UNIVERSITÀ DEGLI STUDI DI CAMERINO

FACOLTÀ DI SCIENZE E TECNOLOGIE

Corso di Laurea in Informatica classe 26

Economia Digitale

Dipartimento di Matematica e Informatica

DEFINIZIONE DI POLITICHE DI MONITORAGGIO DEL SISTEMA HP OPENVIEW NNM APPLICATO AD UN SISTEMA DI RETE COMPLESSO

Tesi di Laurea compilativa
In
Politiche di Rete e Sicurezza

Laureando

Marco Francioni

Relatore

Dott. Fausto Marcantoni

Correlatore

Dott.ssa Maria Laura Maggiulli

ANNO ACCADEMICO 2005 / 2006

INDICE GENERALE

INDICE DELLE FIGURE

INTRODUZIONE

Nell'ultimo decennio si è assistito ad un grande sviluppo delle tecnologie legate agli elaboratori e alla loro interconnessione. È proprio quest'ultimo aspetto che ha assunto particolare risalto grazie anche alla diffusione di Internet.

Tale diffusione massiccia dei calcolatori ha aperto nuovi scenari riguardo l'utilizzo e l'implementazione di nuove tecnologie.

Se si pensa ad Internet e alla sua struttura ci si può rendere conto della mole di informazioni che viaggiano ogni giorno sui mezzi di trasmissione ad esso connessi.

Questo sviluppo è stato incentivato anche dall'aumento della velocità di trasmissione dei dati, dalla maggior velocità di elaborazione e dalla minor incidenza sui costi di acquisto.

Infatti, la produzione in scala di quantitativi rilevanti di beni porta ad una riduzione dei costi di produzione e se non si è in presenza di un regime monopolistico[1], si riflettono su minori costi all'atto dell'acquisto.

Con queste premesse il computer si è evoluto da mero strumento per l'elaborazione in locale a strumento facente parte di una grande rete mondiale interconnessa, Internet.

Si precisa che lo sviluppo delle reti porta con sé un inevitabile incremento delle loro dimensioni; il concetto di rete, che una volta era legato soprattutto ad ambiti aziendali o aree locali, si estende ricoprendo intere aree geografiche.

1 mercato in cui c'è un unico grande produttore

Quest'accrescimento in dimensione e numero delle reti può creare ad amministratori di rete notevoli problemi di gestione e manutenzione della network stessa.
Gli amministratori non possono raggiungere fisicamente tutti i nodi, anche quelli più lontani, così vengono in loro aiuto i software creati appositamente per facilitare il monitoraggio[2] e la gestione in remoto dei vari nodi della rete.
Detto questo, possiamo introdurre il concetto di Network Management, ovvero un'infrastruttura di gestione della rete, locale o geografica, che permette all'amministratore di tenere sotto controllo la rete stessa, i sistemi che ne fanno parte, le applicazioni e i dispositivi di rete.
Tale attività di "monitoring" e "managing", viene effettuata da una stazione centrale di monitoraggio, detta "Network Management Station [3]".

Naturalmente per implementare queste attività, bisogna avvalersi di particolari protocolli creati appositamente per soddisfare tali esigenze.
Il protocollo Simple Network Management Protocol, il cui acronimo è SNMP[1], è un protocollo nato nel 1989 che ha lo scopo di mettere in comunicazione e scambiare i dati fra la NMS e i vari nodi della rete. È un protocollo che è stato sviluppato anche in altre due versioni più recenti, ma comunque la versione originale rimane la più utilizzata. Tale protocollo è il fulcro delle attività di gestione di rete via software. Bisogna ricordare che lo standard SNMP è supportato da una grandissima quantità di dispositivi, alcuni dei quali esulano dalla categoria dei componenti di rete, come ad esempio alcune stampanti. Non bisogna comunque dimenticare che viene utilizzato e quindi sponsorizzato da aziende come HP e IBM che vendono i due software commerciali più diffusi; rispettivamente OpenView Network Node Manager e NetView.

