reprinted from Proceedings of HF '95: Nordic Shortwave Radio Conference, Fårö, Sweden *(invited paper)*

HF Radio in the International Information Infrastructure

Eric E. Johnson

New Mexico State University
Las Cruces, NM, USA 88003-8001
ejohnson@nmsu.edu

Abstract

In building the international information infrastructure, communication planners have emphasized terrestrial high-bandwidth service to urban users. Satellite links are assumed for customers who are either mobile or too distant from the high-capacity backbones for terrestrial service. However, automated HF radio provides a viable low-cost alternative for many of these users. This paper presents an overview of how HF radio systems can be usefully integrated into the rapidly expanding global Internet.

1. INTRODUCTION

Advancements in the international information infrastructure daily bring concepts from science fiction into the everyday fabric of society. Only a few years ago, the rapid, asynchronous communication provided by electronic mail became a compelling argument for buying a computer for the home. Today, home computer users contemplate personal "agents" that will nightly scour information sources to produce a customized electronic "newspaper" in time for breakfast.

Underlying this explosion in new capabilities is a dense web of networks including the global telephone network and the Internet (the latter relying largely upon the services of the former). However, some communities of potential users of these information resources are not well served by the existing networks. Many of these users could make good use of HF radio technology for "on ramps" to or "bridges" in the "information superhighway."

Due to the relatively low bandwidth available from HF data channels, however, most scenarios for routing Internet traffic through HF subnetworks involve special circumstances:

a) *Voice or data to remote locations*. HF is currently in use to provide relatively low-cost voice service to locations too remote for economical landline or line-of-sight radio service. With the addition of modern HF automation, such remote sites can be linked together into HF subnetworks, with multiple gateways into the information infrastructure to improve the robustness of connectivity to these sites.

b) *Voice or data to mobile platforms*. For communications to mobile platforms beyond line of sight, HF provides an economical alternative to satellite communications. Automatic Link Establishment (ALE) has been shown to largely alleviate the link-level connectivity problems that formerly plagued HF. Automated HF Node Controllers (HFNCs) will integrate individual voice and data terminals, as well as the networks aboard larger platforms, into the high-bandwidth, low-cost stationary infrastructure. For example, shipboard LANs may be linked within a task force using UHF, VHF, and HF radio (as appropriate for each link), with long-haul trunks carried by an optimized mix of satellite and HF radio.

c) *Emergency connection to severed networks.* Natural or man-made disasters can sever segments of our backbone networks. A backup network of automated HF radio stations can quickly detect and bridge such faults to carry high-precedence traffic into and out of emergency areas. Bandwidth limitations will require priority and preemption mechanisms to optimize use of the HF links.

d) *Connection to rapid deployment networks*. From disaster areas to combat theaters, the transportability, low cost, and long range of HF radio make it a primary quick-response medium. With an automated capability to link HF subnetworks into the Internet, deployed teams can use familiar communication tools such as electronic mail to ease the transition to operations in the field.

2. JOINING THE INTERNET

2.1 Compatibility

If HF radio is to be used to transparently extend the information infrastructure to these new user communities, we need to ensure that HF technology is compatible with the assumptions implicit in the Internet architecture. Beginning with the characteristics of HF systems, one of the key aspects of the HF medium that distinguishes it from more popular Internet media is that propagation is highly variable over a wide range of time scales:

- multipath effects on the scale of milliseconds
- fading on the scale of seconds to minutes
- diurnal variation on the scale of hours
- ionospheric disturbances and sunspot activity on the scale of days to years

The unique characteristics of HF technology are largely the results of addressing this challenging environment, including unique modems, interleavers, and coding for shorter-term variations, and adaptive frequency and antenna selection for the longer-term variations. The ability of automated HF node controllers to rapidly adapt to changing conditions is steadily improving the reliability of HF links (see next section). However, the data rates that can be reliably achieved over long-haul HF skywave channels are substantially lower than those expected over Internet backbones (or even dial-up modem links); this will impose some limits on the functions that can be efficiently performed over HF Internet links, as discussed below.

The architecture of the Internet emphasizes issues at a higher level[1] than those that make HF radio unique. The essence of the Internet is technology which links disparate subnetworks into a seamless network of networks. The key component of this technology is the Internet Protocol (IP) which provides “datagram” service to higher-layer end-to-end protocols. Because datagrams sent via a subnet are not guaranteed to emerge from that network in order, or without duplication (or even to emerge at all), the upper-layer protocols bear the burden of providing a user’s expected quality of service. Thus, the existing Internet protocol architecture is already prepared to cope with the vagaries of HF propagation.

2.2 Performance Limitations

Given that HF networks and the Internet are compatible on this most fundamental level of interoperability, we must examine issues of performance and congestion that arise in HF

1. Higher “layer” in terms of the ISO Open Systems Interconnection Reference Model [4].

subnetworks due to the restricted bandwidth of HF links. Although HF modems with data rates of 9600 bps are currently in development, achievable throughput over HF links is currently closer to 1200 bps, an order of magnitude less than the rates achievable over wire-line modems. For example, a pair of 14.4 kbps (v.32bis) modems operating within a metropolitan area and using v.42bis data compression may be expected to achieve a user data throughput on the order of 8 kbps for text transfer. HF data modems, operating over a mid-latitude skywave path (Boulder, CO to San Diego, CA, USA) were able to achieve about 1 kbps user data throughput [1].

The data rates required by Internet users vary over several orders of magnitude, depending on the application. Electronic mail typically requires only a few thousand bytes per day, while a World-Wide Web browser on a multimedia workstation can easily sustain data rates of a million bytes per second. Clearly, users of multimedia applications will be disappointed with the throughput of an HF connection to the Internet, while other users may be satisfied. The key to expanding the class of potential satisfied users of HF Internet links is improving the throughput of user data.

Three possible avenues for increasing the usable data bandwidth of HF links are as follows:

- Increase the allocation of HF spectrum per link.
- Improve the data efficiency of the modem (in bits/Hz).
- Increase the information content (reduce redundancy) in the modem bit stream.

