

APENDICE B.

PROTOCOLOS MOS Y SNMP.

B.1. Protocolo MOS (Media Object Server).

B.1.1. Antecedente del MOS.

Durante el verano de 1998 en la conferencia del revelador de ENPS del AP, en Orlando la Florida, fue celebrada la primera reunión del grupo del desarrollo del protocolo MOS (*Media Object Server*); donde participaron algunos de los mejores vendedores del software y de hardware de la industria de la difusión con la idea de desarrollar un protocolo abierto de acuerdo con la regeneración de los vendedores presentes del hardware y del software, y deseo propio del AP. De ahí, fue lanzado los conceptos fundamentales de este protocolo al dominio público. El primero de enero de 1999 participaron más de dos docenas de compañías en el desarrollo del MOS cuya meta era desarrollar y poner un protocolo de comunicaciones en ejecución común que permita la integración del equipo diverso de NRCS y del MOS. En esperanza de que éste crezca en un estándar de-facto-facto que se pueda entonces presentar al comité.

B.1.1.1. Las metas del grupo del MOS.

- ✓ Desarrollar e implementar un protocolo de comunicación en ejecución para el uso entre NCS y el MOS que permitan que estas máquinas se comuniquen con uno a independiente de vendedores.

- ✓ La implementación de un protocolo común que estará sobre una red de TCP/IP vía la comunicación del (*socket*) zócalo.

- ✓ El desarrollo del protocolo será hecho de una manera expeditiva para poder traer los productos del software y del hardware que apoyan el protocolo al mercado rápidamente.
- ✓ Cada nueva versión del protocolo será un "sistema estupendo" de la versión anterior, permitiendo a las máquinas que usan una más vieja versión del protocolo, un método de comunicarse con máquinas más nuevas, aunque usando un vocabulario más pequeño, más viejo, y reducido de la característica.
- ✓ Los mensajes serán sucintos y optimizados para la velocidad de la transmisión y procesamiento.
- ✓ Los mensajes harán uso de un formato marcado con etiqueta del *unicode* del texto.
- ✓ El protocolo será extensible para satisfacer los requisitos futuros de la industria.
- ✓ El desarrollo del protocolo estará con la cooperación de compañías que participan.
- ✓ Los que participan en el desarrollo del protocolo acuerdan apoyarlo público con su propia banda y esfuerzos de comercialización como iniciativa de la industria que participen y apoyen.
- ✓ El protocolo será presentado a los cuerpos de los estándares apropiados en una fecha más última. Sin embargo, se reconocen que el proceso de tener un protocolo repasado y adoptado como estándar "oficial" puede ser un proceso muy largo.

B.1.2. ¿Qué es el protocolo MOS?

Es un poderoso protocolo de comunicaciones utilizado para integrar y enlazar el sistema computarizado de NewsRoom (NCS) y (MOS) tales como los servidores video, los servidores audio, aún los almacenes, y generadores de carácter, aplicaciones de producción en la radiodifusión y equipos. El cual permite a los periodistas ver, utilizar y controlar dispositivos de medios incorporado en interfaces ENPS, quitando las barreras técnicas como los pedazos individuales de la tecnología de producción del NewsRoom hablando en un sentido común.

Fue desarrollado y apoyado con la colaboración cooperativa entre vendedores del equipo, vendedores del software y usuarios del extremo. En general, el protocolo MOS es responsable de la creación, de la modificación, y de la cancelación de objetos de los medios y de sus meta datos asociados y el NRCS, por su parte, se encarga de la creación, de la modificación, y de la cancelación de la información editorial, incluyendo *playlists*.

B.1.3. ¿Qué hace el protocolo MOS?

El protocolo de comunicaciones (MOS) permite que los sistemas informáticos de NewsRoom (NRCS) y (MOS) intercambiar informaciones usando un protocolo estándar es decir en (lengua y vocabulario). Este protocolo permite el intercambio de tipo siguiente de mensajes:

- ✓ **Datos descriptivos para los objetos de los medios.** En este caso, el MOS "empuja" la información descriptiva e indicadores al NCS mientras que los objetos se crean, se modifican, o se suprimen en el MOS. Esto permite que el NCS esté "enterado" del contenido del MOS y permite al NCS realizar búsquedas encendido y manipular los datos que el MOS ha enviado.
- ✓ **Intercambio de Playlist.** Es decir que, el NRCS puede construir y transferir la información del *playlist* al MOS. Esto permite que el NRCS controle la secuencia que los objetos de los medios son jugados (*Played*) o presentados por el MOS.