2 è l'attività di acquisizione di dati relativamente ad una rete o parte di essa
3 da ora in poi NMS

L’obiettivo di questa tesi è quello di analizzare il funzionamento dell'applicativo OpenView Network Node Manager e mostrare alcune configurazioni che possono aiutare ogni amministratore di rete nella personalizzazione di tale software in funzione della tipologia di rete da gestire. Questo ha il fine di personalizzare le politiche di monitoraggio della rete.

Come premessa, per comprendere meglio il funzionamento di tali software, nel primo capitolo verrà trattato il concetto di Network Management corredato da alcuni esempi chiarificatori; a riguardo verrà anche illustrato lo standard di riferimento ISO per il Network Management.

Nel secondo capitolo si parlerà dei Principali protocolli di rete utilizzati dal software di gestione preso in esame e del loro funzionamento, incentrandosi maggiormente sul protocollo SNMP.

Il terzo ed ultimo capitolo riguarderà l’introduzione ed utilizzo del software Network Node Manager, i passi principali per raggiungere una sua corretta configurazione e l’illustrazione di politiche di rete applicate ad un sistema di reti complesso.

1 NETWORK MANAGEMENT

Come prima precisazione indichiamo la definizione corretta di Network Management:

> il processo o tecnica, effettuata in locale o in remoto, di monitoraggio o gestione delle reti

Per comprendere maggiormente ciò che di seguito viene trattato, si introducono degli esempi pratici che meglio di ogni altra cosa aiutano a farsi un'idea sul funzionamento di tale concetto.

Considerando alcuni scenari del mondo reale, non attinenti alle reti, in cui un sistema complesso ha molti componenti che interagiscono e devono essere monitorati, gestiti e controllati da un amministratore, si possono fare due esempi esplicativi:

- il pilota di un aereo può essere visto come l'amministratore di una rete complessa, e la cabina di pilotaggio come la NMS. In tale cabina sono presenti molti strumenti che permettono al pilota di controllare e comandare i componenti relativi l'aeroplano. Al variare di alcuni parametri, corrisponderà una reazione del pilota, che può essere statica (non fa nulla) o dinamica (agisce in conseguenza dei parametri letti dagli strumenti)
- nelle centrali elettriche è presente una sala di controllo dove manometri, interruttori e dispositivi luminosi monitorano a distanza lo stato (es. temperatura, pressione, ...) di tubi, valvole e altri componenti dell'impianto. Come nel precedente esempio, questi dispositivi, nel loro insieme, permettono all'operatore di monitorare i componenti principali dell'impianto e lo avvisano nel caso si incorra in guasti o quando un guasto è imminente.

L'operatore di tale impianto, visiona i dati ricevuti dai vari parametri e agisce di conseguenza.

Negli esempi appena riportati un "responsabile" effettua il monitoraggio sui dispositivi remoti e analizza i dati da loro raccolti; se i dati rientrano nei limiti consentiti non ci sarà alcuna reazione, altrimenti verranno presi dei provvedimenti riguardo i parametri che eccedono i vaolri di soglia.

Alla stessa maniera l'amministratore di una rete deve monitorare i parametri che vengono acquisti dal software apposito e reagisce al verificarsi di situazioni inattese.

Con la diffusione dei calcolatori e la loro successiva aggregazione in reti, la gestione di queste ultime non corrisponde più al semplice invio di un comando di ping[4] per vedere se un apparato è down[5] o meno; ma diventa un sistema complesso di gestione di svariate centinaia, se non migliaia, di nodi interconnessi.
Per aiutare il network administrator in questa gestione sistematica del gran numero di componenti hardware e software presenti nella rete, vengono in aiuto gli applicativi di Network Management.

Un tempo, quando ancora tali applicativi, non esistevano, ci si accorgeva del problema solo quando un utente ne subiva le conseguenze (ad es. quando un utente rientrando in ufficio la mattina trovava i computer non connessi alla rete aziendale); oggi invece si possono anche prevedere dei problemi a seconda del valore che viene assegnato a dei parametri, così da riuscire a scongiurare alcuni intoppi che altrimenti pregiudicherebbero la buona riuscita del lavoro o comunque dell'attività svolta.
Con tali software si possono risolvere infatti sia quei problemi che si sono manifestati, sia quelli che probabilmente si manifesteranno. Per capire

