AWIPS WAN Update

Hoi Y. Chong
Northrop Grumman Information Technology, McLean, Virginia

1. INTRODUCTION

The AWIPS Wide Area Network (WAN) is a nation-wide private network. The network was built to interconnect about 140 AWIPS sites and provide the point-to-point, and multipoint-to-point communications. High network availability and data delivery timeliness are the major requirements of this network. The WAN was fully deployed in July 1999. Since then, the WAN has gone through a network circuit bandwidth upgrade followed by transitioning its circuits from the AT&T FTS2000 network to the MCI/WorldCom FTS2001 network. Enhanced monitoring tools have been installed to improve the network monitoring capability. This paper briefly discusses the network architecture, network monitoring capability, domain name system, circuit bandwidth upgrade and the transition from the FTS2000 network to the FTS2001 network.

2 AWIPS WIDE AREA NETWORK ARCHITECTURE

2.1 *Network Topology and Routing Protocol*

The AWIPS WAN is an Internet Protocol (IP)-routed network. It consists of routers and dedicated circuits that interconnect about 140 of the 150+ AWIPS sites. The remaining sites obtain their data from co-located sites. The WAN interconnects the Weather Forecasting Offices (WFOs), collocated WFO/River Forecast Centers (WFO/RFCs), National Centers (NCs), Regional Headquarters (RHs), and the Network Control Facility (NCF). It covers the Contiguous US (CONUS), Alaska, Guam, Hawaii, and Puerto Rico. The network uses frame-relay permanent virtual circuits (PVCs), fractional T1s and T1s for dedicated circuit connections. It uses the Integrated Services Digital Network (ISDN) and Switched 56K (Switched Data Service) for backup. Figure 1, AWIPS Terrestrial Backbone Network and Hub Nodes, and Figure 2, AWIPS Sites to Backbone Hub Node Connectivity illustrate the AWIPS WAN topology. The Collocated WFO/RFCs serve as network hubs. The network hubs and NCF are interconnected to form a backbone network as shown in Figure 1. Other sites, except in Alaska and the Pacific Region, each have two PVCs that connect to two backbone hubs. The Alaska region only uses a single hub and the other sites there have one PVC each connecting to it. The Pacific region, consisting of the sites in Hawaii and Guam, use T1 and fractional T1 circuits in place of PVCs.

The AWIPS WAN runs Open Shortest Path First (OSPF) routing protocol. The network is divided into 9 OSPF areas that do not correlate exactly with the organizational NWS Regions:

- Area 0—backbone network that interconnects the hubs and NCF.
- Area 1—the NCF and other sites at Silver Spring, MD.
- Area 2—Northeast and Mid Atlantic RFCs, NC, RH, and WFOs.
- Area 3—Ohio and North Central RFCs and WFOs.
- Area 4—Missouri Basin and Arkansas/Red Basin RFCs, RH, NC, and WFOs.
- Area 5—Pacific, Northwest, California-Nevada RFCs, RH, and WFOs.
- Area 6—Colorado Basin and West Gulf RFCs, RHs, NC, and WFOs
- Area 7—Lower Mississippi and Southeast RFCs, NC, and WFOs.
- Area 8—Alaska RFC, RH, and WFOs.

The WAN is assigned one class B and nine class C IP network addresses.

2.2 *Redundant Features and Backup Scheme*

The AWIPS WAN is a high availability network with considerable redundancy. Figure 3, Typical WFO Configuration, shows these redundant features. A typical WFO has two routers and 2 PVCs connected to a single CSU/DSU for the site's frame-relay network access. A Switched 56K circuit provides WAN access dialup in the event both PVCs fail. The two routers and both PVCs actively share the traffic in and out of the site, to balance loads on the circuits. The serial ports of router-1 and router-2 at each site provide backup capabilities.

Figure 4, Typical Collocated WFO/RFC to Frame Configuration, depicts a CONUS network Hub. A collocated WFO/RFC has between two and four frame-relay network access ports, the number being determined by the number of nodes it must support. Each access has a dedicated CSU/DSU. These sites also have four Switched 56K circuits.

