SNMP CONTROL FOR A SOFTWARE-DEFINED RADIO

Dave Dohse (General Dynamics Decision Systems, Scottsdale, Arizona, USA; dave.dohse@gd-decisionsystems.com);
Jim Crowe (General Dynamics Decision Systems, Scottsdale, Arizona, USA; jim.crowe@gd-decisionsystems.com)

ABSTRACT

Use of the Simple Network Management Protocol (SNMP) within a Software-Defined Radio (SDR) aligns control mechanisms with an accepted computer industry standard for network controllable devices. Incorporating SNMP in an SDR architecture challenges both the Real-Time (RT) nature of radio applications and the desire to make direct use of Common Object Request Broker Architecture (CORBA) messaging. To overcome these challenges, General Dynamics Decision Systems engineers have implemented a gateway between SNMP and CORBA. The gateway effectively de-couples the RT aspects of the radio from non-RT control by introducing translations between SNMP and CORBA. This paper discusses in greater detail the SNMP translation mechanisms including the concept of shadow objects. Also elaborated are the benefits of applying industry standard SNMP control to an SDR.

1. THE CASE FOR SNMP MANAGEMENT OF AN SDR

SNMP is not the only option for arbitration of external control into an SDR; however, it is our assessment that SNMP is the best solution at this time based upon a number of assessment factors. **Table 1** contrasts SNMP with the Common Management Information Protocol (CMIP) and direct CORBA control mechanisms [1] [2]. The table characterizes the relative merits of each approach for a set of attributes deemed significant to an SDR such as those defined by the Joint Tactical Radio System (JTRS) Software Communication Architecture (SCA) [3].

An SNMP-based approach to radio management addresses numerous factors that are key to providing an optimal SDR control structure. An SDR must often respond to control from a variety of devices (e.g., Human Machine Interface (HMI), Mission Computer, Remote Control Devices) over a potentially diverse set

Table 1. SNMP is a sound choice for SDR management as demonstrated by comparison with CMIP and Direct CORBA

Attributes	SNMP	CMIP	Direct CORBA access	Advantage
Industry Acceptance	Widely used for network management in conjunction with routers, etc.	In limited use	Emerging use in telecom applications but not yet for network management	SNMP
SDR Acceptance	Used in the Navy Digital Modular Radio (DMR) as the interface to an NT-based HMI and SPAWAR developed Remote Control Processor (RCP).	Unknown	Prototype SDRs exist with direct CORBA control. The JTRS SCA defines CORBA as the SDR control interface.	None
Language Bindings	Generic ASN.1 definitions can be compiled into C, C++, etc.	C/C++	Generic IDL bindings to C/C++/Java	None
Required Resources	Minimal	Large (10x SNMP)	Would require incorporating ORB into legacy environments	SNMP
Ease of Use	Simple, easy to understand Based upon well-defined Management Information Base (MIB) structure	Complex, few experts, difficult to use	Makes network management a transparent extension of normal programming	Direct CORBA
Monitoring and Analysis Utilities	Numerous Third Party tools and monitors available Analysis packages widely available including Shareware	Less Common	Custom with some emerging commercial tools (e.g., Vertel CORBA Explorer)	SNMP
Access Management (including multiple controllers)	Authentication via SNMP V3 and mechanisms to lock and restrict access to portions of the MIB	Built in authorization, access control and security logs	"Policy Objects" associated with CORBA security services offer flexibility but are not as intuitive as controlling access to variables in a database (e.g., MIB)	None

of bus structures (e.g., MIL-STD 1553, Switched Fabrics and Ethernet). SNMP provides the means for consolidating these device and bus interfaces within a common structure. Given the stringent availability requirements for SDRs, there is a desire to incorporate mature COTS products adapted to a wide range of operating environments. SNMP is widely accepted within industry and is compatible with a variety of platforms including Windows NT, Unix™, Linux™, Wind River's VxWorks™ and Green Hills Integrity™. COTS vendors also offer an extensive set of products for monitoring SNMP. SDR management must incorporate adequate locking mechanisms to prevent corruption from simultaneous controller modifications and restrict SDR access to authorized users. SNMP v3 offers the necessary security and integrity features for SDR-coordinated access management and control.

