

POTENTIAL IP SOLUTIONS FOR NETWORKING SELECTED FAA WEATHER SYSTEMS

Ezra Jalleta, Minqi Liu, Mark Simons, The MITRE Corporation, McLean, Virginia

Abstract

This paper presents an analysis of the network connectivity between the Automated Surface Observing System (ASOS) and the Automated Weather Observing System (AWOS) Data Acquisition System (ADAS). The study was conducted to determine the feasibility of transporting legacy network protocols over Internet Protocol (IP) routed networks. Suggested areas for possible technology upgrades to facilitate this transition are highlighted.

1. Introduction

Knowledge of current and forecasted weather conditions is an important aspect of air traffic management. While pilots are responsible for avoiding severe weather, controllers must be knowledgeable of severe weather to effectively reroute traffic in a safe and efficient manner when requested by pilots, or on a time-available basis when duties permit. Over the past decade, the FAA has developed many systems to better serve pilots and controllers with specialized weather products.

The design and architecture of weather systems depends heavily on the use of point-to-point circuits for communication between weather sensors and their associated distribution and processing systems located in air traffic facilities. New service options offered by the FAA Telecommunications Infrastructure (FTI) program may allow the agency to transition wide area network (WAN) transport for these weather systems to the more cost-effective technology of routed networks and the Internet Protocol (IP).

Today, ASOS stations connect to weather data processing systems using the High-level Data Link Control (HDLC) protocol. In order to make use of IP technology for WAN transport, the FAA must upgrade weather systems like ASOS to natively use IP or devise transitional mechanisms that can

accommodate the legacy communication protocols and the network interfaces.

Two mechanisms are considered in the transitioning of AWOS, ASOS, and ADAS to an IP routed infrastructure. One such mechanism is the Serial Tunneling (STUN) technique, which has the capability of being able to encapsulate legacy protocol information in packets with IP headers and deliver them to the destination where de-encapsulation takes place. The other mechanism uses techniques of protocol conversion where legacy protocol headers are modified during the conversion process and made compatible with IP technology.

This paper presents an examination of the ADAS and its associated systems, the AWOS and the ASOS. The goal is to identify what technologies could facilitate a transition of these systems to native IP network connectivity. It also describes evaluations of transition approaches, including a description of laboratory test sessions held at the FAA's William J. Hughes Technical Center (WJHTC).

2. Aviation Surface Automation

The AWOS and the ASOS are part of the Aviation Surface Weather Observation Network (ASWON) which comprises most types of surface sensing systems. Both ASOS and AWOS are similar in design and technology, and they produce similar types of alpha-numeric observation data. The Automated Weather Sensing System (AWSS) is the next generation AWOS/ASOS and is in the initial phase of deployment.

The FAA currently has 571 ASOS systems supporting the NAS. The NWS has 313 ASOS, roughly 100 of which currently support the NAS, with an additional 170 expected to be connected to NAS systems in the near future. The FAA has about 170 AWOS systems operational in the NAS

and a total of about 30 AWSS systems, some of which are now becoming operational [1].

The ASOS, AWOS and, soon the AWSS, are connected to the ADAS using the Data Multiplexing Network (DMN). The ADAS hosts are located at the Air Route Traffic Control Centers (ARTCCs) and some sites are consolidated onto DMN multi-point circuits to help minimize telecommunication costs.

The AWOS Data Acquisition System (ADAS)

The ADAS is hosted on hardware located at each ARTCC. The ADAS collects data from AWOS and ASOS stations using the HDLC protocol. There is enough capacity on an ADAS to connect up to 137 AWOS/ASOS; typically an ADAS supports about 38 stations. Codex 3600 modems provide the digital-to-analog conversion for ASOS data.

Each ADAS also maintains interfaces to Weather Message Switching Center Replacement (WMSCR) to provide hourly AWOS/ASOS data, and interfaces to the local ARTCC Weather and Radar Processor (WARP) and up to 6 Integrated Terminal Weather System (ITWS) Product Generator (PG) sites, to provide minute-by-minute observations. ADAS uses the National Airspace Data Interchange Network (NADIN) II Packet Switched Network (PSN) to exchange data with WMSCR, WARP, and ITWS. ADAS manages connections using the Transport Protocol 4 (TP4) specified by the International Organization for Standardization (ISO).