The network backup scheme is built upon the use of Switched 56K at the field sites, with Switched 56K circuits and ISDN PRIs (Primary Rate Interfaces) at NCF. If a WFO site becomes isolated from the WAN, it can use its Switched 56K circuit to connect either to its normal backbone hub or directly to the NCF. This Switched 56K backup scheme has served its purpose well during individual circuit outages. However, the sites have occasionally experienced complete WAN outages resulting from more extreme events, such as optical fiber cable cuts. This can cause both frame-relay PVCs and the Switched 56K circuit to fail.

2.3 *AWIPS Domain Name System*

The AWIPS WAN uses a standardized Domain Name System (DNS). The AWIPS hosts reside on one or more local area networks (LANs) at each site. Each LAN can have up to 126 hosts but a typical site will have about 40. The total number of AWIPS LAN hostnames is thus about 6,000. The AWIPS DNS uses a distributed data base structure to facilitate the hostname and IP address lookup. The AWIPS domain name is `awips.noaa.gov`. Under “awips” there are 6 subdomains according to the NWS administrative region structure:

- er: Eastern Region,
- sr: Southern Region,
- cr: Central Region,
- wr: Western Region,
- ar: Alaska Region,
- pr. Pacific Region.

The AWIPS host domain name structure is: ‘host-site.subdomain.awips.noaa.gov’. For example, a host application server1 (as1) at the Kansas City RFC (krf) uses the domain name `as1-krf.cr.awips.noaa.gov`.

The DNS data base files are kept manageable by limiting their content to the LAN hostnames and associated IP addresses. Reverse lookup is also available for the LAN host IP address. The point-to-point subnet hostnames and their IP addresses are not incorporated into the data base. The NCF is the primary server for all 6 subdomain data bases. The field sites have two secondary-servers, each containing from 1 to 3 subdomain data bases.

2.4 *Network Security*

The AWIPS network is a private network that does not exchange any IP routes with any outside networks. The network is protected by a firewall at any AWIPS site having connections to other networks. All the dial up circuits either have a call-back or password feature enabled. The NCF also retrieves the WAN router configuration files periodically to verify their integrity.

3. WAN MONITORING

3.1 *Commercial Off-the-Shelf Tools*

The AWIPS WAN is maintained by the NCF. The NCF is manned 24x7, and the staff monitors the network and takes corrective actions when needed. The primary network management tool is Hewlett-Packard (HP) OpenView IT/Operations (IT/O). IT/O monitors all the router ports by periodically pinging the router port IP addresss. If a router port does not respond properly, an IT/O alarm is triggered at the NCF IT/O management console. The router also generates simple network management protocol traps for numerous conditions, such as port interface up and down. These traps are automatically caught by IT/O, allowing the NCF to monitor the WAN circuit and router conditions in near real time.

The WAN probes are installed at network hubs to monitor all the frame relay PVCs. The WAN probes collect traffic statistics for each PVC. The WAN traffic characteristics can be analyzed by using the embedded Netmetrix tools.

The NCF also runs TrendSNMP to collect all active router port traffic data such as input/output byte counts, error packets, etc. TrendSNMP generates a daily report of router ports showing an error rate greater than 15%. These reports allow the NCF to rapidly correct any hardware or circuit problem.

3.2 *In-house Developed Tools*

The COTS WAN monitoring tools check only active circuits and their corresponding router ports; backup circuits are not monitored. After encountering situations in which backup circuit did not work when needed, the project developed an interactive software program (programmed in Expect, Expect is a Tcl-based toolkit for automating interactive program) to exercise all the dialup circuits periodically. This allows NCF to detect any backup circuit problem before it is needed for operations.

Figure 3 and 4 depict interconnections between the routers and the circuits. The router serial ports and circuits are interconnected by switch modules. Normally both routers are active and the switch modules are on “A” position. The routers back each other up by switching to the “B” position. The NCF occasionally finds one or more switch modules switched to “B” with no attendant error condition. Since this could affect the redundant feature and circuit load balancing, the NCF now runs an interactive software program (programmed in Expect) to periodically query the switch module status at each site. The program will trigger an IT/O alarm if it detects any switch modules set to the “B” position.