Despite the case made for use of SNMP to control an SDR, it would be a mistake to apply SNMP directly to file transfers or streaming data. To overcome this limitation, SNMP can be used to orchestrate setup of a secondary connection (e.g., FTP, NFS) between an external controller and the SDR. SNMP essentially steps aside during the actual data transfer.

2. SNMP TO CORBA [illegible] AN SDR FROM NON[illegible]

Use of SNMP within an S[illegible] with an accepted computer industry standard for network-controllable devices. Incorpo[illegible] SNMP into an SDR architecture challenges both [illegible] time (RT) nature of radio applicati[illegible] [illegible]ke direct use of CORBA messaging. To overcome these challenges, General Dynamics Decision Systems has implemented a gateway between SNMP and CORBA, as shown in **Figure 1**. The gateway effectively de-couples the RT aspects of the radio from non-RT control initiated from an HMI, by introducing translations between SNMP and CORBA.

As applications are instantiated within the SDR, they are assigned a Circuit ID. SNMP-related "shadow" objects (i.e., data caches) register with the CORBA gateway. The registration process establishes an interface repository linking a group of MIB variables to a corresponding CORBA shadow object. As an SNMP "get" or "set" request is received at the SDR, the gateway searches its interface repository for the corresponding "Arg Name" and "Circuit ID" and routes the request to the appropriate CORBA object. The "Arg Name" is internally linked to an SNMP Object Identifier (OID).

The SNMP Management Information Base (MIB) hierarchy specifies information that can be communicated to or from an SNMP-compliant device. SNMP agents for network devices (e.g., routers, printers and SDRs) are affiliated with a specific MIB branch. This affiliation enables the dynamic discovery of [illegible]Rs b[illegible] early stages of MIB [illegible], it [illegible]tice to produce an [illegible] MIB to test ideas and control methods. The [illegible]sed for standardization [illegible] has proven to [illegible]. To manage access from multiple external controllers (i.e., SNMP managers), [illegible]ter SNMP manager is given writer privileges; [illegible]ers are only readers (or "observers"). This ground rule eliminates many [illegible] problems [illegible] current access [illegible]rrent update).

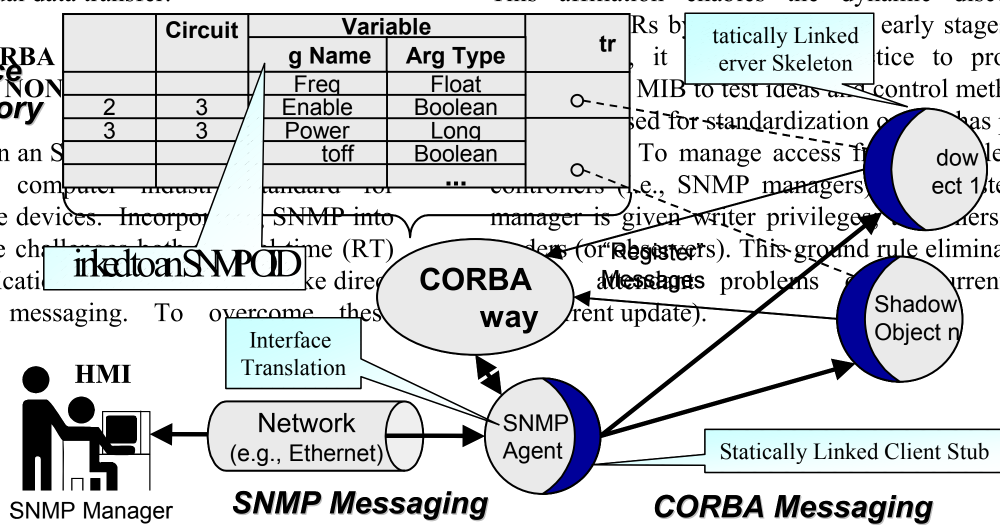

Figure 1. Managing External Control with SNMP by providing a gateway into CORBA environments