The ADAS also interfaces with the National Lightning Detection Network (NLDN)¹ using commercial satellite service. NLDN messages are sent to the AWOS/ASOS for inclusion in the surface observation report. The Automated Lightning Detection and Reporting System (ALDARS) software hosted on the ADAS helps manage this interface. A high-level diagram of ADAS connectivity is provided in Figure 1.

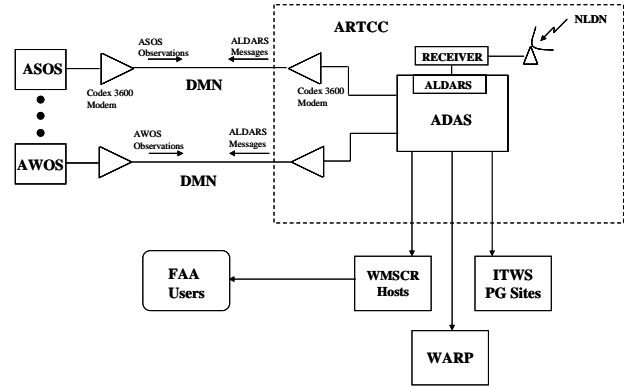


Figure 1. High-Level connectivity for ADAS[1]

Automated weather sensing systems such as ASOS are connected to an ADAS located at ARTCCs. ADAS hosts are located at ARTCCs rather than at more centralized locations to reduce the distance to ASOS sensors. This arrangement reduces the cost associated with the point-to-point circuits required to transport ASOS data[2]. ADAS uses the NADIN II network available at ARTCCs to transport the data to WMSCR, a gateway system with hosts located in Salt Lake City, Utah and Atlanta, Georgia.

Also, some ASOS are connected using multi-point circuits to share transport infrastructure. A diagram of the multi-point and point-to-point circuits is shown in Figure 2.

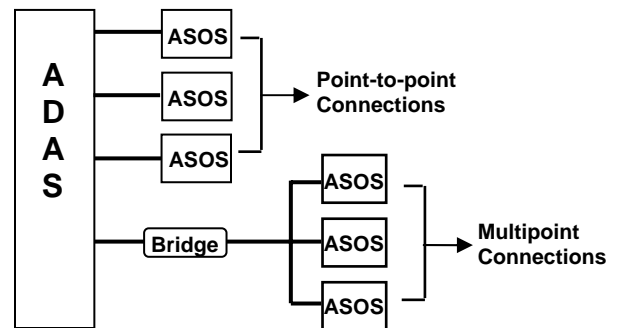


Figure 2. ADAS Multi-Point and Point-to-Point Configurations

ASOS-to ADAS Interface

A version of the High-Level Data Link Control (HDLC) protocol called the Normal Response

¹ The NLDN is a commercial service offered by the Vaisala Group. More information may be found at <http://www.lightningstorm.com/tux/jsp/discover/nldn/index.jsp>.

Mode (NRM) is used to transfer data between systems. Using the HDLC-NRM protocol, the ADAS acts as a primary station that commands the ASOS to send data, the ASOS then responds with the requested data as instructed by the ADAS. In keeping with the HDLC-NRM specification the systems will format information for transport as shown in Figure 3-3. ADAS requests data from the ASOS every minute and every hour. The ADAS and ASOS also use a supervisory formatted frame when exchanging management-plane information, such as polls, errors, and acknowledgements. This format is similar to that depicted in Figure 3, with the information field omitted. Flags are continuously transmitted on the link between frames to keep the link active. On an ASOS interface operating at 2.4 kilobits per second (kbps), 300 of these inter-frame fill flags can be transmitted in one second[3].