The first is beyond the scope of this paper; the second is properly the domain of my esteemed colleague, Stephen Cook [2], which leaves for this paper an evaluation of compressing Internet traffic to improve the response time to users within the constraint of relatively low actual link data rates.

The lower data rates of HF links compared to wireline modems, local-area networks (LANs) and so on, allow more time per channel data bit for compression. Although this increased time will not result in commensurate increases in compression, it does allow for somewhat better compression than the high-speed technique commonly used in wireline modems. The figures below illustrate the improvement in compression achievable when increasing computational effort is applied. All are variants of the Lempel-Ziv algorithm. Timings were collected on an IBM RS/6000 model 580 workstation running AIX 3.2.5.

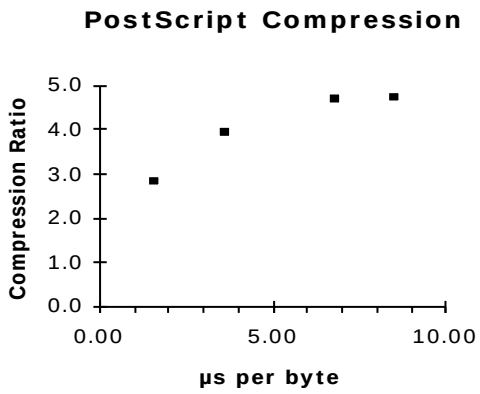

Figure 1: Compression of PostScript

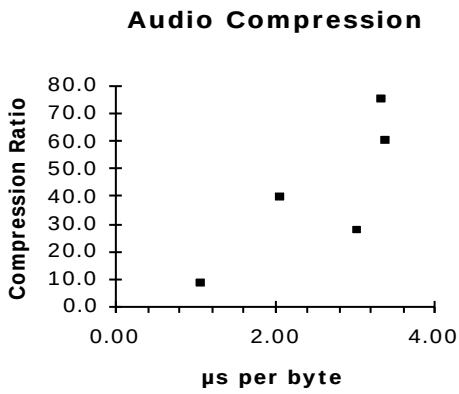

Figure 2: Compression of Audio (.WAV)

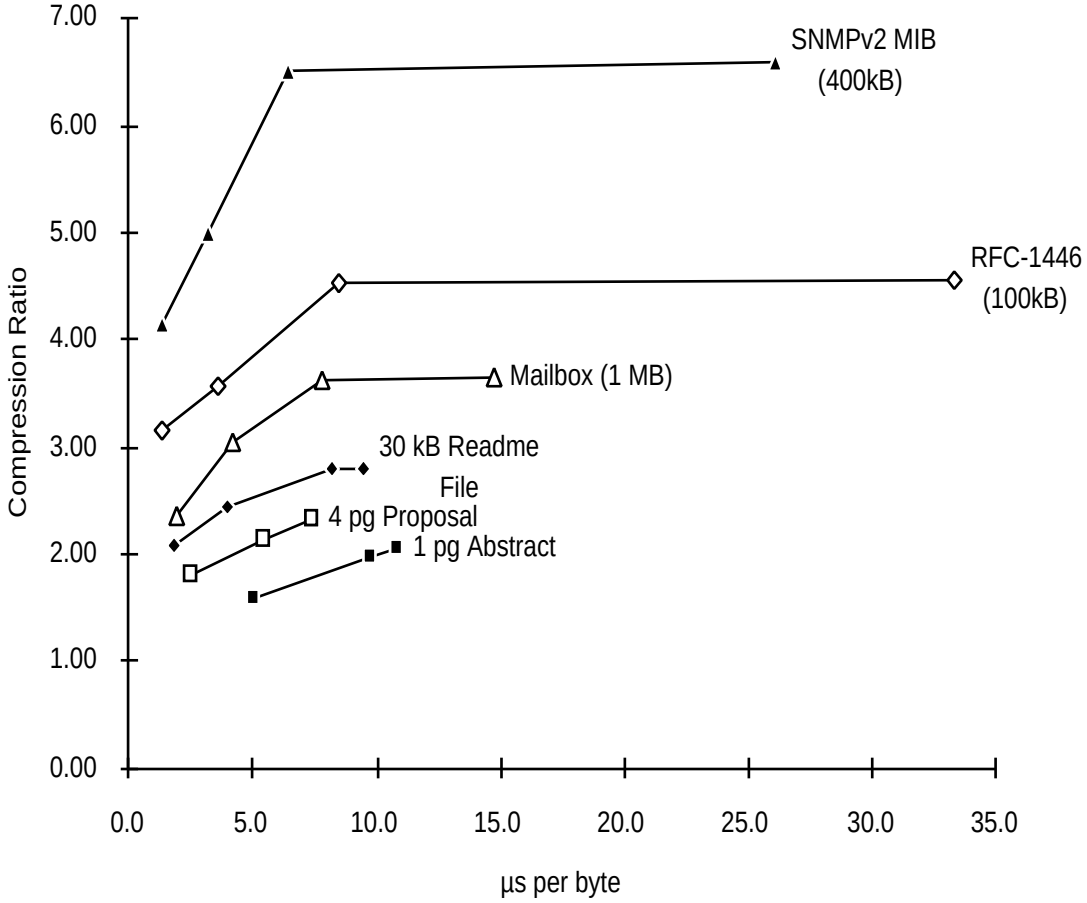

Figure 3: Compression of Text Files

The compression of text files (Figure 3) is much the same as for PostScript files (Figure 1). The lowest compression ratio in every case is achieved by the Lempel-Ziv-Welch (LZW) algorithm, which is widely used (e.g., in GIF files and the Unix `compress` command) due to its high compression speed. For HF applications, we can achieve 50% better compression by instead using a more aggressive implementation of the Lempel-Ziv algorithm such as that in the `gzip` utility (which produced the third point in each case in Figure 3).

Graphic images (GIF) and QuickTime movies (MOV) are stored in a compressed format by default, so no additional compression by networks is usually feasible. However, given the potential payoff for HF users, it may be worthwhile to remove the LZW compression and re-compress using more powerful techniques for improved image throughput on HF links.

From these compression results, it is apparent that Internet access via HF is most likely to prove satisfactory for applications that are text- or PostScript-based, because the additional compression achievable partially mitigates the lower data rates of HF versus wireline modems. Audio files can also be compressed remarkably well. However, applications that require the transfer of large photo or video files will probably not work well over HF links.

