

Il protocollo SNMP per il Fault Detection dei trasmettitori DVB-T

ing. Silvestro Terranova¹,
ing. Francesco Maria Raimondi²,
prof. Giansalvo Cirrincione³,
ing. Danilo Pellegrino⁴

1. Generalità

Fin dall'inizio delle trasmissioni la Rai è stata concessionaria del servizio radiotelevisivo pubblico, questa concessione viene rinnovata periodicamente con un contratto di servizio. L'articolo 22 del contratto di servizio recita:

“La RAI procede a dotare le proprie reti di tutti i mezzi atti alla telesorveglianza e al telecontrollo necessari al loro buon funzionamento” [1].

Il telecontrollo degli impianti è quindi un elemento vincolante per lo *status* di servizio pubblico ma “diventa sempre di più una necessità indispensabile per una emittente radiofonica o televisiva: conoscere a distanza lo stato di efficienza dei propri impianti di diffusione, in tempo reale, ma senza muovere uomini e macchine, è diventato ormai essenziale per “certificare” la propria affidabilità nella gestione di una rete di trasmissione” [2].

L'esercizio di una rete di diffusione comprende un insieme di attività molto diversificate: in prima analisi vi si possono convenzionalmente distinguere la

L'articolo sintetizza la tesi di laurea di Silvestro Terranova “Applicativo per l'integrazione del Fault Detection di nodi SNMP nel sistema di telecontrollo dei centri trasmettenti di Rai Way”

– Università di Palermo – Facoltà di Ingegneria – Corso di Laurea in Ingegneria Informatica – A.A. 2003-2004.

¹ Rai Way – Gestione Reti – Bologna

² Relatore - Università di Palermo – Dipartimento di Ingegneria dell'Automazione e dei sistemi.

³ Correlatore - Università di Palermo – Dipartimento di Ingegneria dell'Automazione e dei sistemi.

⁴ Tutor Aziendale - Rai Way – Ingegneria - Roma

Sommario

Le specifiche per il controllo delle stazioni trasmettenti della Rai sono state scritte nel 1985. In queste specifiche è descritta la struttura di una stazione trasmittente e per ciascuna sezione vengono elencati i comandi, i segnali e gli allarmi necessari per il telecontrollo. I primi sistemi di telecontrollo si basavano su tecnologie analogiche, i segnali e i comandi erano di tipo ON/OFF. Lo sviluppo delle tecnologie digitali e delle comunicazioni, l'uso sempre più diffuso di sistemi a microprocessore e l'introduzione di nuovi protocolli di gestione ha consentito l'integrazione dei primi sistemi di telecontrollo in un unico sistema SCADA (il SITT) e ha semplificato il fault detection dei nuovi trasmettitori dedicati al digitale terrestre attraverso il protocollo SNMP.

“conduzione” e la “manutenzione” degli impianti; poiché questi ultimi sono di regola realizzati in modo da garantire un funzionamento automatico, la conduzione consiste soprattutto nel verificare il buon funzionamento degli impianti e nell'impartire opportuni comandi affinché essi svolgano correttamente il prescritto servizio [3].

Le specifiche per il telecontrollo degli impianti trasmettenti sono state redatte nel 1985 da un apposito gruppo di lavoro. In questo documento viene illustrata la sistemistica delle varie sezioni di una stazione trasmettente. Per ciascuna tipologia di sistema e per ciascuna sezione d'impianto vengono elencati dettagliatamente i comandi locali e distanti, i segnali locali e distanti e gli allarmi con cui si può controllare l'impianto.

All'inizio il telecontrollo degli impianti di trasmissione è stato pensato a livello locale: gli impianti di ciascuna regione erano controllati dai tecnici e da uno o due centri controllanti presidiati situati nella stessa regione o nelle regioni limitrofe.

I comandi dal centro di controllo verso i centri trasmettenti e i segnali dai centri trasmettenti ai centri di controllo viaggiano su canali telefonici in banda fonica. La visualizzazione dei segnali e degli allarmi ha progredito nel tempo, dapprima venivano visualizzati attraverso tessere luminose, poi attraverso messaggi testuali su monitor e schemi grafici realizzati con caratteri ASCII fino ad arrivare alle interfacce grafiche gestibili attraverso un comune browser web.

Nel sistema Microstudi, ad esempio, un centro controllante può gestire al massimo 10 stazioni controllate e ciascuna stazione controllata può essere gestita al massimo da tre centri controllanti.

2. Il SITT Rai Way

Alla fine degli anni 90 è iniziata la fase di digitalizzazione dei collegamenti in ponte radio utilizzando il protocollo SDH dovuto anche al fatto che la legge imponeva lo spegnimento di molti fasci analogici per liberare le frequenze a favore della telefonia mobile. Questo comportava una diminuzione della capacità trasmissiva analogica per i canali telefonici.

Ci si è trovati quindi nella necessità di dovere convogliare tutte le informazioni provenienti dai centri TX in un unico centro di controllo (Centro Nazionale di Controllo Reti di Diffusione, CNCRD) utilizzando dei flussi digitali messi a disposizione dal sistema SDH e abbandonando la trasmissione attraverso i canali telefonici analogici, considerando anche che i sistemi di telesorveglianza installati nei diversi centri TX sono diversi ed utilizzano quindi diversi protocolli di comunicazione; il sistema Microstudi è solo uno dei diversi sistemi installati nel corso degli anni, infatti sui

Fig.1 - Foto del Centro di Controllo Reti di diffusione di Milano.



centri Rai Way sono installati anche sistemi Algorab, Sarte, Cet, ecc.