3. MIB STRUCTURE FOR THE NAVY DIGITAL MODULAR RADIO

The famil stand moni mana Obje famil Num inter Curr Expe WITS (3556). Thus, all MIB fall under the base the early stages of MI practice to work on a controls are still evolv proven effective, th standardization. The WI and MIB II as defined in

The WITS MIB is separated into groups for System Control, Interfaces, Waveforms and Security as shown in Figure 2. The MIB Groups further resolve into collection tables used l structure mple, the n Control own/restart of SNMP o f l, e x, " e d x g

System Control Group (1)	Interface Group (2)	Waveform Group (3)	Security Group (4)
Properties (1)	Audio (1)	**Amplitude Modulation (AM) (1)**	•
Presets (2)	Serial (2)	Frequency Modulation (FM) (2)	•
Bridges (3)	Radio Frequency (RF) (3)	Application 3 (3)	•
GPS (4)	Power Amplifier (4)	Application 4 (4)	
Events (5)		•	
Maintenance (6)		•	
Line Replaceable Unit (LRU) (7)		•	
Monitor (8)			
Software Update (9)			
Built In Test (BIT) (10)			
Time Management (11)			
Diagnostic Logging (12)			
Event Handling (13)			

MIB Entry	Element	Access	Data Type	Values	Description
1	**amCircuitControlTable**				Contains the parameters specific to the AM waveform. Each instantiation of AM creates a new MIB row in this table.
1.1	amCircuitControlEntry				
1.1.1	amCircuitIndex	read-only	Integer32	CKTID	Specifies the WITS circuit associated with this waveform instance.
1.1.2	amModulationIndex	read-write	Integer32	0..95	Sets the modulation index of this waveform instance.
1.1.3	amReceiveFrequency	read-write	Unsigned32	amMinRxFrequency-amMaxRxFrequency	Sets the receive frequency of this waveform instance.
1.1.4	amTransmitFrequency	read-write	Unsigned32	amMinTxFrequency-amMaxTxFrequency	Sets the transmit frequency of this waveform instance.
1.1.5	amSquelchLevel	read-write	Integer32	$0..2^{32}-1$	Sets the percentage of the squelch level. (Rel6.0: Range is 0..100%)
1.1.6	amReceiveSignalStrength	read-only	Integer32	(0-max) dBm *max dBm*	Reports the level of signal received by this waveform instance.
1.1.7	amBandwidth	read-write	Integer32	**0:** External Bandwidth **1:** Wideband Mode **2:** Narrowband Mode	Sets the bandwidth for the AM waveform. The External Bandwidth value allows the waveform to read the bandwidth from the external data device on the port. The other two values set the waveform bandwidth directly.

Figure 2. The WITS MIB is part of an extensible MIB structure registered within the IANA hierarchy.

4. SNMP MESSAGING WITHIN THE DMR

A closer look at th
shown in **Figure 3**
with the CORBA C
Event Manager. **Pa**
to CORBA convers
protocols and busses
and CORBA over a
within the radio). SN
CORBA Refreshes b
path translates COR
Objects to SNMP Ge

originating in the radio are logged in the “Event
at ultimately
I. The radio
hirty seconds
nse) to avoid
ic messaging
nitial SNMP
g information
he request is
the radio’s
ystematically
and CORBA