2.3 HF Interface to Internet

One inexpensive technique for connecting an HF subnetwork to the Internet is shown in Figure 4. Here, a desktop computer (labeled Gateway) executes off-the-shelf Internet Protocol software that routes packets among any connected data links. The figure shows both an Ethernet board and an HFNC present in this computer, so it serves as the gateway between all nodes reachable via the Ethernet (probably the entire Internet) and all nodes reachable from the local HF station.

Figure 4: HF Internet Gateway

Although communications with the Mobile station could be direct from the Gateway, a Relay station is shown as an intermediate node in the path to illustrate the capabilities of the new generation of automated HF technology, described in the next section.

3. NEW STANDARDS FOR HF AUTOMATION

The United States Department of Defense recently published MIL-STD-187-721C [3], a planning standard that identifies a suite of technologies to automate the operation and management of HF radio networks. (Similar work is underway in the development of a range of U.S. Federal Standards including FED-STD-1046, -1047, -1048, and -1052.)

3.1 HF Node Controllers

For the purposes of discussion, the network layer [2] functionality of an automated HF station is considered to reside in HF Node Controllers. Figure 5 shows the conceptual organization of the HF automation physical, data link, and network layer functionality, followed by a block diagram of the HFNC in Figure 6.

In Figure 6, "S&F" refers to the Store and Forward function, which is responsible for finding a route through the subnetwork, using relays and other media as necessary. "AME" refers to the Automatic Message Exchange function, which is responsible for conveying messages over each data link in the path through a subnetwork.

The Routing Table is a listing of previously computed Destination – Next Station pairs for use in routing incoming messages. For each message destination, the Routing Table contains the address of one or more recommended relay stations to use when direct transmission to that destination is not possible. The Path Quality Matrix is a dynamically-updated table of aggregate (single- or multi-link) voice and data path qualities to various destinations via the best known paths to those destinations.

Figure 5: HF Automation Overview

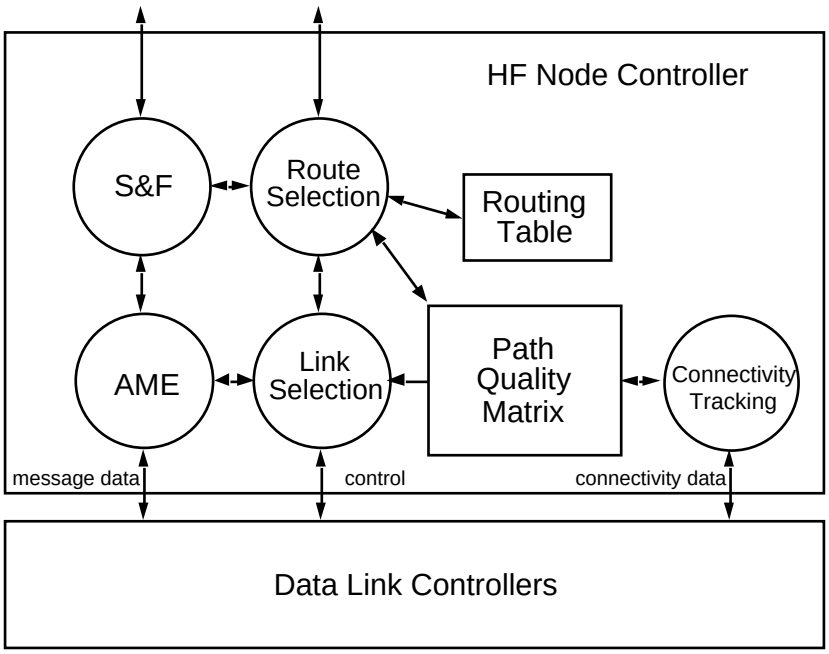

Figure 6: HF Node Controller Functions

MIL-STD-187-721C defines four standard levels of HFNC functional capability [5]:

- A Level 1 HFNC has no Routing Table, Path Quality Matrix, nor Store-and-Forward functionality. It can route messages only to directly-reachable stations. Thus, indirect routing must be generated by an external router, which will explicitly name the next relay station when passing a message to the HFNC for delivery.
- A Level 2 HFNC includes a Routing Table and Store-and-Forward ability, but no Path Quality Matrix. Indirect routing is performed automatically, but the Routing Table will usually be generated externally. In a typical application, a level 2 HFNC would receive its Routing Table from a central network control site, with updates provided either manually by local operators, over the air from the network control station, or from its own connectivity tracking function.

  Store-and-Forward functionality in Level 2 (and higher) HFNCs is supported by connectivity monitoring and routing queries. When connectivity is lost to a station listed in the Routing Table, messages destined for that station are queued until a connection is re-established. The HFNC can also actively seek new relay stations through the routing query protocol, and post the results to its Routing Table.
- A Level 3 HFNC adds the Path Quality Matrix and the Connectivity Exchange protocol to the Level 2 capabilities. Level 3 controllers discriminate among possible paths for messages using path quality formulas that consider link degradation due to congestion as well as natural phenomena. Routing decisions thus adapt more quickly in Level 3 HFNCs than in Level 2, because the latter respond only to link loss, while the former can detect a deteriorating link and switch before the link becomes unusable.
- A Level 4 HFNC adds an Internet router to the capabilities of a Level 3 HFNC, and can therefore act as a gateway between HF and other subnetworks.

HF subnetworks in Internet applications will typically employ Level 4 HFNC gateways at interface points between HF and other media, with Level 2 or 3 HFNCs at other stations in the network. Unlike the mesh topologies commonly found in wired wide-area networks (WANs), HF networks will often be hierarchies of star topologies. One possibility is shown in Figure 7, in which Level 4 stations serve as hubs of stars of less-capable stations, and are themselves linked into a "backbone" star.

