

style networking to radio links. In a similar way that Ethernet operates, 802.11 uses a carrier sense multiple access (CSMA) scheme to control access to the transmission medium.

IEEE 802.11 uses carrier sense multiple access collision avoidance (CSMA/CA) rather than the carrier sense multiple access collision detection (CSMA/CD) scheme used by 802.3 (Ethernet). CSMA/CA attempts to avoid col-

lisions. CSMA/CD detects collisions, stops transmitting and then retransmits the data.

IEEE 802.2 at the Data Link Layer

IEEE 802.11 uses the IEEE 802.2 encapsulation. The logical link control (LLC) sublayer protocol allows the 802.3 and 802.11 protocols to carry multiple, logical sub-network traffic of each protocol over the

LARRY LEDLOW JR, N1TX

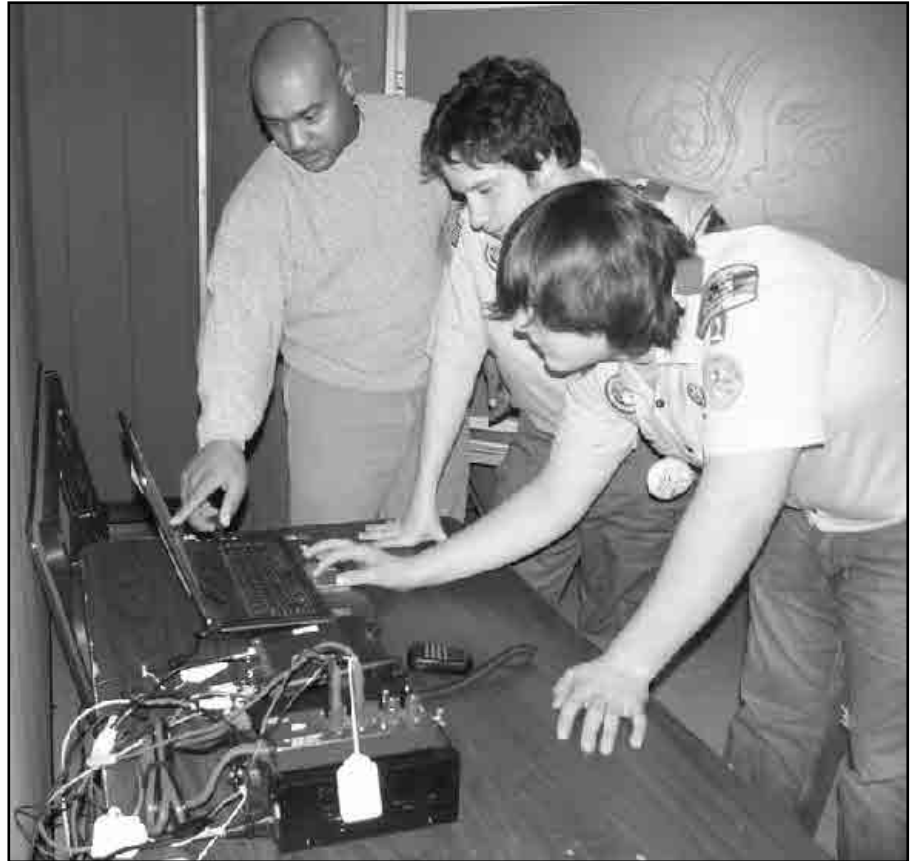


Fig 3 — Rod, KL1Y, explaining the possibilities that exist when using 802.11 with Amateur Radio. The two Boy Scouts are Michael Walsh (closest to Rod) and Jackson Drew.



Figure 4 — Denise Mitchell, KL10P (Rod's wife), sits at the operating position and monitors activities on the Paclink server.



Figure 5 — Breannah Jayde Mitchell (Rod's daughter) prepares a message for transmission from a wireless enabled computer on the integrated network.

same physical medium such as the LAN.⁹

The LLC sublayer provides an interface with the network layer protocols. The LLC sublayer is responsible for the ordered delivery of frames, including retransmission of missing or corrupt packets and for flow control (moderating flow so that one system does not overwhelm the other).¹⁰

IEEE 802.3u at the Data Link Layer

IEEE 802.3u (Ethernet) is used to provide connectivity between the Paclink server and WAP via the SOHO router. IEEE 802.3u specifies a standard capable of sending data at 100 Mbps (Newton, 2005, p 31).¹¹ At layer 2 Ethernet uses the CSMA/CD media access control.