4 comando di echo che verifica se un dispositivo remoto è raggiungibile
5 si dice di un apparato che ha disabilitate tutte le interfacce di rete, ovvero che risulta scollegato

meglio quest'ultima affermazione può venire in aiuto la visone di una piccola rete aziendale:

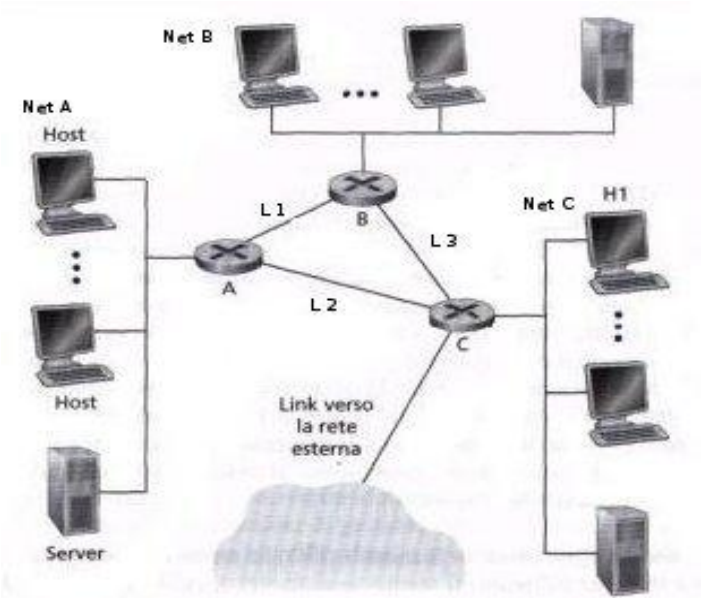

Figura 1.1 - Rete aziendale

nel caso in cui tutti i router (A, B, C) presentino delle route statiche, la rottura o disabilitazione di un link interno alla rete (L1, L2, L3) può potenzialmente escludere all'accesso esterno o interno uno o più segmenti di rete. Se per esempio si dovesse rompere il link L1 e nel router A sono impostate delle route statiche che gli indicano di passare per L1 al fine di raggiungere il router B, tali reti non potrebbero scambiarsi dati. In questo caso, vedendo che il link L1 è down, si può far passare il traffico proveniente dalla Net A e destinato alla Net B attraverso il link L2 che collega i router A e C e poi, attraverso il link L3, arrivare al router B e quindi alla Net B.

Questo è solo un banale esempio di una situazione che realmente potrebbe accadere e che se non correttamente gestita genererebbe dei seri problemi (basti pensare all'ipotesi che nella Net B ci siano tutte le stampanti; come potrebbe un utente della Net A stampare un documento senza bypassare il

problema?).

Anche in una piccola rete, come quella appena visionata, si possono trarre molti benefici, implementando un software per il suo managing e monitoring.
Alcuni vantaggi possono riguardare:

- **Rilevazione di un guasto riguardo un link della rete:** (come da esempio sopra)

- **Monitoraggio del traffico di rete:** si può monitorare il traffico della rete o magari dei link o apparati considerati cruciali in modo da cercare di garantire sempre una certa qualità del servizio (QoS). Questa modalità di impostazione può far sì che l'amministratore del sistema possa essere avvisato in automatico del superamento di un certo livello, relativo traffico, che è stato precedentemente impostato. Può anche accadere che a causa del numero sempre maggiore di nodi che si collegano ad una certa rete si debba aumentare la banda disponibile. Per questo il monitoraggio è un utile strumento anche per prendere decisioni che comportano un costo per l'azienda

- **Rilevazione di guasti ad un'interfaccia di uno switch[6] o un host[7]:** è molto utile un'informazione riguardante tale componente hardware, in quanto i dati passano necessariamente attraverso esso. Se un interfaccia di rete di un host utente si guasta, tale host non può in alcun modo connettersi alla rete senza prima sostituire tale componente. Ipotizzando la rottura di una porta di uno switch a cui è collegato un hub[8] (come spesso si fa per contenere i costi), gli utenti che fanno riferimento a tale hub non potranno connettersi alla rete. Logicamente nel caso in cui una