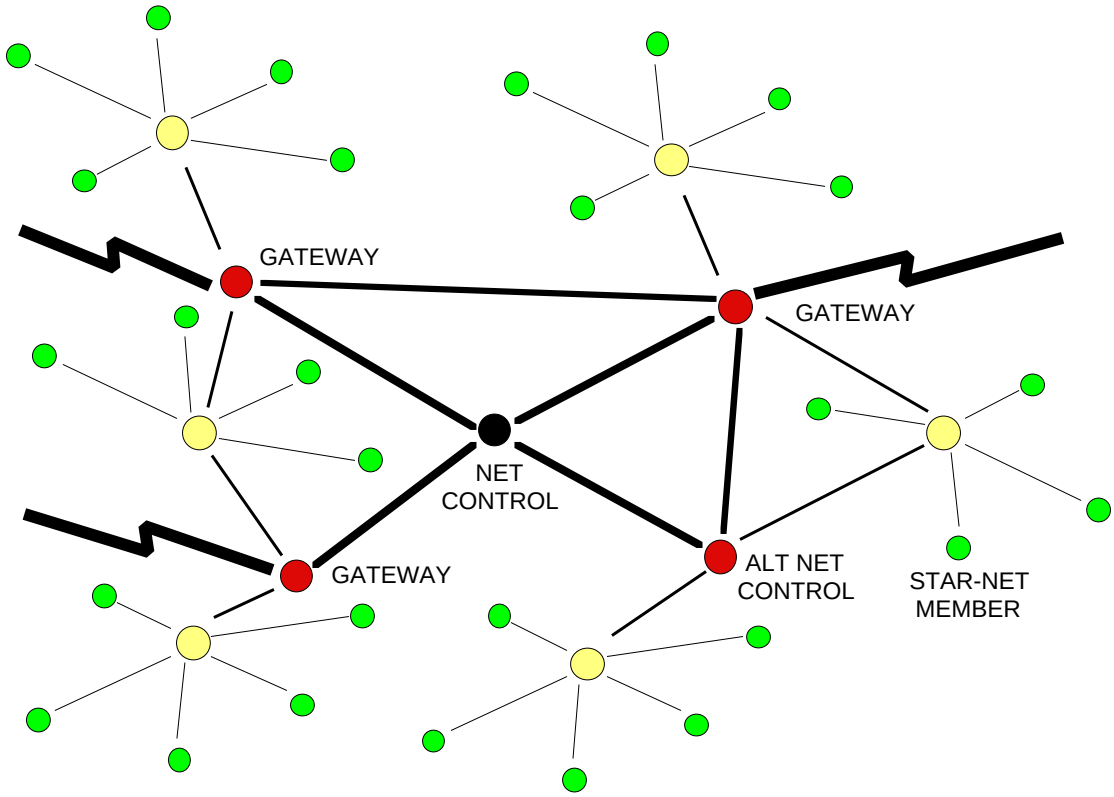

Figure 7: Example HF Subnetwork Topology

3.2 Network Layer Protocols

The suite of protocols at the network layer supports automatic message exchange, connectivity exchange, relay management, and station status monitoring.

Automatic Message Exchange. The Automatic Message Exchange (AME) protocol [6] provides a simple, connectionless, datagram service. A port number is included in the AME header to support internal routing of AME datagrams to higher-layer entities such as the Internet Protocol, the HF Network Management Protocol, or the operator display (for orderwire messages).

The AME header also includes a flexible mechanism for appending source routing to messages: in addition to the source and destination station addresses, additional stations can be named as recommended or mandatory relay stations for the message. This supports, for example, a network consisting only of Level 1 HFNCs, with source routing performed by operators or by host computers that maintain routing tables.

Connectivity Exchange. The Connectivity Exchange protocol [7] is used by Level 3 and 4 HFNCs to share path quality data. For example, if station A receives a report from B about

the path from B to C, A can combine its measurement of the link quality to B to compute the end-to-end quality of the path from A to C through B.

HF Relay Management Protocol. HRMP [8] is used to remotely control repeaters, and to query directly-reachable stations about connectivity to a locally unreachable station. Precedence and preemption are supported for optimum use of network resources.

HRMP also includes a connectivity monitoring mechanism that can be used to track indirect connectivity without the overhead of the full CONEX protocol (which can consume sizable fractions of HF channel bandwidth). For example, assume station A routes messages to C through B. Station A may request that B asynchronously report loss of connectivity to C so that A could then find (or activate) an alternate route to C.

HF Station Status Protocol. HSSP [9] may be used to support a notification based mechanism for tracking the status of network member stations with less overhead traffic than a polling-based approach. Status reports are sent when a station changes scan set, begins radio silence, goes out of service, assumes network management duties, returns to normal operation, and so on.

Although the level of network monitoring provided by these protocols may be sufficient within an HF subnetwork, management of interconnected subnetworks in the Internet usually requires the ability to examine detailed operating statistics at key stations, and to remotely manipulate their control states. This capability is extended to HF networks by the HF Network Management architecture, described in the following section.

3.3 HF Network Management

Use of HF radio to extend Internet services to the users identified in the Introduction will result in increasingly complex HF networks, with equipment often placed at remote sites. This, along with programs to consolidate high-power HF assets among military services into unmanned “lights out” facilities, indicates the need for a standardized protocol for remotely controlling HF stations and for remotely diagnosing problems in HF networks. Similar needs in the existing Internet have led to the development of the Simple Network Management Protocol (SNMP). However, the hostility of the HF medium presents clear challenges to the development of a mechanism for reliably monitoring and controlling distant radio stations.

MIL-STD-187-721C describes a protocol that addresses these challenges, while maintaining compatibility with the standard Internet SNMP network management architecture.

3.3.1 Background

Automation of High Frequency (HF) radio networks to date has simplified the tasks related to establishing links using HF radios. However, Automatic Link Establishment (ALE) and other HF automation technology [3] have brought a new problem to managing radio networks: the automatic controllers use a number of intricate data structures that must be kept consistent throughout a network if operations are to proceed smoothly.

Another aspect of network management that has not been addressed by the ALE standards is the need to observe network connectivity and equipment status from network control sites (Figure 8) so that corrective action can be initiated promptly when malfunctions or other disruptions occur.

Managers of packet networks have been at work on these problems for some time. The most mature and widespread of the existing network management architectures is the

Internet-standard Network Management Framework, which was developed in the late 1980's. This technology is more often referred to by the protocol that it employs for managing network nodes, the Simple Network Management Protocol, or SNMP [10].