4. WAN CIRCUIT BANDWIDTH UPGRADE

During the AWIPS deployment phase, each WFO (including NC or RH) frame relay had a committed information rate (CIR) of 64 Kbps and each backbone frame relay PVC had a CIR of 256 Kbps. The WAN traffic at that time was not particularly demanding. However, radar products would soon traverse the network. The WAN bandwidth upgrade was planned and implemented to meet this anticipated increase in traffic.

This upgrade required new T1 rate frame relay access circuits at some hub sites. At these sites, some existing PVCs were moved to new access circuits. This required reconfiguring frame-relay CSU/DSUs at all sites with new channel assignments. The process was complicated by the requirement to remain operational throughout the upgrade. The redundancy designed into the AWIPS WAN architecture permitted a WAN upgrade without a network outage.

5. WAN CIRCUIT TRANSITION FROM AT&T FTS2000 NETWORK TO MCI/WORLDCOM FTS2001 NETWORK

Soon after the WAN bandwidth upgrade was completed, the NWS began to transition all AWIPS WAN circuits from the AT&T FTS2000 Network to the MCI/WorldCom FTS2001 Network. The NWS’s transition task order included the following requirement: *All NWS sites to support dual network operations during the transition from FTS2000 to FTS2001. Dual network operation is defined as both the AT&T and*

MCI/WorldCom network being available for operation but not being used by AWIPS simultaneously.

The effort to transition the circuits from one network to another without experiencing WAN down time was more complicated than the earlier upgrade. The NWS did what it could to simplify the effort by requesting that MCI/WorldCom reuse the AT&T frame-relay PVC data link control identification (DLCI) wherever possible. The redundant AWIPS WAN architecture including dual WAN access was again critical in remaining operational during the transition. The new circuits were tested before being accepted for operational traffic by adding a few switch modules at each WFO site (including RH and NC), extra switch modules and a transition router at each hub site (collocated WFO/RFC), and two transition routers at the NCF. With this minimal hardware installation at each site, the system transitioned to FTS2001 circuits with no network down time.

6. CONCLUSION

So far the AWIPS WAN has served its purpose well. The network architecture has supported the network circuit bandwidth upgrade and circuit transition from the FTS2000 network to the FTS2001 network smoothly. The AWIPS WAN is an evolving network. As new application and traffic requirements arise, the network will be adjusted to continue providing reliable support.