6 è un apparato di connessione della rete che mantiene la banda totale per ogni host
7 è una macchina collegata in rete cha ha un proprio identificativo univoco
8 è un apparato di connessione della rete. Lavora al Livello Fisico del Modello ISO/OSI

scheda di rete di un computer host sia configurata male non si può "colloquiare" con tale pc e quindi il sistema, in questo caso non sa se l'interfaccia di rete è rotta o meno, ma ci dice solo che non risponde ai pacchetti di interrogazione inviati. Comunque se un amministratore si rende conto che, ad esempio, c'è un incremento degli errori riguardo il checksum[9] nei frame[10] che sono stati inviati attraverso l'interfaccia prossima al guasto, può intervenire tempestivamente richiedendo la sostituzione dell'interfaccia stessa

- **Rilevazione dei cambiamenti riguardo le tabelle di instradamento:** il cambiamento frequente delle entry nelle tabelle di instradamento può far presagire una rottura di qualche genere (ad es. in un router ci può essere un'interfaccia di rete che a volte non funziona correttamente) o magari si è configurato in maniera errata un router

- **Rilevazione delle intrusioni:** in alcuni casi ci si può accorgere anche di intrusioni volte magari a prelevare dati importanti dalla propria rete. Ad esempio se si vede che, attraverso il monitoraggio del traffico o attraverso il ricevimento di un messaggio innescato da una trap[11], avviene un sospetto spostamento massiccio di dati da un indirizzo interno ad uno esterno, si possono impostare delle ACL[12]

- **Monitoraggio degli SLA (Service Level Agreements):** in alcuni casi si stipulano contratti nei quali vi deve essere una soglia minima garantita di servizio. Il monitoraggio di parametri che riguardano tali livelli sono importanti, specialmente per

9 è una somma di controllo inserita alla fine dei pacchetti per controllare, una volta arrivati a destinazione, che non si ano stati modificati o alterati
10 unità di trasmissione dei dati facente riferimento al Livello Data Link Del Modello ISO/OSI
11 meccanismo di avviso automatico che si attiva al presentarsi eventi preimpostati
12 Access Control List è una lista di regole che vengono eseguite sequenzialmente

aziende che pagano un lauto compenso per avere un servizio garantito di un certo livello (es. 4 Mbps di banda garantita)

Ora si può meglio comprendere il significato di un sistema di Network Management.
Questa tipologia di sistema è strutturata come un insieme di componenti hardware e software, attraverso i quali si può monitorare e interagire con le varie risorse di rete (router, switch, server, ...).
Tale struttura permette anche delle azioni automatiche configurabili che permettono il self problem solving relativamente a degli eventi, facendo così guadagnare tempo all'amministratore che si può dedicare ad altre attività a più alto valore aggiunto (es. sviluppo della rete, analisi dell'affidabilità, ...)
Più semplicemente si può affermare che il Network Management è un servizio che implementa una serie di tools, applicazioni e dispositivi che assistono l'amministratore del sistema nel monitoraggio e gestione della sua rete, eseguendo anche in parte un lavoro che un tempo l'administrator doveva svolgere direttamente.

Andando ad analizzare gli obiettivi, si possono schematizzare nel seguente modo:

- **aumento della competitività:** per fare ciò si ha bisogno di garantire il buon funzionamento della rete massimizzando l'efficienza e la produttività
- **conservare una corretta ed accurata informazione**: riguarda la configurazione della rete e eventuali modifiche apportate al fine di non creare problemi nel caso in cui tale rete debba essere gestita, una volta configurata correttamente, da un altro administrator
- **segnalazione tempestiva:** è impostante segnalare il prima possibile l'insorgere di errori, allarmi o malfunzionamenti al gestore, al fine di provvedere quanto prima alla risoluzione del

problema, evitandone quindi l'insorgere di altri

- **riconfigurazione:** riconfigurare la rete secondo i risultati ottenuti dall'attività di monitoring, in modo da migliorare le prestazioni complessive o migliorarne la sicurezza

- **riduzione dei costi:** in questo senso va ricordato che gli apparati con il passare del tempo costano sempre meno; aumenta invece il costo del personale destinato alla gestione delle reti. Così per minimizzare i costi del personale si adopera software gestionale sempre più avanzato e in grado di svolgere automaticamente delle operazioni di routine.