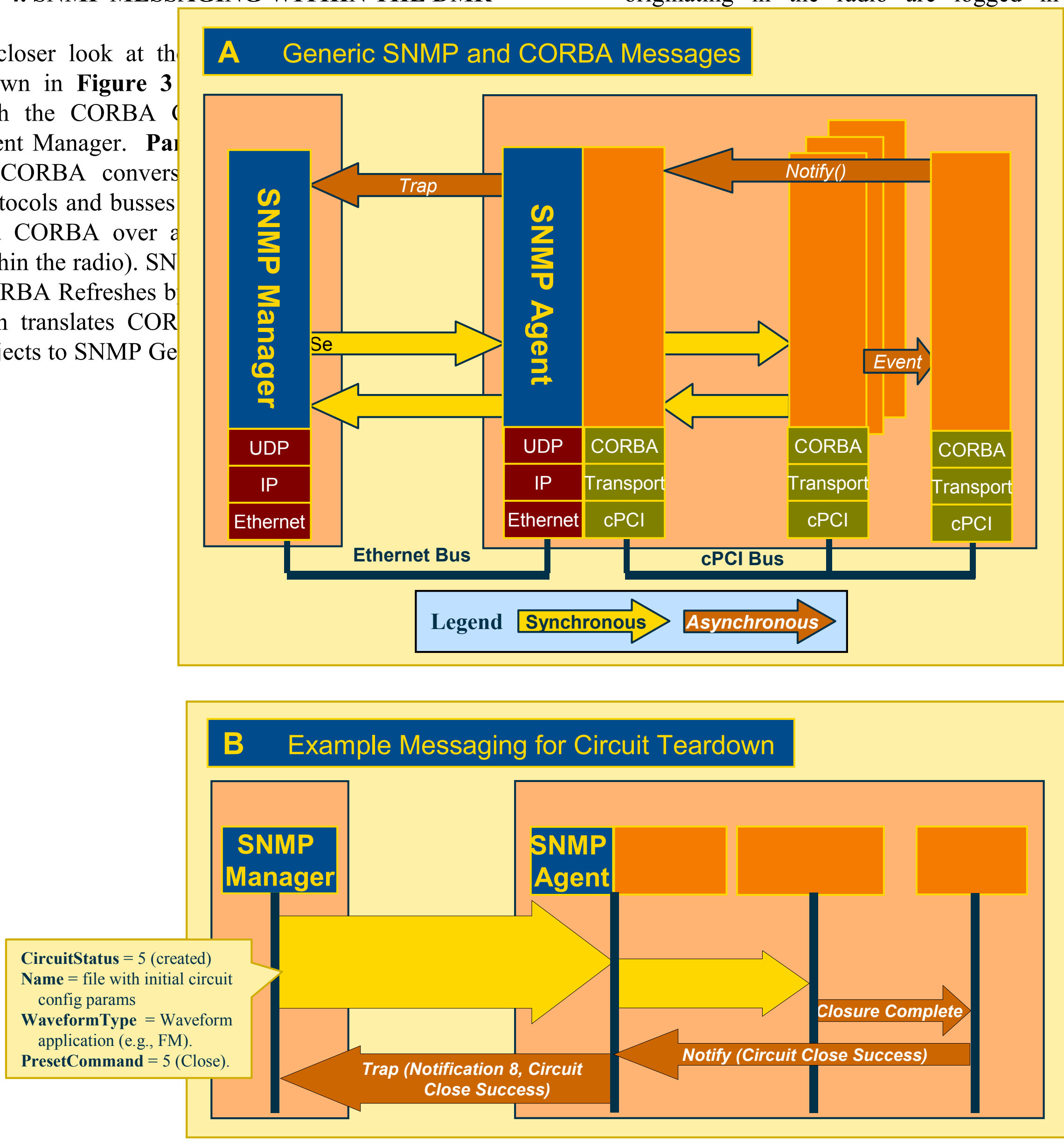

Figure 3. The CORBA Gateway within the DMR translates SNMP Messages to CORBA.

connections before reclaiming the application's resources (processing, memory, devices). The final steps involve use of the event services to send a Notify and ultimately a Trap back to the HMI signaling the successful closure of the circuit. At this stage the resources previously held by the closed application are now available for establishment of a circuit for a new application instantiation.

It is possible to extend SNMP by bundling commands and data for more efficient operation. SNMP "set" and "get" primitives can be "stacked" as multiple entries in the "variable-bindings" list within an SNMP Protocol Data Unit (PDU) as described in RFC 1157. A front end to the SNMP agent that queues received SNMP commands provides a means of allowing an HMI to initiate multiple and potentially extended operations (e.g., instantiation of applications) such that SDR processing occurs in receive sequence (i.e., eliminates operator waiting between command initiation). Multiply indexed MIB tables can be introduced to add efficiency and extensibility to MIB structures (e.g., directory structure with multiple routing entries and associated attributes for address, subnet, priority, etc.). Finally, "collection" objects can be introduced to aggregate multiple SNMP "set" and "get" operations [7].