F	A	C	I	FCS	F
---	---	---	---	-----	---

<u>Field Name</u>	<u>Length</u>
Flag Field (F)	8 bits
Address Field (A)	8 bits
Control Field (C)	8 or 16 bits
Information Field	Variable
Frame Check Sequence (FCS)	16 or 32 bits
Closing (F)	8 bits

Figure 3. HDLC-NRM Information Transfer Frame Format

The use of dedicated point to point circuits for transport requires 20 ADAS systems to be located throughout the NAS. In contrast, only two ADAS systems (1 primary and 1 backup) would be needed if an IP based “network cloud” were used for ASOS/ADAS transport. Having just 2 ADAS systems would reduce operational and hardware costs. ASOS/ADAS connections could take advantage of the FTI IP infrastructure (even if their interfaces have not been upgraded to IP) using a variety of transition mechanisms.

3. Transition Alternatives

Transition mechanisms that can be used to move from a legacy network environment (e.g., X.25, HDLC) to an IP based environment can be categorized into two major areas. The first is

tunneling where encapsulation/de-encapsulation of incoming legacy packets is performed without doing any modification to the headers of packets. The second method is protocol conversion where headers of incoming packets are modified to native IP format and then routed in an IP network. While the first scheme is simpler from a packet handling perspective, there can be overhead costs and performance issues primarily at the ingress and egress devices where encapsulation and de-encapsulation of the packets takes place. On the other hand, protocol conversion is more complicated when it comes to packet handling because modifications are made in the headers of the packets. Once the packets are turned into native IP format they are treated like any IP packet and there will not be overhead issues incurred while in transit to the destination system.

The tunneling technology that was used in the proof of concept evaluations is Serial Tunneling (STUN)[4]. STUN is a proprietary tunneling technology that has been used for integrating/transitioning legacy systems to IP environments. In the case of ADAS/ASOS connectivity, STUN Basic is the proper variation of STUN to use since serial protocol addressing is not important for HDLC. HDLC uses the 7E flag to maintain connections which, in effect, keeps the STUN session active from an HDLC perspective.

Another tunneling technology is Circuit Emulation over IP (CEoIP). In CEoIP, the legacy data is treated as a random bitstream regardless of prior format. It is mostly used for wide area transport. It is a candidate solution for ASOS-to-ADAS connectivity, but was not included in this study

4. ADAS/ASOS Connectivity Tests

Proof of concept lab tests were performed to evaluate STUN and protocol conversion as interim solutions for ASOS-to-ADAS connections on the path to a native IP connectivity. Simulations were also performed to determine how router performance is affected by increasing the number of STUN tunnels.

Tunneling (STUN) Tests

The first test was performed to determine whether an ASOS-to-ADAS connection facilitated via a serial tunnel (STUN Basic) between routers could result in a successful handshake between the ADAS and ASOS as shown in Figure 4. Routers were connected serially to the end systems. A back-to-back “WAN” connection, a STUN tunnel, and routing were created between the routers. Communication was then established between the ASOS and ADAS while application level handshake and subsequent data exchange was monitored using a protocol analyzer connected in-line. The test results showed the creation of a satisfactory STUN connection with an underlying robust TCP session between the ASOS and ADAS ports under test.

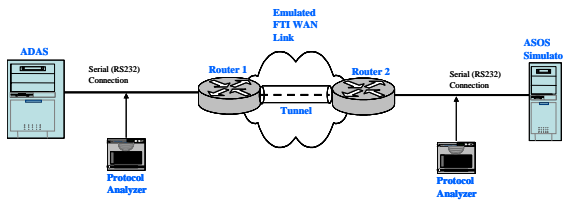


Figure 4. Test Setup for ADAS-to-ASOS Tunnel Connectivity Test

A second test was performed to investigate the effect of speed modification between the end systems and corresponding router connections (e.g., ADAS to Router 1), as well as between the routers themselves (if a serial interface is used between the routers, see Figure 4). It was observed that while the connection speed between ADAS and Router 1 could be increased to the ADAS limit, the connection to ASOS would not work properly at higher rates and would therefore determine the overall rate.