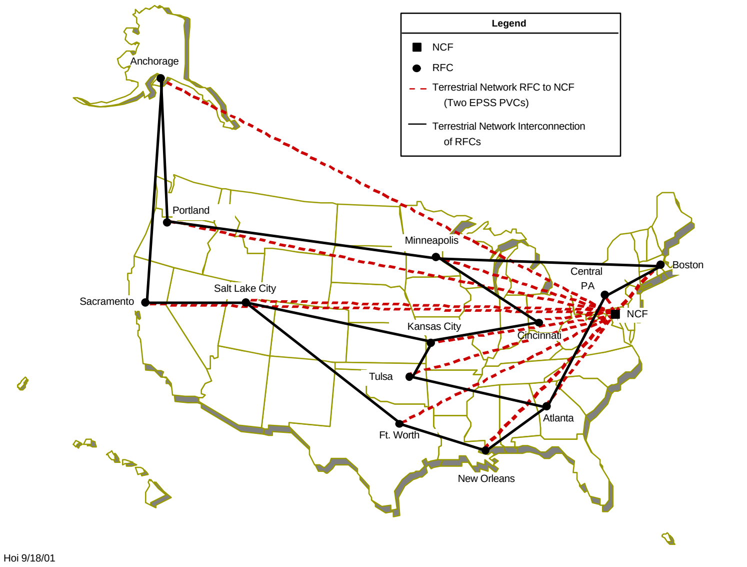

Figure 1. AWIPS Terrestrial Backbone Network and Hub Nodes

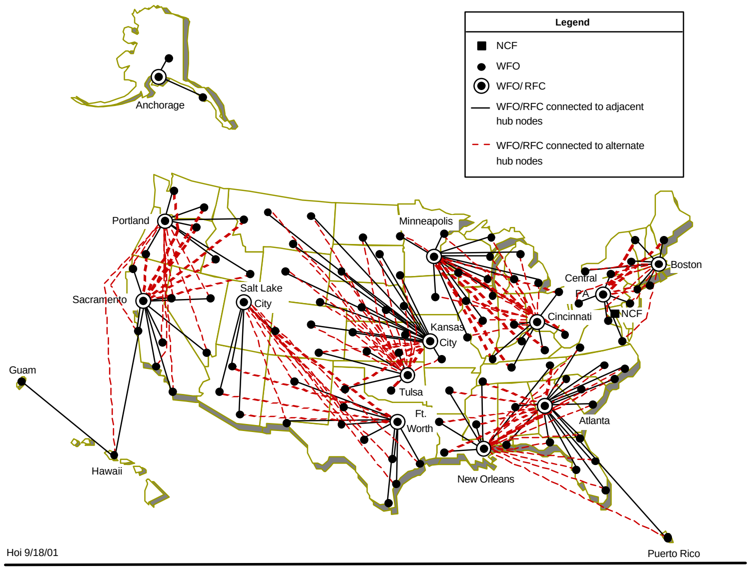

Figure 2. AWIPS Sites to Backbone Hub Node Connectivity

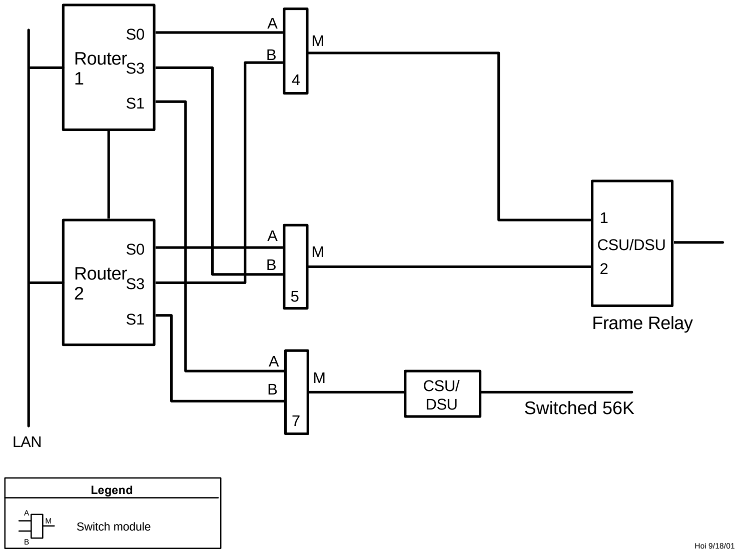

Figure 3. Typical WFO Configuration

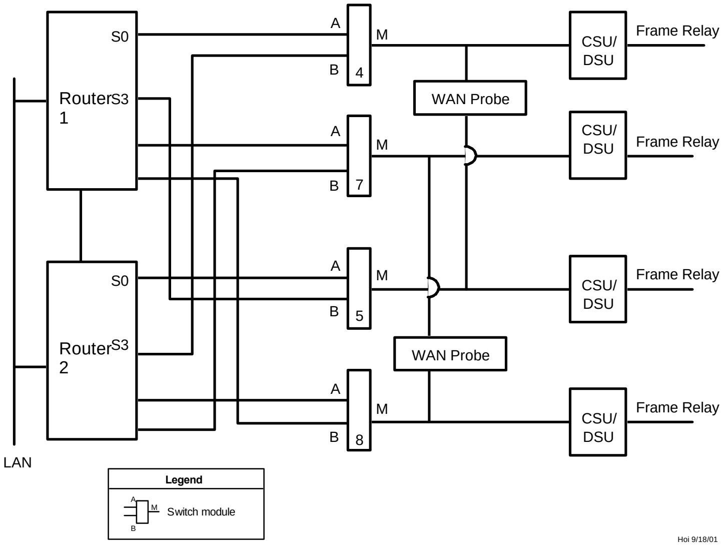

Figure 4. Typical Collocated WFO/RFC to Frame Relay Interface