5. THIRD PARTY CONTROL OF AN SDR VIA SNMP

One of the advantages SNMP affords is the introduction of auxiliary controllers to the standard HMI interfaces. Such controllers may facilitate coordination within distributed environments that include legacy ancillary devices requiring interfaces into an SDR. The Remote Control Processor (RCP) in **Figure 4** is an example of third party control for the DMR Information Transfer Unit (ITU) (i.e., radio platform). Control and status

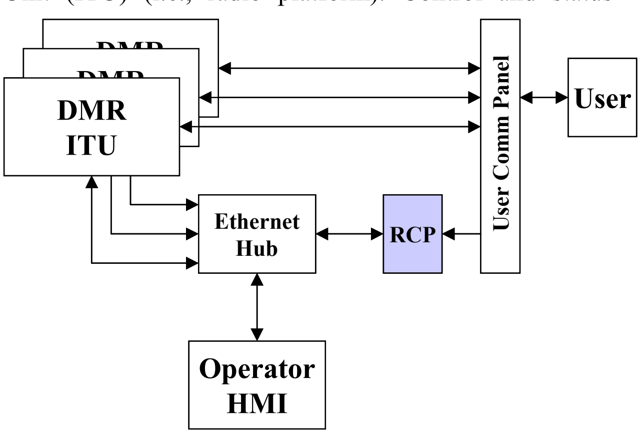

Figure 4. SNMP allows the Navy's RCP to serve as a secondary control source for the DMR

access to a DMR is possible from either an RCP or HMI through a standard Ethernet hub. The RCP serves as an intelligent communication device for translating controls from the Navy's integrated shipboard switching system into SNMP commands. Navy SPAWAR is developing the RCP with support from General Dynamics Decision Systems. The SNMP interface allows communications users to configure attributes of a waveform without direct operator interaction. The RCP converts user settings from a communications panel into SNMP requests for control and status. Through the use of SNMP, the RCP has the capability of commanding a subset of the operations possible from the DMR HMI (e.g., setting radio frequencies).

6. SUMMARY

SNMP offers benefits for SDR external control and management that exceed alternative approaches using CMIP or direct CORBA access. Real-Time performance in an SDR can be maintained by use of a CORBA gateway that decouples HMI control from radio data traffic. The Navy's Digital Modular Radio demonstrates viability of SNMP within an SDR while serving as an example for the adaptations necessary to succeed. SNMP opens the door for use of third party controllers and offers a significant pool of COTS SNMP analysis tools.

7. REFERENCES

[1] L. Deri, B. Ban, "Static vs. Dynamic CMIP/SNMP Network Management Using CORBA," Fourth International Conference on Intelligence and Services in Networks, Cernobbio, Italy, pp. 329-338, May 27-29, 1997.

[2] T. Vallillee, "SNMP & CMIP: An Introduction To Network Management", [online], 1996 <URL: http://www.geocities.com/SiliconValley/Horizon/4519/snmp.html>.

[3] Modular Software-programmable Radio Consortium, *Software Communications Architecture (SCA) Specification*, Version 2.2, Joint Tactical Radio System (JTRS) Joint Program Office, November 17, 2001

[4] Object Management Group, The Common Object Request Broker: Architecture and Specification, Revision 2.4.2, February 2001.

[5] J. Reed, *Software Radio: A Modern Approach to Radio Engineering*, Prentice Hall PTR, 2002.

[6] D. Perkins, *Understanding SNMP MIBs* (ISBN 0-13-437708-7), Prentice-Hall PTR, 1997.

[7] Atos, "CORBA/SNMP Gateway", [online], January 1999 <URL: http://www.si.fr.atosorigin.com/sophia/download/DS_GW1.pdf>.