Sulla base delle precedenti considerazioni nasce il Sistema Integrato Telesorveglianza Territoriale.

3. Struttura hardware

Tutti i centri trasmettenti dislocati sul territorio sono collegati attraverso una rete IP dedicata integrando i sistemi di telesorveglianza già esistenti.

Nell'ambito di ciascuna stazione esiste una rete LAN. L'inserimento in LAN dei concentratori base avviene attraverso un'unità di interfaccia RTU (Remote Terminal Unit) realizzata dalla STAER di Roma. Questa unità si interfaccia con la porta seriale presente sul concentratore base del vecchio sistema di telesorveglianza. Ad ogni RTU, e quindi ad ogni centro, viene assegnato un indirizzo IP. Un router collegato a dei mux link permette l'inserimento in rete, attraverso un flusso a 2 Mbit/s, inserito nella rete SDH tramite un'interfaccia standard (figura 2).

Dalla figura si vede anche la possibilità di un collegamento ISDN che il router attiva in caso di interruzione dei flussi a 2 Mbit/s. Su qualche centro è presente anche un PC con il quale è possibile accedere alla rete.

I centri dislocati sul territorio sono suddivisi in tre zone: Nord, Centro e Sud. Ogni zona fa capo ad un server in configurazione Cluster, ossia due computer funzionano contemporaneamente, in caso di guasto o di manutenzione di uno, il controllo passa immediatamente all'altro.

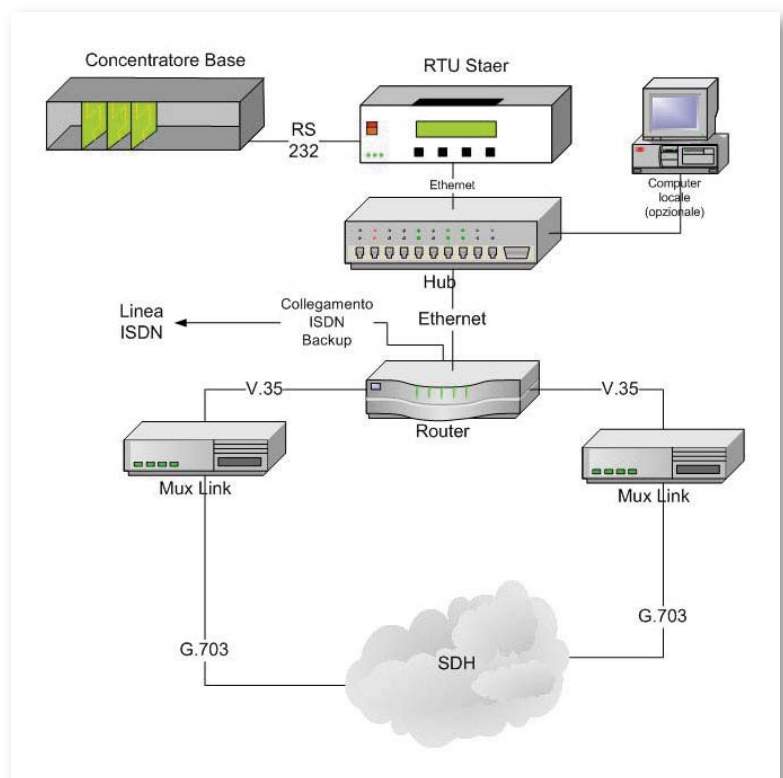


Fig. 2 - Schema dell'inserimento in LAN del sistema di telesorveglianza.

4. Struttura software

In figura 3, è riportata la struttura software del SITT [4].

La filosofia seguita nel realizzare il software è:

- Software ad architettura Modulare;
- Informazioni in formato unificato;
- Interfaccia WEB (accesso con un browser standard);
- Funzioni di security:
 - o Login e password associate a ciascun operatore;
 - o Viste differenziate per operatori con funzionalità diverse.

Il software ha un'architettura modulare di tipo client-server.