The specific layer 2 functions of Ethernet include encapsulation and de-encapsulation of user data, media access management, collision detection and handling data encoding and decoding and finally, channel access to the LAN medium.¹²

Amateur Radio at the Data Link Layer

Amateur Radio protocols at layer 2 are AX.25 and Keep it Simple Stupid (KISS). The AX.25 protocol functions at both the physical and data link layers. KISS functions only at the data link layer. At layer 2, AX.25 encapsulates the e-mail messages for transmission over the air through radio frequencies. AX.25 ensures that compatibility exists between two Amateur Radio stations at layer 2.

The data rate between the TNC and radio is only 1200 bps. This provides a throughput of 1200 bps across the backbone link. The robustness and stability of this protocol are sufficient enough to make up for the low throughput. These qualities are suitable for text messages and small (30 kB) attachments.

KISS (Keep It Simple Stupid) is the layer 2 protocol used for connectivity between the Paclink server and the TNC. This connectivity is over an RS-232 serial port. The KISS protocol on the TNC gives the Paclink server complete control over and access to the contents of the HDLC (high level data link control) frames transmitted and received over the air.¹³

The TNC simply converts between synchronous HDLC, spoken on the half-duplex radio channel, and a special asynchronous, full duplex frame format spoken on the Paclink server/TNC link. Every frame received on the HDLC link is passed intact to the host once it has been translated to the asynchronous format; likewise, asynchronous frames from the host are transmitted on the radio channel once they have been converted to HDLC format.¹⁴

The KISS protocol uses p-persistence. P-persistence causes the TNC to wait for an exponentially distributed random interval after sensing that the channel has gone clear before attempting to transmit. With proper tuning of the parameters p and SLOTTIME, several

stations with traffic to send are much less likely to collide with each other when they all see the channel go clear. One transmits first and the others see it in time to prevent a collision. This is similar to the CSMA/CA technology used by 802.11.¹⁵

Network Layer

Network Router at the Network Layer

The network layer of this integrative project employs the use of a router. The router is the gateway to the LAN and allows remote clients to access the e-mail server. The router forwards the packets throughout the LAN/WLAN based on their logical addresses.¹⁶

The network router used in this implementation is an SMC small office/home office (SOHO) router. This router uses logical addresses (IP addresses) to direct data between networks or segments.¹⁷ The router used in this project has a WAN port that is connected to another network (separate broadcast domain). Nodes in the same broadcast domain can communicate with one another without passing data through a router.

Internet Protocol (IP) at the Network Layer

IP version 4 (IPv4) at the network layer of the OSI model is used for this project. The Paclink server and the wireless clients communicate by IP. The Paclink server is assigned a static IP address and the wireless clients may be addressed by dynamic or static configuration. The Paclink server is the e-mail gateway and provides access to the AX.25 channels. The WAP communicates with the Paclink server via the IP. Each wireless client, the WAP and Paclink use a

32 bit IP address. The addresses are within the same broadcast domain (network). The WAP has a management IP address that is in a separate broadcast domain.¹⁸

The Paclink server is the gateway device that provides connectivity between the IP network and the AX.25 network. The network layer IP datagram is passed through the gateway to the data link layer AX.25 protocol that resides on the Paclink server (gateway) for encapsulation and transmission through the Amateur Radio portion of the network. This process works in reverse as the frames come in through Amateur Radio and reach the TNC, then the gateway (Paclink Server) for transmission to the wireless clients.

Transmission Control Protocol (TCP) at the Transport Layer

TCP is the transport layer end to end protocol. TCP provides reliable, sequenced, and unduplicated delivery of bytes to users on the wireless LAN (WLAN) and LAN.¹⁹

TCP is a connection-oriented protocol. TCP first establishes a connection between the two systems that intend to exchange data. TCP formats segments for the network layer by breaking the segments into packets that are the appropriate size for the network.²⁰ TCP assigns each packet a sequence number. The packets are reassembled at the distant station in accordance with their sequence numbers. TCP uses a checksum to verify the accuracy of the message. If the checksum is accurate the recipient sends an acknowledgment (ACK). If the checksums do not match, the recipient asks the sender to resend the message.²¹



Figure 6 — The components of the integrated network are pictured left to right: Astron power supply, MFJ power strip, Yaesu FT-8800 transceiver with KPC3+ TNC sitting on top, Winbook laptop with Paclink AGW, Paclink Post Office and AGW Packet Engine software installed. To the right of the server is the SMC router and behind the router is the DWL-2100AP modified by NETKROM.