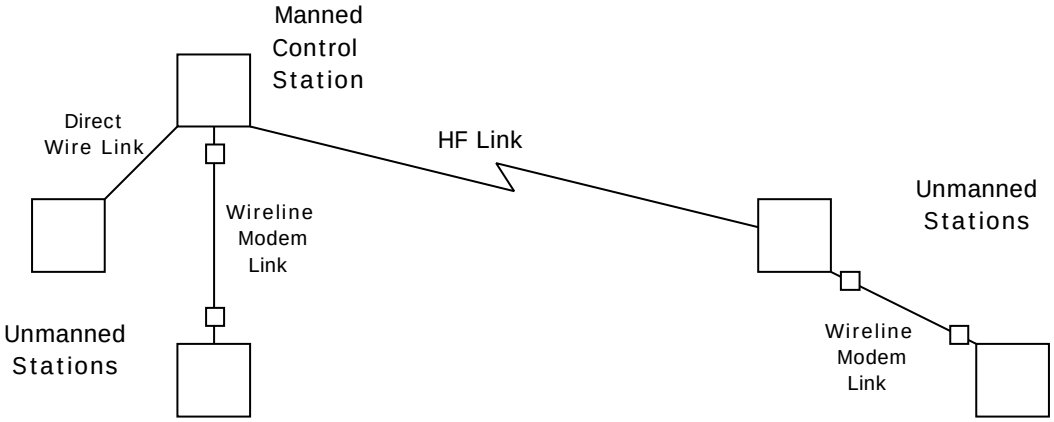

Figure 8: Network Management Example

SNMP was designed so that it "explicitly minimizes the number and complexity of management functions realized by the management agent itself" [10]. That is, the development costs of including SNMP in managed equipment are minimized, at the expense of (perhaps) increasing the complexity of the software that manages such nodes. Fortunately, the ratio of managed nodes to management stations is large, so the benefit of widespread implementation has greatly outweighed the cost of implementing the management software.

To briefly summarize the salient points of the SNMP approach:

- *Network management stations* monitor and control *network elements* by communicating with *agents* in those elements.
- This interaction uses SNMP [10] to *get* and *set* the values of defined data objects. Agents may also send *trap* messages to management stations to announce important events asynchronously.
- The defined data objects are described in the *Management Information Base* (MIB), which is currently strongly oriented to the TCP/IP protocol suite, but is easily extensible. Object definitions are expressed formally in *Abstract Syntax Notation 1* (ASN.1) [11].
- Object names and values are encoded for transmission in accordance with a set of ASN.1 *Basic Encoding Rules* [12].
- When elements do not implement SNMP, they may still be managed by using *proxy agents* that translate the standard SNMP messages into messages understood by these elements.
- Authentication is included in the standard, although current practice uses only trivial authentication. The mechanism is extensible using ideas similar to HF linking protection [13-17].
- SNMP requires only a connectionless datagram transport service (e.g., the User Datagram Protocol UDP [18] in the Internet).

3.3.2 HF Network Management Requirements

The assets to be managed in an automated HF network include media-specific equipment such as transceivers, modems, ALE controllers, and HF Node Controllers (HFNCs). Figure 9 depicts a network management station and a controlled HF network node. The management station as shown uses HF links to control this node, but it could just as well employ a wide area network (WAN), wireline modems, or other types of links.

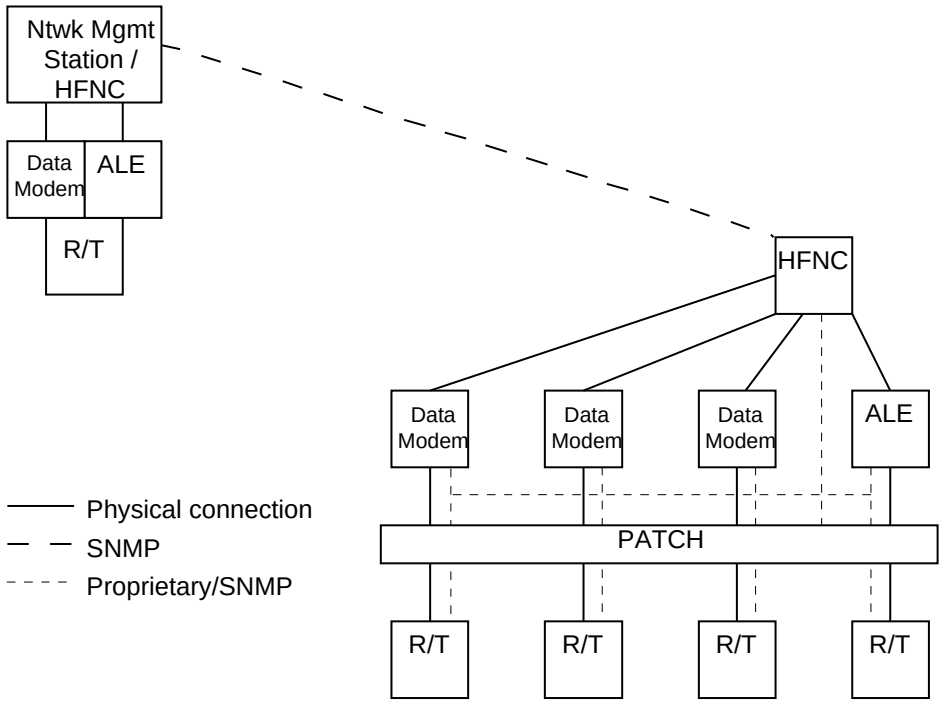

Figure 9: Management of HF Network Nodes

An automated network management system must support the efficient control of automated HF stations and networks, including the following functions:

- Monitoring and reporting network status (topology, capabilities, congestion, faults, etc.).
- Updating network routing tables.
- Manipulating the operating data of automated communications controllers.
- Identifying software versions, and updating the software, in ALE and other communications controllers.
- Re-keying linking protection scramblers.
- Remotely operating all communications equipment, including adjusting transmitter power of linked stations, reading “meters,” rotating antennas, and so on.