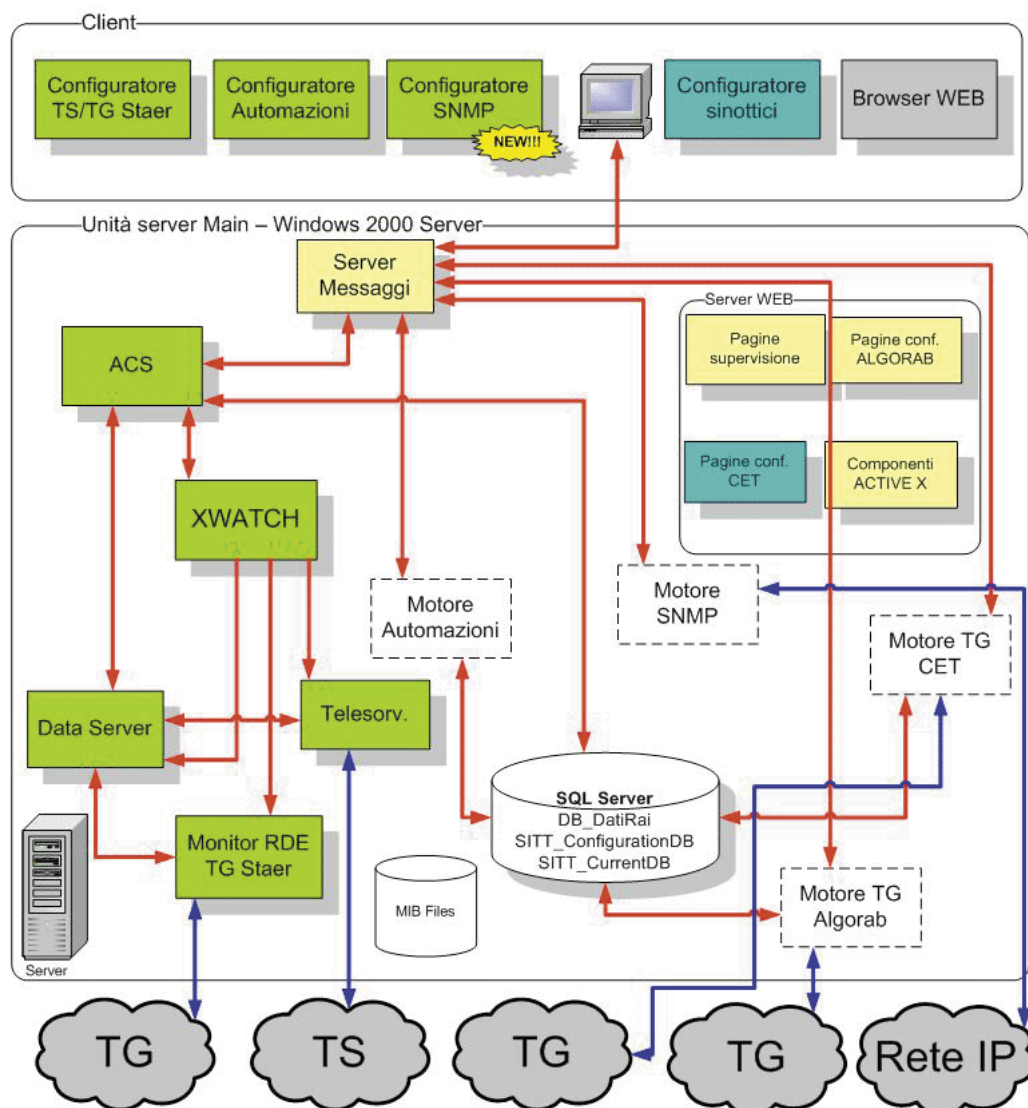
Nota 1 -
Interrogazione
ciclica dei
dispositivi.

Su ciascun server è installato il sistema operativo Microsoft Windows 2000 Server e su di esso girano i *driver* o *motori*, che in figura 3 sono indicati con un rettangolo bianco, cioè i programmi che gestiscono la comunicazione con i dispositivi di campo (RTU) e scrivono i dati ricevuti sulla base dati di processo. Il driver interroga periodicamente tutti i centri TX (*polling*^{Nota 1}) e registra sul database i dati ricevuti. Esiste un motore per ciascun tipo di sistema di telesorveglianza e i singoli motori sono stati sviluppati da ditte diverse.

5. Naming Convention del SITT Rai Way

I motori che eseguono il *polling* sono stati realizzati da ditte diverse e ciascuno di essi può utilizzare per il suo funzionamento delle tabelle di un database residente sul server. In fase di progettazione si è però posto il vincolo di rispettare una *name convention*, i singoli punti (telesegnali) vengono cioè individuati univocamente scorrendo un albero, così come schematizzato in figura 4.

Fig. 3 - Struttura software del SITT.



Come si vede dalla figura, l'ultimo livello dell'albero è costituito dai punti che possono essere suddivisi in telesegnali, telecomandi e telemisure. I telesegnali e i telecomandi sono associati a punti di tipo ON/OFF, fisicamente costituiti da contatti elettrici mentre le telemisure sono dei valori numerici ottenuti da una conversione analogico/digitale.

Ogni punto può prevedere più stati (tipicamente 2 ON e OFF) e a ciascuno di questi può essere associata una diversa severità. La severità indica la gravità del verificarsi dell'evento e va da *clear* a *critical*.

6. Il protocollo SNMP

La tecnologia Simple Network Management Protocol [5] nasce come evoluzione di SGMP^{Nota 2} (Simple Gateway Monitoring

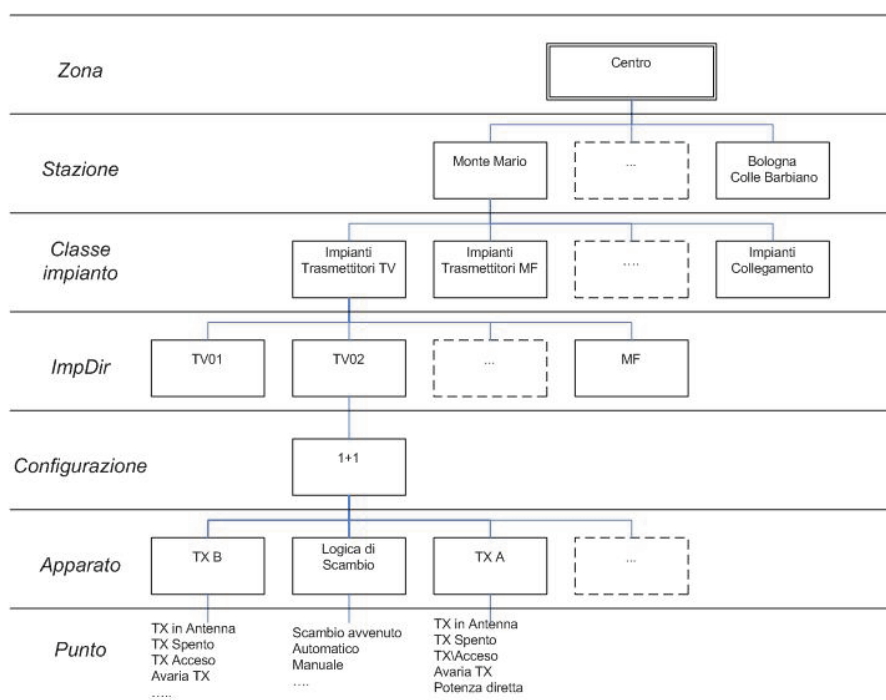
Protocol). Dal '90 ad oggi l'evoluzione di SNMP non si è mai fermata: dal 1993 al 1996 l'IETF è stata impegnata nei draft di SNMP versione 2 (SNMPv2) e nel Gennaio '98 viene pubblicato il primo RFC [6] per SNMP versione 3 (SNMPv3). Nel Marzo 2002 l'IETF ha approvato come standard SNMPv3.