TCP uses ports to establish communications between the various application layer protocols used in this network. Ports are a logical point of connection in the context of TCP. TCP uses port values in the range of 0 to 65,535. The application level protocols and ports used in this network are shown in Table 1.

HTTP (application level protocol) port 80 is used for management of the WAP and router. SMTP port 25 and POP3 port 110 are used by the e-mail clients for messaging. On the client computer, additional ports are used at random to establish a connection on the server with the ports listed above. This was revealed during an analysis using an Ethereal protocol analyzer. Port 8000 is used to connect *Paclink AGW* to the *AGW Packet Engine*.

TCP/IP Sockets at the Session Layer

TCP/IP sockets are used at the Session layer of the OSI model. At this layer the logical links are bound and unbound between application layer protocols (users of service). The session layer maintains and controls the dialogue between the users of the service.²²

In TCP/IP the socket number is the joining of the senders' (or receivers') IP address and port numbers for the service being used (Example: 192.168.25.38:80). The combined IP address and port number identifies the unique connection in the network.²³

B2 Forwarding (B2F) Protocol at the Presentation Layer

B2F is used at the presentation layer for preparing messages for transmission over the single channel Amateur Radio.

B2F describes an alternate "automatic only" addressing and protocol scheme for delivering messages within the Winlink 2000 system. Poor, W5SMM, et al explained that "messages consist of three parts: header; body and attachments."²⁴ All parts of the message are combined into a single file that is compressed by *B2Compress.exe*, the B2F protocol compression program, as a unit before transmission.

Application Layer

SMTP at the Application Layer

The simple mail transfer protocol (SMTP) is used with the Paclink server. SMTP facilitates the outgoing message transfer function for e-mail clients. If an e-mail program such as *Outlook Express* is used on the Paclink server, the outgoing mail field is set to LOCALHOST. The WLAN and LAN client e-mail programs' outgoing mail field is set to the IP address of the Paclink server.

Post Office Protocol 3 (POP3) at the Application Layer

The POP3 service is provided by the Paclink server. The server facilitates the in-

coming message transfer function for e-mail clients. If an e-mail program is installed on the Paclink server this e-mail program's incoming mail field is set to LOCALHOST. The WLAN clients' e-mail program's (*Outlook, Netscape, etc...*) incoming mail field is set to the IP address of the Paclink server.

DHCP at the Application Layer

DHCP (Dynamic Host Configuration Protocol) is an application layer protocol (Dean, 2006).²⁵ DHCP is used in this network to provide automatic IP addressing for computers that connect to the integrated network through the WAP or directly to the switch. One of the many functions of the SMC small office/home office (SOHO) router is the DHCP server function. The Paclink server is not setup for DHCP. DHCP addresses could change automatically as leases expire therefore it is better to setup the Paclink server with a static IP address. Clients require seamless connectivity to the Paclink server. Changing the IP address on an inconsistent basis would disrupt the seamless connectivity. Dynamically assigning addresses to clients is a good idea because it lightens the administrative duties of the network administrator.

Software Packages Explained

The software packages used in this project provide connectivity and driver functions to facilitate the transfer, compression of data and transmission of data over the radio waves. The software used by the integrated Amateur Radio and 802.11 project include *AGW Packet Engine, Paclink AGW, Paclink Post Office* and the e-mail program, *Outlook Express*.

AGW Packet Engine

AGW Packet Engine is the TNC driver that resides on the Paclink server. The packet engine interfaces the TNC and *Paclink AGW* software. *AGW Packet Engine* is setup in KISS mode to communicate with the TNC. The packet engine controls the radio data rate and issues all commands required to facilitate communications between Paclink, the TNC, and radio. *AGW Packet Engine* creates channels with communications ports for *Paclink AGW*. These pre-defined channels allow Paclink to send data over the radio via the TNC.

Paclink AGW

Paclink AGW communicates with *Paclink Post Office* and *AGW Packet Engine*. *Paclink AGW* formats the messages for delivery by compressing the message with the B2F protocol. *Paclink AGW* has an open dialog box that allows the network administrator or radio operator to monitor the connection, compression and message dialog between the Paclink server and the PMBO. In addition to other functions provided by *Paclink AGW*, AX.25 functions and

features are provided by this software.