- ✓ **Intercambio del Estado.** Aquí, el MOS puede informar al NRCS el estado de los *clips* específicos o del sistema del MOS en general. El NRCS puede notificar el MOS del estado de los artículos específicos del *playlist* o de las órdenes corrientes.

B.1.4. Funciones ejecutable en el sistema gracias al protocolo MOS.

Algunas de las funciones que se ejecutan en el sistema del noticiero, gracias al protocolo MOS, son las siguientes:

- ✓ El reportero puede buscar *clips* de un determinado tema para acompañar una nota.
- ✓ El sistema alerta al productor cuando en la lista de emisión hay inconsistencias o vacíos (notas sin imagen o gráficos sin título, entre otros).
- ✓ El productor puede cambiar la lista de emisión cuando el programa ya está al aire.
- ✓ MOS permite llevar un registro de los materiales usados para reutilización posterior.
- ✓ MOS permite que servidores de diferentes fabricantes se conjuguen en un mismo sistema de noticias.

B.1.5. ¿Cuáles son objetos de los medios?

Por lo general, un *Media Object Server* (MOS) es cualquier dispositivo capaz de almacenar objetos de los medios; a continuación se nombran algunos:

- ✓ CGs (objetos del generador de carácter).
- ✓ Audio
- ✓ Aún almacenes
- ✓ Video

Generalmente, aunque no es un requisito, que estos objetos serán almacenados en un dispositivo no linear. Sin embargo se presume que, más adelante, se puede agregar otros tipos de objetos de los medios a esta lista.

B.2. Protocolo SNMP (Simple Network Management Protocol).

B.2.1. ¿Qué es el Protocolo SNMP?

El *Simple Network Management Protocol* (SNMP) es un protocolo basado en un sistema de **petición-respuesta**, aprobado por el IAB en 1988 y está fundamentado en SGMP que permite manejar los *routers* en Internet para la gestión de redes TCP/IP. Actualmente, el SNMP está soportado en muchos sistemas distintos tales como puentes, PC's, estaciones de trabajo, encaminadores, terminales, servidores, *hubs*, concentradores, y tarjetas avanzadas ethernet, *token ring* y FDDI. Los dispositivos no-SNMP deben utilizar agentes proxy que es un conversor de protocolo que traduce las órdenes SNMP a las comprensibles por el protocolo de gestión propio del dispositivo.

B.2.2. Arquitectura del SNMP

La arquitectura del SNMP consta de los siguientes componentes:

- ✓ **Gestores** (NMS's)
- ✓ **Agentes** (nodos administrados)
- ✓ **MIB** (base de datos con información)
- ✓ **SMI** (administración de la base de datos)
- ✓ **protocolos** (órdenes)

B.2.3. El SNMP y sus aportes.

Como aportes del protocolo SNMP se nombran a continuación:

- ✓ Define el diálogo entre una estación de control y un nodo de red.
- ✓ Permite conocer el estado de un aparato.

- ✓ Administra los eventos excepcionales.
- ✓ Permite la medición del tráfico y de los errores a distancia.
- ✓ Facilita la configuración de aparatos a distancia.

B.2.4. Amenazas a la seguridad.

El protocolo SNMP proporciona mecanismos para el acceso a un almacén de información jerárquica compuesta por un conjunto de variables. Se distinguen dos tipos distintos de acceso a dicha información: un acceso para lectura que permite consultar los valores asociados a cada una de las variables y un acceso para escritura que permite modificar dichos valores.

Los mensajes de la primera versión del protocolo incluyen una cadena de caracteres denominada nombre de comunidad que se utiliza como un sencillo mecanismo de control de acceso a la información. Los agentes que implementan dicha versión del protocolo disponen generalmente de dos comunidades, o conjuntos de variables (no necesariamente disjuntos), identificadas por un nombre de comunidad configurable por el administrador del sistema. Una de dichas comunidades recibe el nombre de comunidad pública, y sus variables pueden ser accedidas sólo para lectura. Por el contrario los valores asociados a las variables que componen la otra comunidad, denominada comunidad privada, pueden ser modificados.

Toda la seguridad proporcionada por el sistema se basa en el hecho de que es necesario conocer el nombre asignado a una comunidad para conseguir el acceso a la información proporcionada por sus variables. El nivel de protección ofrecido por la versión original del protocolo es, por tanto, muy débil. Más aún si se tiene en cuenta que los nombres de comunidad incluidos en los mensajes del protocolo SNMP viajan por la red en texto plano y por consiguiente pueden ser obtenidos como resultado de ataques pasivos (escuchas malintencionadas).