SNMP si basa su una semplice architettura "manager-agent". Ogni nodo della rete (host, bridge, router,...) può contenere un software dedicato al network management denominato agent. Tale agent svolge i seguenti compiti:

- accede ai parametri relativi allo stato del dispositivo;
- tiene traccia della configurazione del dispositivo;
- rivela malfunzionamenti del dispositivo o azioni significative che lo interessano, ad esempio il login di un utente, segna-

Nota 2 - protocollo progettato nel 1987 per la gestione dei router che costituiscono il backbone di Internet.

Fig. 4 - Struttura dell'albero della naming convention.



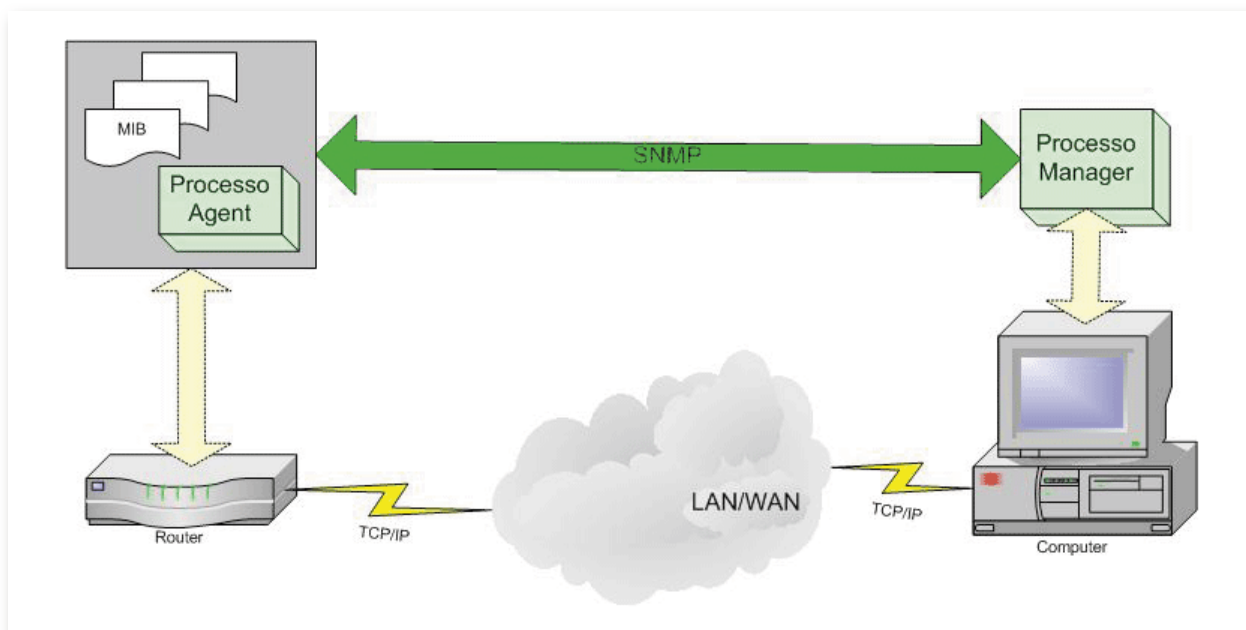


Fig. 5 - Architettura del sistema di gestione SNMP.

landoli alla stazione di gestione tramite l'invio di eventi (chiamati *trap*);

- risponde ai comandi inviati dalla stazione di gestione.

Ogni agent, quindi, si occupa del mantenimento delle informazioni relative all'oggetto gestito che possono essere utili nelle attività di gestione. Queste informazioni costituiscono un database chiamato *Management Information Base* (MIB). È interessante notare che le informazioni utilizzate dalla stazione di gestione sono memorizzate all'interno dei MIB di tutti i dispositivi gestiti, che costituiscono, quindi, un database distribuito.

In figura 5 viene visualizzata l'architettura di un sistema di gestione SNMP.

I principali standard specificati nell'ambito della gestione SNMP sono:

1. **SMI** (*Structure of Management Information*). Definisce le modalità con cui le informazioni di gestione sono strutturate

internamente;

2. **MIB** (*Management Information Base*).

Definisce un'organizzazione gerarchica per le informazioni di gestione. I MIB sono costituiti dai managed objects e sono identificati dagli object identifiers. Un managed object (che a volte è chiamato MIB object o object o anche MIB) è una delle tante caratteristiche di una risorsa monitorata (managed device). L'object ID (OID) identifica univocamente un managed object nella gerarchia MIB. Una gerarchia MIB può essere rappresentata come un albero la cui radice è un nodo senza nome e in cui ogni livello è assegnato ad una diversa organizzazione. La figura 6 illustra un MIB-tree. Gli object ID nei livelli più alti del MIB-tree appartengono a diverse organizzazioni degli standard (CCITT, ora ITU-T; ISO; ISO e CCITT insieme). I livelli inferiori sono assegnati ad associazioni affiliate con le organizzazioni di livello superiore. Le aziende

possono definire rami privati del MIB-tree in modo da includere gli object ID dei loro prodotti. I MIB che non sono stati standardizzati vengono collocati, tipicamente, nel ramo experimental. Gli object possono essere referenziati univocamente dal loro object name o, in modo equivalente, dall'object descriptor: una sequenza di numeri che permette di esplorare l'albero fino all'oggetto richiesto. Ad esempio, l'object atInput può essere individuato dal suo *object name*:

*iso.identifiedorganization.dod.internet.
private.enterprise.cisco.temporary.variables.AppleTalk.atInput*

o dall'object descriptor:

1.3.6.1.4.1.9.3.3.1.