A third test was conducted to determine whether STUN supports multipoint connectivity for systems that use HDLC for communication such as ADAS/ASOS. The test setup is shown in Figure 5. In this test, several serial tunnels (STUN Basic) belonging to the same group were created on two routers and configured with the same IP address belonging to the loopback interface of the opposite router. It was observed that STUN sessions were not established and the test failed. This test seems

to confirm that the vendor’s implementation of basic serial tunneling does not support multipoint connectivity for the HDLC protocol.

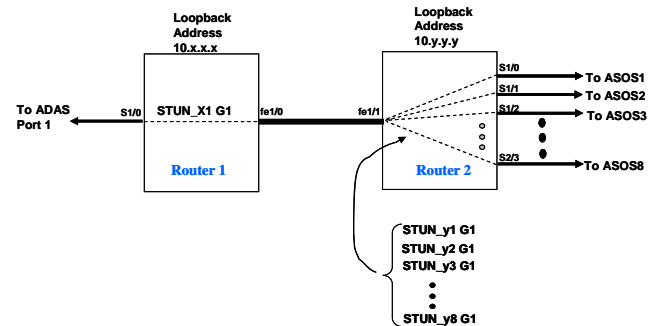


Figure 5. Multipoint Test

A fourth and final test determined that an ADAS-to-ASOS connection facilitated via a serial tunnel (STUN Basic) between routers was robust and could recover from failures without major reconfiguration. The setup in Figure 4 was used for this test. Failure was introduced by disconnecting cables. The result for this test showed that brief connectivity disruptions did not result in session failures.

Protocol Conversion

The objective of this test was to determine whether an ADAS-to-ASOS connection facilitated via protocol conversion could result in a successful handshake between the two systems. Protocol converters were connected via an Ethernet switch as shown in Figure 6. The end systems (ADAS and ASOS) were connected serially to the converters. Communication was established between the ADAS and ASOS while application level handshake and subsequent data exchange was monitored using a protocol analyzer connected in-line.

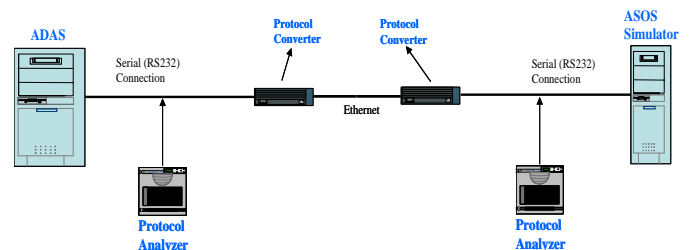


Figure 6. Back-to-Back Connection of Converters

A second test was performed to determine whether an ADAS-to-ASOS multipoint connection facilitated via protocol conversion could result in a successful handshake and data transmission between the two systems as shown in Figure 7 (Note that in actual field implementation the converters would communicate via IP routers that would form an IP cloud). The test was set up to emulate the connection of an ADAS port to two ASOSs. Three protocol converters were used where one converter was connected to the ADAS port and the other two were each connected to the two ASOSs using the serial ports of the converters. All three converters were interconnected via an Ethernet switch and communicated using IP. The test showed that the protocol converters can successfully perform HDLC packet conversion and establish IP sessions with peer converters.

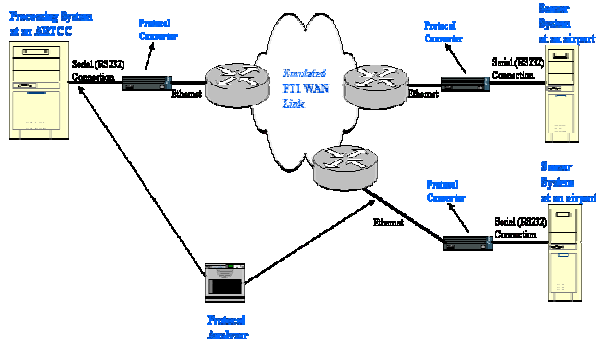


Figure 7. Multipoint Protocol Conversion Test

A third test was conducted to determine whether an ADAS-to-ASOS connection facilitated via protocol conversion was robust and could recover from failures without major reconfiguration. The setup in Figure 7 was used for this test. Failure was introduced by disconnecting cables and shutting down router interfaces via router operating system commands. The result for this test showed that brief connectivity disruptions did not result in session failures.