Paclink Post Office

The integrated Amateur Radio and 802.11 network uses *Paclink Post Office* as a component of the Paclink server. *Paclink Post Office* is the program required to provide connectivity between *Paclink AGW* and the user's e-mail program. *Paclink Post Office* provides the POP3/SMTP mail server functions.

In this installation *Paclink Post Office* uses the Amateur Radio call sign KL1Y for the Paclink site. *Paclink Post Office* may be configured for use on the local machine and LAN. The SMTP port number used is 25 and the POP3 port number is 110. *Paclink Post Office* listens on these ports for connection requests from e-mail programs.²⁶ When each e-mail program requests to connect to the POP3 server for the purpose of sending and receiving e-mail, the Paclink POP3 server validates the username and password.

The use of tactical addresses and the ability to use a common e-mail application are two key aspects of this network that allow the Amateur Radio community to seamlessly integrate with supported agencies and provide quick and reliable support. Tactical addresses are non-Amateur Radio call signs. An example of a tactical address is: **fbksemcomm-1@winlink.org**.

E-mail Program

This project uses Microsoft *Outlook* and Microsoft *Outlook Express*. It is possible to install and use any e-mail program capable of POP3 configuration. Messages sent to targeted recipients are viewed by any e-mail program capable of viewing text messages.

The Support Team

John Champa, K8OCL, HSMM Chairman, was instrumental in providing advice and mentorship in developing this document. Many local Amateur Radio operators supported the development of this local implementation. The operators readily provided logistics support and technical expertise. Linda Mullen, AD4BL, obtained a grant to purchase the amateur gear used in the project, Kody Moore, KLØRN, hand made the interface cables that connected the radios to the TNC,

Larry Ledlow Jr, N1TX, provided guidance as my mentor during the entire project. Larry devoted countless hours to reading drafts and the discussion of technical details.

Jerry Curry, KL7EDK, was instrumental as the Participating Mailbox Office (PMBO) Operator and packet expert. Dan Wietchy, KL1JP, was helpful in providing feedback and advice for the original paper.

Conclusion

This integrated network provides connectivity to the Amateur Radio network

through 802.11. The use of 802.11 in this scenario allows connectivity without wires. This extension of the radio network provides a convenient messaging system that can be quickly deployed.

In backbone architectures the VHF Amateur Radio network has proven much more reliable than 802.11 networks despite the low throughput of the Amateur Radio network. The use of 802.11 is not out of the question for the WAN links. An 802.11 WAN network is highly dependent upon line of sight connectivity with minimal obstruction.

Notes

- ¹T. Dean, *Network+ Guide to Networks*, 4th Edition, Boston: Course Technology, 2006.
- ²See Note 1.
- ³T. Tuma and I. Fajfar, "Hands on approach to teaching the basic OSI reference model." *International Journal of Electrical Engineering Education*, 37(2), 157, 2000.
- ⁴W. Beech, D. Nielsen and J. Taylor, *AX.25 Link Access Protocol for Amateur Packet Radio*, Revised Edition, Tucson Amateur Packet Radio Corporation, 1998.
- ⁵H. Newton, *Newton's Telecom Dictionary*, 21st Edition. San Francisco: CMP, 2005.
- ⁶West Penn Wire. *RG-8/U Coaxial Cable Flexible Design*, 2005. www.westpenncdt.com/pdfs/RF_Transmission_50-OHM_cables/808F.pdf.
- ⁷See Note 1.
- ⁸M. Gast, *802.11 Wireless Networks*, 2nd Edition, Sebastopol, CA, O'Reilly Media, Inc, p 14.