Because of the mission-critical nature of the networks to be controlled, authentication must be integral to the network management protocol.

3.3.3 Applicability of SNMP for HF Network Management

Several questions must be addressed in assessing SNMP for HF network management [13]: whether it can support all of the functions required (functionality), work over the HF medium (compatibility), and perform acceptably without imposing unacceptable overhead (performance). These issues are discussed below.

Functionality. Over-the-air data manipulation functions clearly depend upon the interrogation and revision of data at remote sites, which is precisely the model supported by SNMP. Over-the-air rekeying can also be cast as an authenticated transfer of new values to defined objects, in this case the storage locations of keys. Remote control is less clearly supported by the SNMP approach, but, as noted in the SNMP standard, all control actions may be implemented as "side effects" of writing to appropriate variables in an automated controller. For example, rotating an antenna occurs as a side-effect of updating a variable that specifies the azimuth of that antenna. Thus, all of the network management functions can be supported by SNMP.

Compatibility. Because SNMP was designed to help network managers find problems in networks under crisis conditions, it makes few assumptions about the reliability of the communications paths to the managed elements. It expects only unreliable connectionless service from the transport layer. This can be satisfied either by implementing UDP on top of IP, or through the use of no transport protocol at all, on top of the Store and Forward capability of the MIL-STD-187-721C network layer. Any available HF modem technology can be used to provide usable HF data links to the network layer.

Thus, SNMP will be isolated from direct interface to the HF medium, and has been designed specifically to work through the unreliable conditions that sometimes plague HF links.

Performance. Network management stations monitor and control network elements by communicating with agents in those elements. This communication is carried in SNMP messages, so both management stations and agents must execute the SNMP protocol. The protocol is deliberately lightweight; this is intended to keep the costs of implementing and executing SNMP sufficiently low that all elements in a network can be directly managed (i.e., that all equipment of interest will implement SNMP).

The result of minimizing the complexity of the software that implements SNMP is that most of the complexity of network management is transferred to the management station software. However, due to the relatively low rate of messages expected in managing typical HF radio networks, even an inexpensive notebook computer should posses adequate processing power to serve as a network management station.

A key requirement for any management protocol to be used over HF channels is that it minimize the number of bits communicated in performing its functions. The minimization of traffic was a goal of the SNMP developers, but the networks for which it was designed place far lower costs on each bit sent. Thus, while SNMP is generally regarded to be a lightweight protocol in the Ethernet environment (10 Mbps), it is not clear that it is sufficiently lightweight to be used over HF, where all overhead traffic is viewed much more suspiciously.

The basic message format for the current version of SNMP (version 2), includes privacy and authentication header fields, an SNMP command (e.g., a *get* to read an object, a *set* to update an object, or a *response* to return a value), a data field that holds a request ID, error status and index fields, and a list of variable bindings. Each variable binding contains an

object identifier and (in *set* requests and *get* responses) a value. It is these variable bindings that carry the management information.

In the variable bindings, each *object identifier* specifies the name of a managed object by describing where it is defined in a tree of standards. This formal system of naming objects typically consumes ten or more octets for each object. *Values* of objects can be encoded in as few as three octets (for integers less than 128); however, strings of N characters will require N+2 octets for their encodings.

No provision is made in SNMP for getting or setting entire tables. Each entry must be individually named in requests and responses.

If the headers for UDP and IP are included, an SNMP message that responds to a request for a three-character address from an ALE controller address table will require on the order of 70 octets, plus the HF Automatic Message Exchange header and data link layer header. Eliminating UDP and IP would remove 28 octets from this total. Reduction of this overhead is one of the key goals of the HF variant of SNMP.

3.3.4 HNMP: The HF variant of SNMP

Because the initial version of SNMP did not provide sufficient authentication capability for HF network management, MIL-STD-187-721C is based on version 2 of SNMP [19-30], usually denoted SNMPv2. This section describes this differences between SNMPv2 and the HF variant of SNMP (termed HNMP), and addresses questions of managing existing assets that do not implement SNMP, controlling access to managed assets, and integrating the management protocol with the existing HF protocol suite.

HNMP is identical with SNMPv2 [19-30], with the following variations:

a. Object identifiers for objects defined in the HF MIB are encoded for transmission using a truncated encoding scheme that reduces overhead.

b. A GetRows variant of the GetBulk message is introduced.

c. A PIN authentication scheme is mandatory, while the SNMPv2 MD5 authentication scheme is optional.

d. Retransmission timeouts in network management programs are adjusted to allow time for link establishment, and for the transmission of requests and responses over modems that may be able to achieve throughputs of 100 bps or less.

The relationship of the network management protocol to the other protocols in use within an HF station is shown in Figure 10. HNMP requires only a connectionless datagram transport service (e.g., the User Datagram Protocol (UDP)). Consequently, Figure 10 shows HNMP using UDP for a transport-layer protocol, IP for an Internet-layer protocol, and the HF Automatic Message Exchange (AME) protocol as the Network-layer protocol. Figure 10 also shows integration of IEEE 802 protocols as an illustration of the use of HNMP over an Ethernet local area network. Other LAN and WAN protocols may be integrated similarly. When interoperation with management stations outside the local HF sub-network is not required, UDP and IP may be eliminated to reduce the overhead of network management messages.

Figure 10: Interrelationship of Protocols

3.3.5 Objects Used in Network Management

SNMP functions by reading and writing data *objects* defined for each functional element (e.g., HF node controller, ALE controller, modem, or radio). These data structures are defined using an abstract syntax so that the details of how the data are stored by individual network components are hidden.

- RFC-1450 defines the objects commonly used to manage TCP/IP internets.
- The standard objects for HF network management are defined in the HF Management Information Base (HF MIB). This MIB module contains groups of objects for radios (and related RF equipment), ALE controllers, linking protection, HF data modems (and associated data link controllers), and networking controllers.
- Objects specific to each manufacturer's equipment are specified in a MIB provided by that manufacturer.

A management station integrates MIB modules from the elements it manages, resulting in access to a wide-ranging and dynamic set of management data. The structure of MIBs is defined in RFC-1442 [20].