The purpose of the final test was to investigate the effect of speed modification between the end systems and corresponding protocol converter

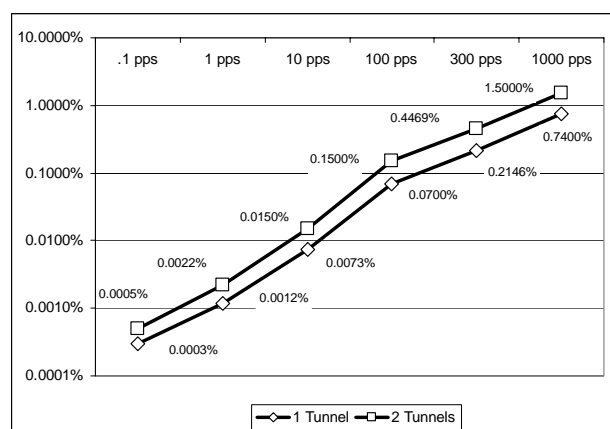
connections (ASOS and ADAS to their respective converters, see Figure 6). It was observed that while the connection speed between ADAS and its converter could be increased to the ADAS limit, the connection to ASOS would not work properly at higher rates and would therefore determine the overall rate (currently 2.4 kbps).

Simulation Description

A simulation study was performed to investigate router performance with multiple STUN tunnels. The simulation used mid-level router² models for the destination and source routers and generic tunneling protocol models to support the STUN configuration. Sources are configurable to transmit data at selected packet rates.

While the simulation allows many generic tunnels to be configured on a router, the number of STUN tunnels that a router can support is, in fact, limited by the number of serial ports available. Mid-level routers may have a limitation of 24 ports, while high end routers may be able to support up to 70 such interfaces.

The simulation performed measures the CPU utilization of the destination router for one to four terminating tunnels operating at various packet rates. The simulated CPU utilization is shown on a logarithmic scale in Figure 8 and Figure 9. Packet rates studied range from one packet per second to 1000 packets per second. Figure 10 shows the ratio of router utilization for four tunnels to the utilization for one tunnel.



² The Cisco 3745 has a port capacity to support 8-12 serial tunnels. The Cisco 7505 would have enough port capacity to support around 20-24 serial tunnels.