3. **SNMP**. È il protocollo di comunicazione vero e proprio (e dà il nome a tutto il modello di gestione). Il protocollo è estremamente semplice ed è costituito da solo 4 operazioni:

1. **Get**: viene usato dal *Network Management System* (NMS) per leggere da un agent il valore di una o più istanze di un object;
2. **GetNext**: viene usato dal NMS per leggere il valore successivo da una lista o da una tabella di valori di un agent;
3. **Set**: assegna un valore ad un object;
4. **Trap**: viene usata dall'agent per informare l'NMS di un evento significativo. È l'unica operazione definita nel protocollo di comunicazione che parte dall'agent per arrivare all'NMS (e non viceversa).

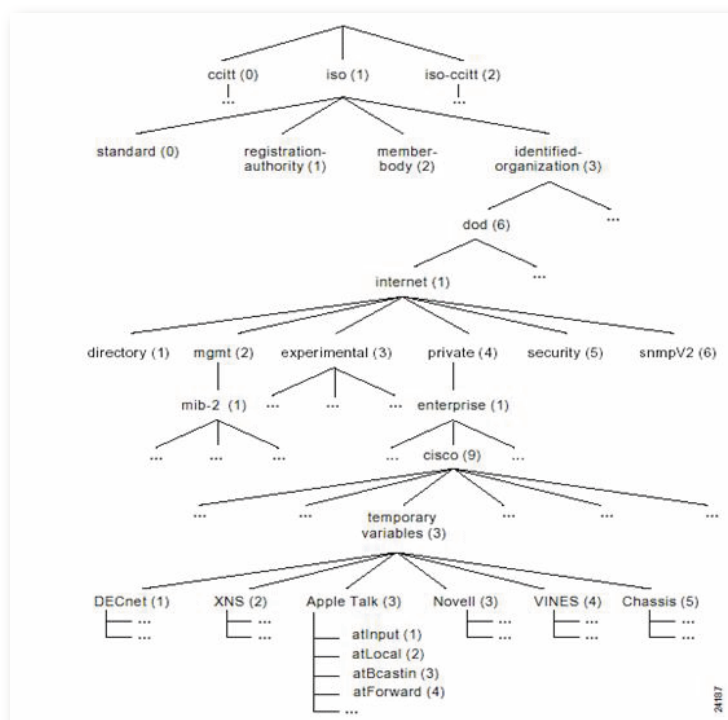


Fig. 6 - Un esempio di MIB-tree.

In SNMPv2 sono state introdotte 2 nuove istruzioni:

5. **GetBulk**: usato dall'NMS per recuperare grandi quantità di dati, come ad esempio più righe di una tabella, contemporaneamente;
6. **Inform**: permette ad un NMS di inviare una *Trap* ad un altro NMS e di ricevere una risposta. Di fatto implementa un modello gerarchico anche fra gli NMS.

Il vantaggio di questo approccio alla gestione risiede chiaramente nella sua estrema semplicità architetturale, fattore questo che ha contribuito ad una sua ampia diffusione.

Ciò nonostante la tecnologia SNMP ha delle limitazioni. È opportuno, infatti, notare che:

- gli agent non sono in grado di svolgere operazioni complesse sui dati, ad esempio la correlazione: tali operazioni vengono demandate alla stazione di gestione;
- le modalità di organizzazione dei dati all'interno degli agent sono staticamente definite e cioè non possono subire variazioni durante la vita dell'agent stesso;
- SNMP si basa sul protocollo UDP. Questo protocollo non garantisce la consegna dei dati a destinazione. Conseguentemente, sia l'invio degli eventi da parte degli agent che dei comandi da parte della stazione di gestione risulta non affidabile.
- SNMP utilizza un meccanismo di sicurezza troppo semplice e poco sicuro.

Per incrementare il meccanismo di sicurezza è stato introdotto SNMPv3

7. Esempio di definizione di un OID

Riportiamo un esempio di definizione di un OID tratto dalla MIB di un trasmettitore del DVB-T costruito dalla Rodhe & Schwarz.

```
rfOn
OBJECT-TYPE
    SYNTAX INTEGER { true(1), false(2) }
    ACCESS read-only
    STATUS mandatory
    DESCRIPTION
        "RF present/on
        (Bit 4 of CCU state register)
        true(1) --> RF present ( RF level > RF
        fault level)
        false(2) --> RF not present ( RF level < RF
        fault level)
        Example: RF fault level    = -3.0dB
        RF level = -3.5dB          ===> RF not present "
 ::= { statusTx 4 }
```

Questa parte definisce un tipo enumerativo o multi stato, l'OID di questo tipo restituisce un valore intero associato ad un particolare significato, ad esempio se viene restituito il valore 1 (true) allora all'uscita del trasmettitore è presente il segnale, se il valore è 2 (false) allora il segnale in uscita è inferiore alla soglia di allarme impostata.