- ⁹D. Spohn, *Data Network Design*, 2nd Edition, New York, McGraw-Hill, 1997, p 255.
- ¹⁰M. Myers. *Managing and Troubleshooting Networks*. Boston: McGraw-Hill, p 50.
- ¹¹See Note 5, p 31.
- ¹²See Note 8, p 260.
- ¹³M. Chepponis, K3MC, and P. Karn, KA9Q, *KISS Protocol*, www.ax25.net/kiss.htm.
- ¹⁴See Note 13.
- ¹⁵See Note 13.
- ¹⁶See Note 1.
- ¹⁷See Note 1.
- ¹⁸See Note 5, p 444.
- ¹⁹See Note 5, p 828.
- ²⁰See Note 5, p 829.
- ²¹See Note 5, p 829.
- ²²See Note 5, p 755.
- ²³See Note 5, p 778.
- ²⁴V. Poor, W5SMM, H. Kessler, N8PGR, G. Muehling, KN6KB, S. Waterman, K4CJX, winlink.org/B2F.htm.
- ²⁵See Note 1.
- ²⁶G. Muehling, KN6KB, and V. Poor, W5SMM, "Paclink AGW a Modern AX.25 WL2K Packet Client Compatible with POP3/SMTP Clients," 2005.

Additional References

- The ARRL Handbook for Radio Communication*, 2007 Edition. Available from your ARRL dealer or the ARRL Bookstore, ARRL order no. 9760. Telephone 860-594-0355, or toll-free in the US 888-277-5289; www.arrrl.org/shop/; pubsales@arrrl.org.
- R. Bass, J. Potter, K. McGinnid, and T. Miyahira, "Surveying Emerging Trends in Emergency-related Information Delivery for the EMS Profession," *Topics in Emergency Medicine*, 26(2), 93-102.

- S. Bender, *Producing the Capstone Project*, Dubuque, IA: Kendall/Hunt.
- H. Berghel, "Wireless Infidelity I: War Driving," *Communications of the ACM*, 47(9), 21-26.
- F. Block and M. Pursley, "A Protocol for Adaptive Transmission in Direct-Sequence Spread-Spectrum Packet Radio Networks," *IEEE Transactions on Communications*, 52(8), 1388-1396.
- M. David, "ARRL's Role in Rescue Offers Lessons for Future," *Electronic Design*, 19.
- Kantronics KPC-3+ Port Pinout Information*, www.kantronics.com/documents/kpc3ppinout.pdf.
- T. Lammler and A. Barkl, *Cisco Certified Design Associate second edition*. San Francisco: Sybex.
- L. Luna, "Getting Back Backhaul Costs," *Telephony*, 246(24), 10-12.
- D. Rickie, "A Three-dimensional Framework for Information Technology Solutions," *IBM Systems Journal*, 39(2), 336.
- C. E. Strangio, *The RS-232 Standard*, www.camiresearch.com/Data_Com_Basics/RS232_standard.html.
- B. Waldo, "Information Technology: Strategies for Success," *Nursing Economic*, 16(1), 33-43.
- K. Schwalbe, *Introduction to Project Management*, Course Technology, Boston.

Rod Mitchell, KLIY, became a licensed Amateur Radio operator in September 2000. He is also a member of the Army MARS program and is licensed as ALM7AQ. He holds a Master of Science in Information Technology from Capella University. He also holds an FCC General Radiotelephone Operator License, is a Cisco Certified Network Associate, Cisco Wireless LAN Support Specialist, Foundry Networks Certified Network Engineer, CompTIA A+ and CompTIA Network+ certifications.

He currently is serving his 21st year in the US Army and holds the rank of Chief Warrant Officer Four (CW4). His present assignment is Officer-In-Charge of the Local Network Operations and Security Center at Fort Wainwright, Alaska. He has recently accepted an appointment as Director, US Army MARS — Alaska.

Rod's previous positions include Communications and Electronics Integration Officer for the 172nd Stryker Brigade, US Army Alaska, Avionics Maintenance Officer-In-Charge, Communications and Electronics Maintenance Officer with 82nd Signal Battalion, 82nd Airborne Division, 514th Signal Company, 35th Signal Brigade and 520th Maintenance Company, South Korea. Rod served as a Special Electronics Devices Technician and Instructor with the US Army. Rod's first opportunity to operate radios was while assigned as a radio telephone operator (RTO) with the 4th Infantry Division. Rod is an adjunct faculty member with the University of Alaska Fairbanks, Tanana Valley Campus, Information Technology Department.



WANTED: C++ PROGRAMMER

We need a part time C++ programmer who likes to work at home but lives in the Orange County/Los Angeles area. We need to automate our test procedures, which involve RF transmitters and receivers to determine if production products pass or fail. Tests include determining RF output, current consumption, PLL lock range, frequency accuracy, and receiver sensitivity by checking each section with a fully or semi-automated test program.