Figure 8 Destination Router Utilization with One and Two Tunnels

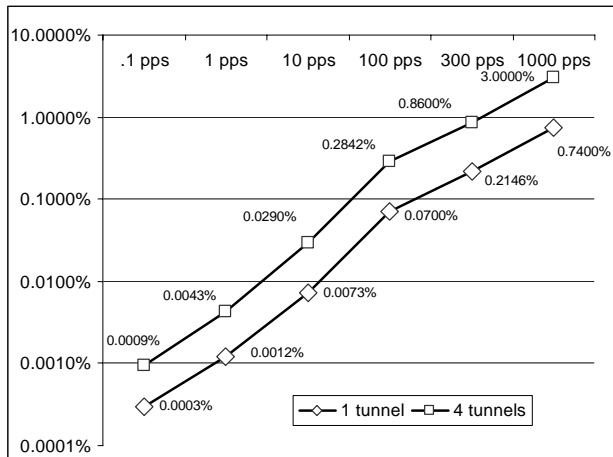


Figure 9. Destination Router Utilization

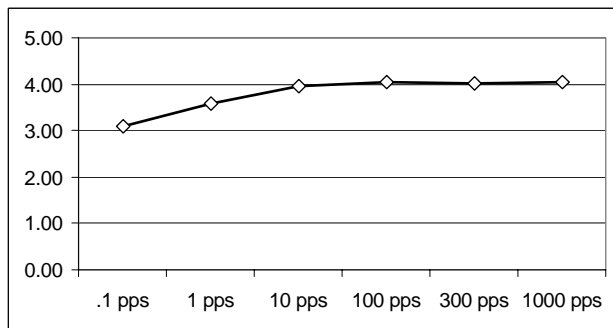


Figure 10. Ratio of Four-Tunnel and Single-Tunnel CPU Utilizations

The data in Figure 10 suggest, as expected at the outset, that router utilization changes linearly for increasing number of supported tunnels. Two tunnels at a packet rate of 300 packets per second (pps) are shown in Figure 8 to cause a 0.45% utilization of the router, approximately double the 0.21% figure for one tunnel. It is estimated by extrapolating to 10 tunnels, as listed in Table 1, that router utilization would approach 2.1%, and by extrapolating to 30 tunnels, to 6.3 %. Extrapolating much more than 30 tunnels would surpass the port limitation of the mid-level routers studied in this analysis. At packet rates less than 100 pps 30 tunnels would not cause more than 1% utilization.

While this study is limited to determining the impact of ASOS tunnels, it should be remembered that the destination router used in this simulation study will likely support other interfaces and tunnels in addition to the ASOS tunnels. It seems reasonable that tunnels supporting the ADAS interface to ASOS should not exceed 10% of CPU utilization.³ At packet rates of 1000 pps, about 13 tunnels can be supported before exceeding the arbitrary CPU limit. At packet rates of 300 pps and less the maximum number of tunnels can be supported for a mid-level router without adverse affect on CPU performance.

Table 1. Extrapolated CPU Utilization Results

Packet Rate	10 Tunnels	20 Tunnels	30 Tunnels
.1 pps	0.0030%	0.0050%	0.0070%
1 pps	0.0120%	0.0220%	0.0330%
10 pps	0.0730%	0.1500%	0.2180%
100 pps	0.7000%	1.5000%	2.1300%
300 pps	2.1460%	4.4690%	6.3000%
1000 pps	7.4000%	15.0000%	22.0000%

6. Summary

Overall, the results from both tunneling and protocol conversion tests were positive for ADAS-to-ASOS connectivity. While STUN Basic worked well in a point-to-point mode, it failed in a multipoint mode. Test cases for routing scheme variation, clock-rate variation, and failure recovery were performed successfully. Testing for multipoint connection using serial tunneling failed.

The protocol conversion testing that was done for the connectivity between ADAS and ASOS produced promising results. It was shown that both

³ This assumes that total CPU utilization should be limited to about 30% with 1/3 of this utilization allocated to the support of AWOS/ASOS tunnels.

point-to-point and multipoint connections can be supported using protocol converters.

CPU utilization was reasonable when STUN tunnels were configured in a mid-level router. Results from scalability studies using a modeling tool show that a reasonable number of tunnels can be supported without major performance impact on the routers.

The tests as well as the simulations performed in this study proved that serial tunneling and protocol conversion are viable options for implementing ASOS-to-ADAS connectivity during the transition to a native IP implementation of ASOS and ADAS applications.

References

1. Kranz, J., July 2004, personal communication, Operational Technologies Services, Inc., Washington, D.C. .
2. Chapman, B., May 2004, personal communication, FAA/ATO, Atlantic City, NJ.
3. Schlain, E., July 2004, personal communication, Titan Corporation, Atlantic City, NJ.
4. Cisco Systems, "Cisco's Implementation of Serial Tunneling," <http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca771.html>.
5. Jalleta, Ezra et al., July 2004 "Analysis of Potential IP Solutions for Networking FAA Weather Systems", The MITRE Corporation, McLean, VA

NOTICE

This work was produced for the U.S. Government under Contract DTFA01-01-C-00001 and is subject to Federal Aviation Administration

Acquisition Management System Clause 3.5-13, Rights In Data-General, Alt. III and Alt. IV (Oct. 1996) [5].

The contents of this document reflect the views of the author and The MITRE Corporation and do not necessarily reflect the views of the FAA or the DOT. Neither the Federal Aviation Administration nor the Department of Transportation makes any warranty or guarantee, expressed or implied, concerning the content or accuracy of these views.

© 2005 The MITRE Corporation