EVLA Monitor And Control Network

Requirements and Description

Version 1.0.0

Revision History

Revision	***Date***	***Authors***	***Description of Changes***
1.0.0	October 7, 2004	James Robnett Bill Sahr (formatting)	This document consists of section 9.6 of the EVLA Project Book as written by James Robnett. It has been reformatted for presentation at the MIB Critical Design Review.

Table of Contents

1 EVLA Monitor and Control Network (MCN)

The EVLA Monitor and Control Network links all antenna, correlator, and backend devices to the central Monitor and Control systems.

1.1 MCN General Description

The MCN, with one minor exception, will be fiber Ethernet. The exception (noted in 1.3.1.2) will be twisted pair copper. TCP and UDP packets will carry commands and status information between the control systems and devices. Each antenna will be treated as its own Class C network.

1.2 MCN Requirements

The MCN must be able to support expected M & C traffic both in functionality and in load. The MCN must also not hinder instrument performance either through RFI or availability.

1.2.1 MCN Hardware Requirements

1.2.1.1 MCN Performance requirements

The MCN must be able to sustain an aggregate 200Kb/s per antenna and 4000 packets/s per antenna. (Assumes 1 packet/10ms* 40 MIBs per antenna.)

1.2.1.2 MCN RFI requirements

The MCN must meet the RFI requirements defined in section 3.8 of the Project Book.

1.2.2 MCN Software Requirements

1.2.2.1 MCN Protocol support

The MCN must support both TCP and UDP packets. The MCN must support any protocol such as FTP, HTTP, RPC mandated by the MC software system. The central distribution switch must support both Layer-2 and Layer-3 routing. This switch must have VLAN capabilities on all ports.

1.2.2.2 MCN Access requirement

Access to portions of the MCN may be required from remote locations. The exact details of this access will be defined at a later time. Those details should not directly affect the physical design of the network.

1.3 MCN Design

1.3.1 MCN Hardware in control building

The MCN will be a mixture of 100-1000Mbit single mode and multi mode fiber. Multiport fiber switches will be used to connect all components of the Monitor and Control System (MCS). The switched fiber fabric should meet performance and software requirements as well as mitigating RFI. QoS (quality of service) functionality may be desirable to ensure proper prioritization of traffic. Specifically the QoS capabilities must extend to VoIP traffic.

1.3.1.1 MCS Central Hardware

All MCS computers in the control building will be connected with 1Gbit full duplex multi-mode fiber through switches. The link between this cloud and other sections of the MCN will be 1Gbit multi-mode. 10Gbit may eventually be required.

1.3.1.2 Deformatters

The MCN connection to the deformatter boards will be through 100Mbit twisted pair copper. These devices will be physically located in the (shielded) correlator room. They will be addressed as if they were in their associated antenna.

1.3.1.3 LO Tx/Rx and power

These devices will be in the control building but will also be addressed as if they were internal to their antenna via the VLAN capabilities of the central distribution switch.

1.3.1.4 Other MCS devices in control building

All other MCS devices in the control building such as the weather station, correlator, and backend cluster will be accessed via multi-mode full duplex fiber. Individual connections will be run at 100Mbit or 1Gbit as required.

1.3.1.5 MCS Control building to Antenna link

Each antenna will be connected to the Control building via a 1Gbit full duplex single-mode fiber. All antennas will be connected using attenuated long distance network interfaces that will work over the entire range of distances.

1.3.2 MCN Antenna Hardware

1.3.2.1 Antenna to MCS Control building link

Each antenna will have a fiber switch with a mate to the control building end of the link. All antennas will be connected using attenuated long distance network interfaces that will work over the entire range of distances.

1.3.2.2 MCN antenna network

Each antenna will have a single fiber switch. One port will be connected to the MCS network as described in the previous section, the remaining ports will be directly connected to the MIBs via 100Mbit multi-mode fiber. Additional ports on the switch will be available for transient devices such as laptops or test equipment. These devices will also connect via 100Mbit multi-mode fiber. Until fiber based phones are available the 100Base-T VoIP phones will be connected to the switch via a media converter. The antenna switch should be capable of isolating broadcast between MIBS while allowing direct MIB to MIB communication where needed.

1.3.3 MCN addressing

The scale of the MCN requires that device addressing be separated into logical blocks of reasonable size.

1.3.3.1 Antenna addressing

Each antenna will be a single Class-C network of the form aaa.bbb.xxx.yyy where xxx defines the antenna and yyy defines the device in the antenna. The aaa.bbb portion will have a fixed value of 10.80. The xxx portion will be the antenna number +100. The yyy portion will be the slot number assigned as per the document "EVLA Hardware Networking Specification" (Wayne M. Koski, document #A23010N0003). As referenced in 1.3.1.3 some devices may be addressed as part of an antenna even though they are not physically in the antenna. Two or three of these Class-C networks will be set up in the AOC to facilitate testing. These networks will be addressed as 10.64.x.y.

1.3.3.2 Control building addressing

The MC systems in the control building that include both control computers, switches and AMCS devices will be addressed together as the zero'th antenna.

1.3.4 MCN access

Access to the MCN will be restricted and based on the point of origin of the remote connection. Types and levels of access from specific sites have yet to be determined. The selection of the 10.x.y.z network automatically precludes direct access from non-NRAO facilities. We are capable of allowing (or blocking) direct traffic to the EVLA for those links for which we have complete end-to-end management.

1.3.4.1 MCN access from VLA systems

Specific access requirements still to be addressed. The VLA network and EVLA network are separated by the site router. Allowing or disallowing traffic flow between the networks can be easily controlled at either router.

1.3.4.2 MCN access from AOC systems

Specific access requirements still to be addressed. The AOC and EVLA sites are directly connected by the VLA and AOC routers. Allowing or disallowing traffic flow between the networks can be easily controlled at either router.

1.3.4.3 MCN access from NRAO systems

Specific access requirements still to be addressed. All NRAO facilities have direct connections to the AOC router and therefore direct access to the VLA site router and EVLA. Traffic flow can be controlled between the EVLA and any of the sites to meet access requirements. The Mauna Kea and Los Alamos VLBA stations are the lone exceptions. From a network perspective they appear as non-NRAO systems

1.3.4.4 MCN access from non-NRAO systems

Because the EVLA is in the 10.x.y.z network, direct traffic flow to the MCN is not possible from non-NRAO systems. By convention packets with this network address are not forwarded by internet routers. Indirect access to the EVLA network from non-NRAO facilities will fall into one of two categories.

Non-NRAO entities at non-NRAO facilities will first connect to a non-EVLA system likely located at the AOC. From there traffic will be limited in the same manner as it is for AOC systems. Since the link from the remote site to the AOC and from the AOC to the EVLA are disjoint, some form of interface or proxy will have to be designed for the AOC end of the system.

NRAO entities at non-NRAO facilities will be supplied with VPN (Virtual Private Network) client software. This will enable them to appear to be physically in the AOC even though they are not. Traffic flow will appear to be direct from the non-NRAO system to the MCN even though it will go through an intermediate system at the AOC. This form of link will not require a separate interface or proxy as the previous style will.

In both cases access can be restricted at the AOC independently of standard AOC traffic if so desired.