8. Il controllo dei trasmettitori DVB-T

Dal 1 gennaio 2004 sono iniziate le trasmissioni televisive di digitale terrestre. I trasmettitori dedicati a questo servizio utilizzano le più moderne tecnologie per il loro funzionamento. Per il controllo dei segnali trasmessi e del funzionamento del trasmettitore vengono utilizzati apparati a microprocessore (figura 7). Questi apparati sono dotati anche di una interfaccia LAN grazie alla quale possono essere inseriti in rete ed avere assegnato un indirizzo IP. Questo permette di gestire questi apparati sia attraverso pagine Web (sono dotati di un web server), sia attraverso il protocollo SNMP.

La gestione via web, benché già pronta, non si può utilizzare per il monitoraggio continuo da un centro di controllo, ci vorrebbe infatti un operatore che ciclicamente andasse a consultare i singoli trasmettitori controllandone lo stato.

Per il controllo, quindi, è più indicato il protocollo SNMP. L'interrogazione ciclica viene effettuata da un nuovo motore. D'ora in poi indicheremo con *nodo SNMP* qualsiasi dispositivo inserito nella LAN che sia gestibile con il protocollo SNMP. Ogni nodo SNMP è fornito con un file di testo che ne descrive la MIB.



Fig. 7 - Foto della logica di controllo del trasmettitore DVB-T denominata NETCCU.

La struttura del SITT all'interno di in centro trasmettente diventa quindi quella di figura 8.

Oltre al motore SNMP è stato necessario realizzare anche il relativo configuratore.

9. Inserimento dei nodi SNMP nel SITT

Come si è visto nei paragrafi precedenti sia la *naming convention* che l'SNMP sono delle strutture ad albero.

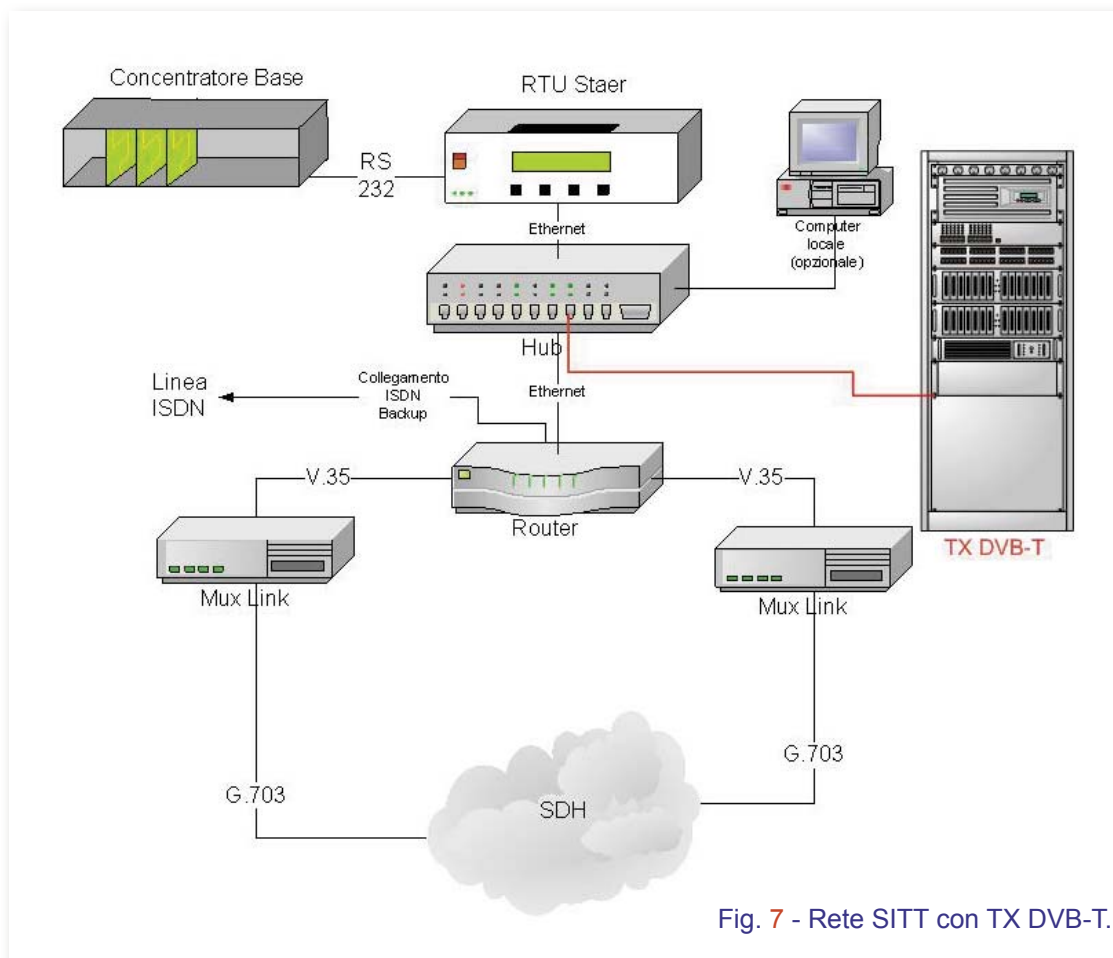


Fig. 7 - Rete SITT con TX DVB-T.