When data is exchanged over the air (or some other medium), it is necessary that all parties to the exchange use the same encodings for the data. Object names and values sent in HNMP messages are encoded IAW the Basic Encoding Rules for ASN.1, found in [12], with a truncated encoding used for OBJECT IDENTIFIERS of objects from the HF MIB [31].

3.3.6 GetRows Mechanism

In addition to the SNMPv2 protocol data units (PDUs), HNMP includes GetRowsRequest and GetRows Response PDUs. The GetRows operation is similar to the SNMPv2 GetBulk operation, except that the response to a GetRows is a new compact PDU. A GetRows response includes the object ID only of the first object in each row, followed by the values of all objects requested in that row. This elimination of the largely redundant transmission of object IDs can dramatically reduce the number of bits sent when reading tables, which is an important consideration for managing ALE controllers and radios over the relatively low

bandwidth of HF channels. A similar idea could be employed for efficiently setting rows of tables, but is not part of the standard.

3.3.7 Access Control

Access to the management information of network elements is controlled in HNMP at two levels. The first level is an administrative model that restricts the objects at each element that are accessible to other parties and the operations that may be performed by those parties.

The second level of access control is authentication of messages; that is, determination that a message actually comes from the party named in the message. The following three mechanisms are available to authenticate HNMP messages:

- *Trivial Authentication.* Check the transport-layer address of the originator of the message.
- *Personal Identification Number Authentication.* Require operator entry of a PIN, which is appended to every message and checked by agents.
- *Cryptographic Authentication.* Attach a *digest* of each authenticated message at the beginning of the message (`authInfo` in the `SnmpAuthMsg`). This digest is computed from the message contents and a secret initialization vector in such a way that it is considered computationally infeasible to "spoof" the authentication system [32]. A time-of-day mechanism is included as well, to limit the effects of replay attacks.

An extra level of access control is imposed on HF access to managed stations when linking protection is used to authenticate ALE calls. In this case, anonymous distant HF stations can be denied the ability to even establish links to the managed network.

3.3.8 Proxy Management

When elements do not implement HNMP, they may still be managed by using proxy agents that translate the standard HNMP messages into messages understood by the non-HNMP ("foreign") elements. As HNMP management of HF radio networks is phased in, few network elements will initially implement HNMP. Proxy agents will be needed to extend the management capability to current-generation equipment. As a general rule, the proxy agent for any foreign network element should reside in the lowest-level controller that has a control path to that element, often an HFNC.

The provision for proxy agents in HNMP will greatly ease its use in HF networks. A phased approach to integrating HNMP into automated HF networks is to initially limit the penetration of HNMP to no level lower than HFNCs, with proxy agent software running within each HFNC to translate HNMP messages into the peculiar command sequences used by the other equipment at each site. This has the clear advantage of limiting the initial round of new software development to equipment that is software-based (HFNCs) rather than requiring upgrades to firmware-based equipment such as fielded ALE controllers.

3.3.9 Performance

The performance of HNMP may be gauged by how many bits are transferred to perform common operations. A fairly complex station such as that shown schematically in Figure 11 may be used for computing some example bit counts.

A similar station containing 1 ALE controller, 7 radios, 10 antennas, 6 HF Data Link Protocol (HFDLP) controllers, 1 antenna matrix, and 1 automated BLACK patch panel was

analyzed [33] with the following results: at 1200 bps, and assuming 50% overhead for ARQ, a complete download of the management information for this station would consume approximately 200 seconds. Of course, over a LAN, a WAN, or even a high-speed modem link, the time for this download would be on the order of one second, primarily determined by the overhead of the lower-level protocols rather than the HNMP overhead.