We need the following:

- Someone with experience writing Visual C++ programs allowing the PC to control the test equipment with RS-232 and or GPIB.
- You need to be familiar with RF test equipment such as spectrum analyzers, oscilloscopes, signal generators, and frequency counters.
- Be familiar with troubleshooting of RF and digital circuits.
- Be able to control relays, switches, etc. through PC I/Os with Visual C++.
- Have TCP/IP programming experience with Visual C++.
- Have CGI programming experience in any language.
- Robotic experience a plus.
- We would like to see examples and or samples of your past work.



COMMUNICATIONS SPECIALISTS, INC.
 426 WEST TAFT AVENUE • ORANGE, CA 92865-4296
 714.938.3021 • FAX 714.974.3420
 US & CANADA 800.854.0547 • FAX 800.850.0547
www.com-spec.com E-mail: spence@com-spec.com

Network/Data Layer Messaging Protocol for Stand-Alone, Free-Field Communications Systems

The author proposes protocols and data formats for a self-organizing network of stations to pass messages.

Lindsay J. Robertson, ZL2LJR

Abstract

Protocols and data formats are proposed that will allow a completely self-organizing network of peer stations using free-field, physical-layer communications to pass message packets from an originating station to a designated destination station at arbitrary distance, needing no other equipment or systems. The proposed system is presented in enough detail to allow implementation, but most importantly, the paper establishes some general principles that can be extended and developed as required.

Briefly, a datagram header format that contains geographical location and a local identifier of the destination station is proposed: peer stations build up internal lists of ID's and locations of other peer stations that they can "hear" — and hence each station that progresses a datagram is able to automatically select an optimum station to which the transient datagram may be passed. Simple protocols are proposed for authenticating and verifying datagram transfer, for rerouting datagrams to ensure a high probability of delivery, and for purging of datagrams that are successfully passed towards their final destinations. An "open" approach that encourages user control and further optimization is proposed. This is different from present Mobile Ad-hoc Network (MANET) protocols, and it also differs in several aspects from current geographic routing proposals and current radio packet transfer systems.

Need for Robust, Free-Field Network Layer System

Life without instant, reliable communication is just about inconceivable — we simply assume reliable communication via the Internet, cellular and "landline" phone services.

Yet a review of existing systems shows that only the long-range point-to-point HF radio system is both independent of a "wired backbone" and capable of long-range messaging. Although workable, the point-to-point HF radio system has limited reliability. (It depends upon ionospheric conditions between two stations, and is a highly inefficient use of bandwidth.)

Reliance upon wired communication backbones represents a significant vulnerability. To appreciate the issue, one only has to consider how useless a cell-phone handset is, without the cell-phone nodes and inter-node routing systems. A news item "The Backhoe: A Real Cyberthreat" describes this issue eloquently.¹

The existing systems therefore do not adequately address any of the following situations:

- Cases where a large number of users (each with limited power) want to exchange messages over long distances, without excessive use of bandwidth.
- Cases where the only open bands are not available to a particular station (stations of limited power, or only VHF.
- A user (particularly a VHF/UHF user) who lives in a geographically remote location, such as at the end of a long valley.
- The aftermath of a natural disaster, (or delib-

erate sabotage) when a user is affected by disruption of either "last mile" or backbone transmission lines, or the loss of third party communication facilities. See Note 1.

- The aftermath of software errors (or attacks) upon a system that relies on a hardwired backbone.^{2,3}
- A user who lives in a region in which backbone communication facilities are operated by authorities whose oversight is unwelcome.

Situations of these types, and the lack of adequate solutions, represent the "need" that is addressed in this paper.

Existing Systems

Classification of Existing Systems

Before considering any proposed "new" system, it is essential to review systems already in existence. Classifications of network systems have been published before, however these have generally been limited to relatively narrow fields. For the purposes of this paper, a very broad approach is taken, and the following categories are proposed:

"Wired" Systems. For these systems, all nodes are hard-wired, and for each route segment, a router selects the next destination node and switches the packet to that node.⁴ (See the referenced text, starting on page 405.) Examples include the Internet, and landline telephones. These offer efficient, high-speed communication, but are totally dependent upon the "wired" connection, and vulnerable to either physical disruption of wired "backbone" (see Note 1), and electronic disruptions (see Notes 2 and 3).

Wireless Neighborhood Networks. These