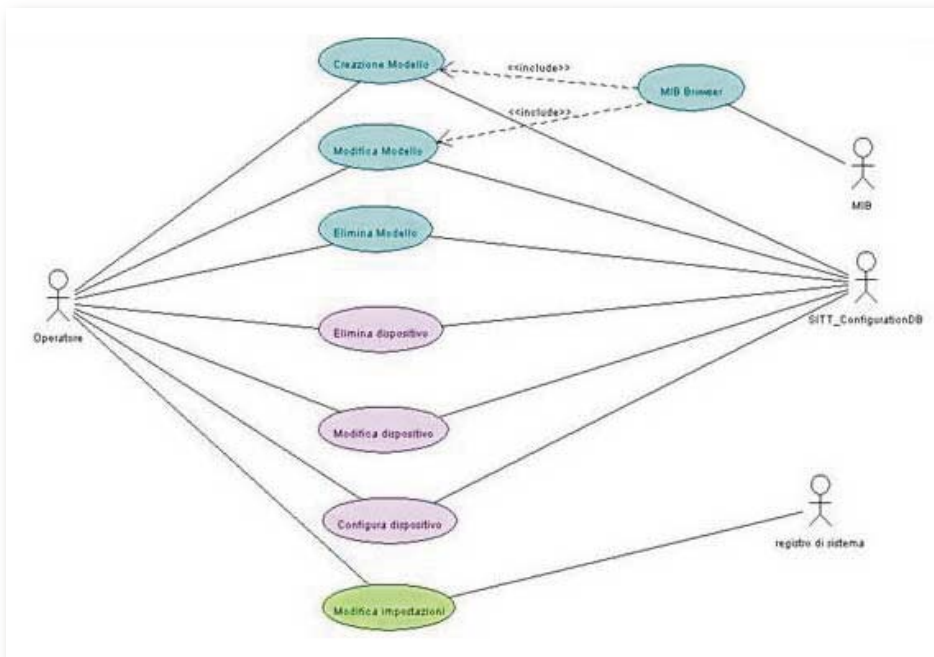
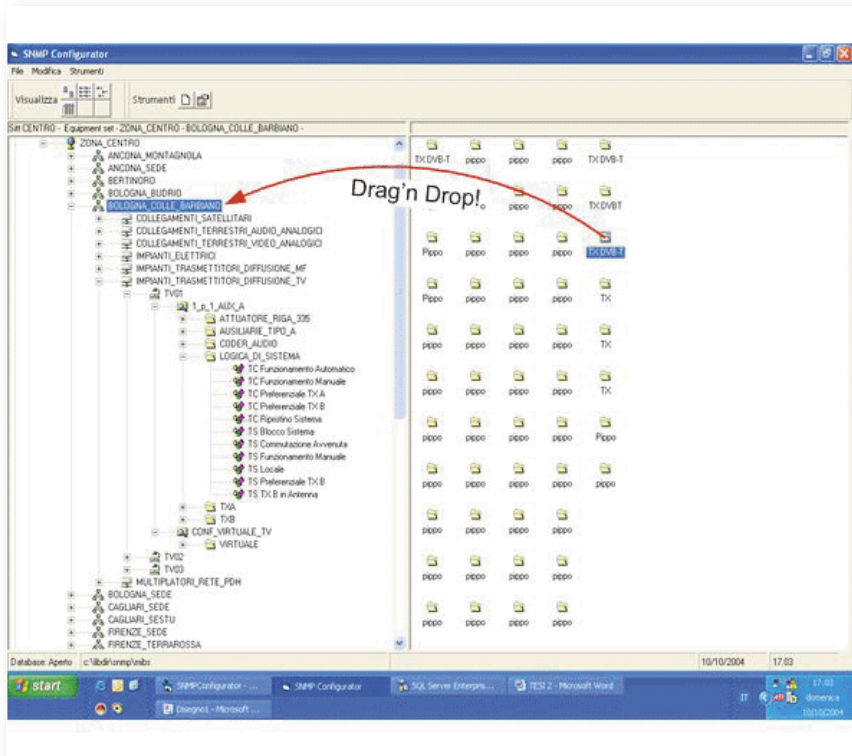


Fig. 9 - Diagramma Use-Case del configuratore SNMP.

Fig.10 - Interfaccia del configuratore SNMP.



Il problema che si pone nell'inserire i nodi SNMP in un sistema di controllo come il SITT, è quello di riuscire ad associare degli OID che possono restituire valori di tipo diverso (stringhe, interi, reali, ecc.), in un sistema che utilizza solo tipi di dato digitali (on/off) o analogici.

Per ciò che riguarda i dati interi o reali tipicamente utilizzati per le telemisure, non ci sono particolari problemi; una soluzione va invece cercata per quegli OID di tipo enumerativo, cioè quelli che restituiscono più valori interi, ciascuno associato ad un particolare significato.

La soluzione trovata consiste nell'utilizzare la possibilità di poter associare a ciascun punto della *naming convention* più valori, ciascuno con una diversa severità. In questo modo si ottiene una corrispondenza tra OID e punti e si utilizzano i valori enumerativi associandoli ad una diversa *severità*. Ad esempio, consideriamo un punto denominato “Bassa RF TX” ed associamolo all’OID “RfOn” visto nel paragrafo precedente; ai valori restituiti si assegneranno due differenti livelli di severità e precisamente al valore 1 (presenza RF) si assocerà la severità “Clear” e al valore 2 (RF < RF Fault) si assocerà la severità “Critical”.

10. Il configuratore SNMP

Per potere inserire nel SITT i nodi di rete SNMP è stato necessario realizzare un software ad hoc, chiamato configuratore SNMP.