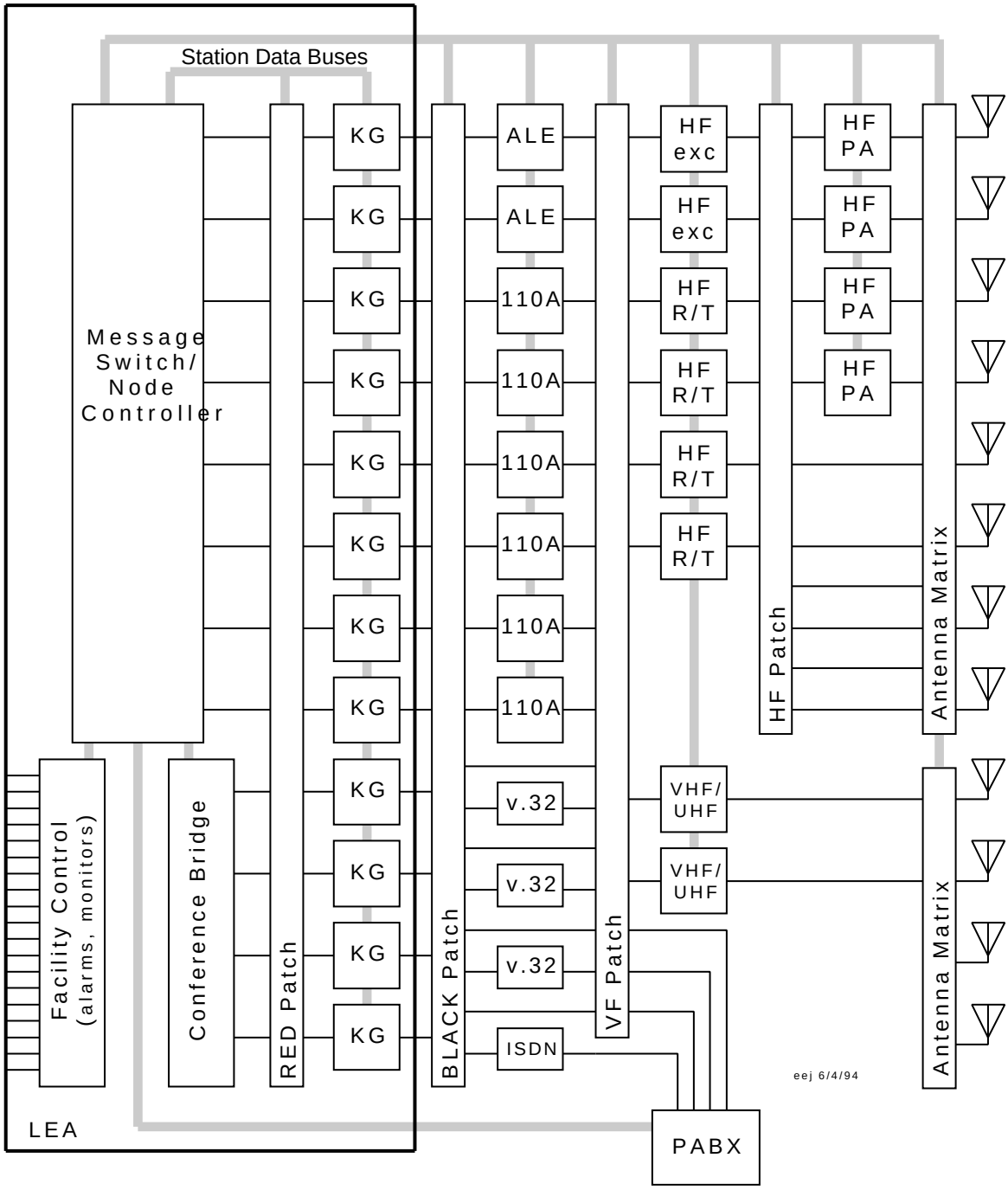

Figure 11: Large-Scale HF Internet Gateway

4. CONCLUSION

HF radio appears well-suited to provide connectivity to and within the Internet for applications that can tolerate the relatively low bandwidth currently available from HF

modems. These applications certainly include text-oriented applications, for which powerful compression algorithms mitigate the lower throughput of HF compared to wireline modems. Audio files can also be compressed substantially, but photo and video files will be more difficult to accommodate without incurring very long file transfer times and producing significant congestion of HF networks.

Due to the compatibility between the standards developed for HF automation and the Internet standards, the integration of HF into the international information infrastructure should be relatively painless. Much of the software required for the end-to-end protocols and internetwork routing is commercially available, with documented interfaces.

New development may be required only to implement the HF-specific protocols and algorithms for routing and station control. This software can be targeted to the inexpensive desktop and portable computers that currently run the higher-layer protocols and applications, and will benefit from the mature development environments available for these machines.

PC Cards are currently available that pack both an Ethernet interface and a fax/data modem into a credit card size form factor. The day may not be far distant when a PC Card implementation of the automated HF technology described here will connect a palmtop computer to a LAN and an HF transceiver to form a small, but complete HF Internet gateway.

5. REFERENCES

1. Minutes of HF Radio Federal Standard Development Working Group Meeting Eight at New Mexico State University, Las Cruces, NM, USA, 24-25 February 1994.
2. S. Cook, “Advances in High-Speed HF Modem Design,” Proceedings of HF-95.
3. MIL-STD-187-721C, “Interface and Performance Standard for Automated Control Applique for HF Radio,” 30 November 1994. Available on the Internet. URL is `ftp://tracebase.nmsu.edu/pub/hf/pubs/mil_std_187_721c.`
4. ISO 7498, *Information Processing Systems - Open Systems Interconnection - Basic Reference Model*, American National Standards Association, 1984.
5. MIL-STD-187-721C, section 4.6.2.7, “Standard levels of capability.”
6. MIL-STD-187-721C, section 5.7.5.4, “Automatic message exchange.”
7. MIL-STD-187-721C, section 5.7.4, “Connectivity exchange.”
8. MIL-STD-187-721C, section 5.7.6, “Relay management protocol.”
9. MIL-STD-187-721C, section 5.7.7, “Station status protocol.”
10. RFC-1157, “A Simple Network Management Protocol” (SNMP).
11. ISO/IEC 8824, *Information Processing Systems - Open Systems Interconnection - Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)*, International Organization for Standardization, 1990.
12. ISO/IEC 8825, *Information Processing Systems - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1)*, International Organization for Standardization, 1990.
13. E.E. Johnson, “SNMP for HF Radio Network Management,” NMSU, 1993.

14. E.E. Johnson, “High Frequency Radio Linking Protection Implementation Guide,” Technical Report NMSU-ECE-91-004, 1991. (see also NMSU-ECE-89-004 and PRC-EEJ-88-001.)

15. C. Redding and E. E. Johnson, "Linking Protection for Automated HF Radio Networks," *Proceedings of 1991 IEEE Military Communications Conference* (MILCOM ‘91), IEEE Press, New York, 1991.

16. E.E. Johnson, “Analysis of HF Radio Linking Protection,” *Proceedings of 1992 IEEE Military Communications Conference* (MILCOM ‘92), IEEE Press, New York, 1992.

17. E.E. Johnson, “Evaluation of HF Radio Linking Protection,” *Proceedings of 1993 IEEE Military Communications Conference* (MILCOM ‘93), IEEE Press, New York, 1993.

18. RFC-768, “User Datagram Protocol” (RFCs may be obtained by anonymous ftp from nis.nsf.net or nic.ddn.mil.)

19. RFC-1441, “Introduction to Version 2 of the Internet-standard Network Management Framework”

20. RFC-1442, “Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)”

21. RFC-1443, “Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)”

22. RFC-1444, “Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2)”

23. RFC-1445, “Administrative Model for Version 2 of the Simple Network Management Protocol (SNMPv2)”

24. RFC-1446, “Security Protocols for Version 2 of the Simple Network Management Protocol (SNMPv2)”

25. RFC-1447, “Party MIB for Version 2 of the Simple Network Management Protocol (SNMPv2)”

26. RFC-1448, “Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)”

27. RFC-1449, “Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)”

28. RFC-1450, “Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)”

29. RFC-1451, “Manager-to-Manager Management Information Base”

30. RFC-1452, “Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework”

31. E.E. Johnson, “Management Information Base for HF Radio Networks,” USAISEC Technical Report ASQB 94089, November 1994 (appended to MIL-STD-187-721C).

32. RFC-1321, “The MD5 Message-Digest Algorithm”

33. E.E. Johnson, “HNMP: Remote Control and Management Protocol for HF Radio Networks,” to appear in *Proceedings of 1995 IEEE Military Communications Conference* (MILCOM ‘95), IEEE Press, New York, 1995.