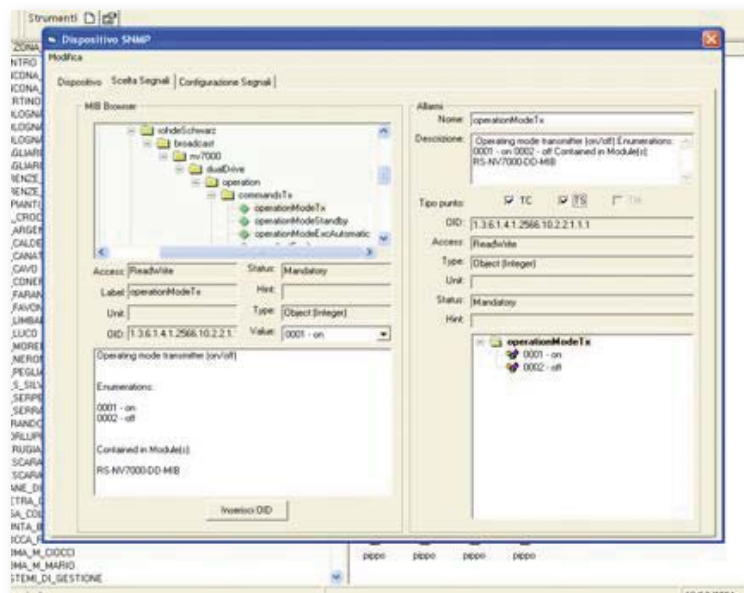
Il configuratore è un'applicazione che gira sui PC client e in pratica è un'interfaccia tra l'operatore e due database: quello del SITT e quello dei file MIB contenenti tutti gli OID e situati in una directory predefinita sul server.

L'interfaccia che si presenta all'operatore (figura 10) è composta da un lato dall'albero della *naming convention* e dall'altro dalle icone relative ai modelli dei nodi SNMP.

Per effettuare la configurazione^{Nota 3} di un nodo di rete SNMP l'operatore quindi deve prima crearne un modello inserendo i dati del dispositivo e selezionando gli OID (figura 11) che devono essere controllati. In questa fase è possibile effettuare l'associazione tra OID e punti della *naming convention* (figura 12).

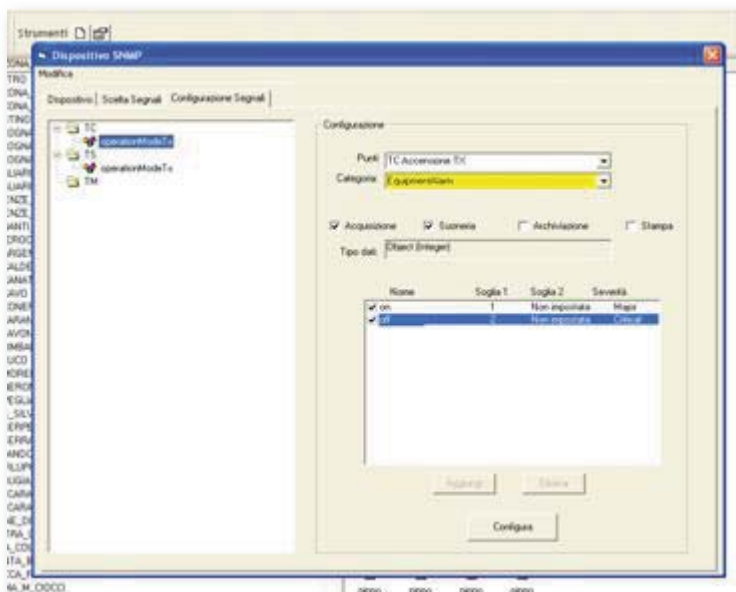
Se il modello è stato creato, l'operatore con una semplice operazione di *drag and drop*, trascina l'icona del modello di nodo SNMP su un nodo dell'albero della *naming convention*, quindi inserisce i parametri specifici del nodo come l'indirizzo IP, l'indirizzo SITT, il tempo di polling, ...; se necessario può modificare i parametri di gestione degli allarmi (severità, suoneria, archiviazione, stampa, ...) e quindi inserire il nodo nel SITT.

Fig.11 - Interfaccia del configuratore SNMP per la selezione degli OID.



Nota 3 - Con il termine *configurazione* si intende l'inserimento di un nodo SNMP nel SITT.

Fig.12 - Interfaccia per l'associazione tra OID e punti della naming convention.



11. Conclusioni

Le tecnologie che hanno permesso la diffusione di internet hanno semplificato notevolmente il telecontrollo degli impianti e sicuramente il rinnovo degli apparati di trasmissione lo semplificherà ulteriormente: i fasci di cavi per i telesegnali e i telecomandi paralleli verranno sostituiti da un cavo ethernet. La velocità delle comunicazioni permetterà inoltre un controllo delle caratteristiche degli apparati sempre più accurato e quindi maggiore velocità di intervento da parte dei tecnici di manutenzione, che comunque rimarranno sempre l'elemento fondamentale per la conduzione di un impianto di trasmissione.

Bibliografia

1. Contratto di servizio tra il Ministero delle comunicazioni e la RAI - Radiotelevisione Italiana S.p.A. - 23 gennaio 2003.
2. Roberto Anzelmo: "RADIOMONITORING E TELEMETRIA - Le due facce del controllo a distanza", Broadcast and Production - Maggio 2000,
3. Specifiche dei comandi e segnali per la conduzione delle stazioni" – Gruppo di lavoro per la "definizione delle specifiche di controllo delle stazioni" - Rai Radiotelevisione Italiana - Supporto Tecnico - 26/6/1985.
4. Tratta dalla presentazione STAER del SITT.
5. J. Case, M. Fedor, M. Schoffstall, J. Davin. "A Simple Network Management Protocol" (SNMP). RFC 1157 (1990).
6. D. Levi, P. Meyer, B. Steward. "SNMPv3 Applications". RFC 2263 (1998).