Dato che le procedure per il Network Management sono complesse e data la necessità di standardizzazione delle stesse, sono state identificate, in accordo con l'ISO[13], cinque aree funzionali descritte nel prossimo paragrafo.

1.1 Standard ISO

L'*International Organizzation for Standardizzation* è un organismo internazionale per la definizione degli standard, composto da rappresentanze di organi nazionali, che produce standard industriali e commerciali a livello mondiale. Tali standard vengono poi adottati dai paesi che vi vogliono aderire.

Tale organismo internazionale, come detto sopra, ha creato un modello di gestione di rete per cercare di catalogare e collocare ogni scenario di rete possibile in uno schema più strutturato. Vengono così definite cinque aree di gestione della rete [2]:

13 International Organizzation for Standardizzation

- **Gestione delle prestazioni:** l'obiettivo della gestione delle prestazioni è di quantificare, misurare, stendere rapporti, analizzare e controllare le prestazioni di differenti componenti di rete (ad es. utilizzo, throughput, …). Questi componenti comprendono sia dispositivi singoli (ad es. link, router, host, …), sia astrazioni end-to-end come un percorso attraverso la rete. In seguito si vedrà che gli standard protocollari, come il protocollo semplice per la gestione delle reti (SNMP), hanno un ruolo centrale nella gestione delle prestazioni in Internet.

- **Gestione dei guasti:** l'obiettivo della gestione dei guasti è di registrare, rilevare e rispondere alle condizioni di guasto della rete. La linea che separa la gestione dei guasti da quella delle prestazioni è piuttosto labile. Possiamo pensare alla gestione dei guasti come all'immediato intervento su un difetto transitorio della rete (ad es. l'interruzione del servizio del link di un host o di un router), mentre la gestione delle prestazioni agisce in tempi più lunghi; questo per fornire livelli accettabili di prestazioni di fronte al variare delle richieste di traffico e all'occasionale guasto di un dispositivo di rete. Come con la gestione delle prestazioni, il protocollo SNMP ha un ruolo centrale nella gestione dei guasti.

- **Gestione della configurazione:** la gestione della configurazione permette a un responsabile di rete di monitorare i dispositivi che appartengono alla rete gestita e di effettuarne la configurazione hardware e software. Una panoramica della gestione della configurazione e dei requisiti per le reti basate su IP si può trovare nel [2].

- **Gestione della contabilità (accounting):** la gestione della contabilità permette al responsabile della rete di specificare, registrare e controllare l'accesso degli utenti e dei dispositivi alle

risorse di rete. Quote di utilizzazione, addebiti basati sull'uso e privilegi di allocazione degli accessi alle risorse rientrano tutti nella gestione della contabilità.

- **Gestione della sicurezza:** l'obiettivo della gestione della sicurezza è di controllare gli accessi alle risorse di rete in accordo ad alcune politiche ben definite. Il centro di distribuzione delle chiavi e l'autorità di certificazione appartengono alla gestione della sicurezza. Si fa uso di firewall[14] per monitorare e controllare i punti esterni di accesso a una rete.

Dopo aver fornito diverse definizioni sui vari aspetti della gestione di rete si va ad analizzare una definizione di gestione di rete, che sinteticamente può essere definita nel seguente modo:

"La gestione della rete comprende l'azionamento, l'integrazione e il coordinamento di hardware, software ed elementi umani per monitorare, verificare, sondare, configurare, analizzare, valutare e controllare la rete e le risorse degli elementi per soddisfare le prestazioni operative in tempo reale e i requisiti di QoS[15] a un costo ragionevole". [3]

1.2 Infrastrutture di rete

Nel paragrafo precedente abbiamo visto che la gestione della rete richiede la possibilità di "monitorare, verificare, sondare, configurare e controllare" hardware e software e i componenti in una rete. Poiché i dispositivi di rete sono distribuiti, questo richiederà che il responsabile della rete sia in grado

14 è un dispositivo hardware o software per limitare gli attacchi provenienti dall'esterno o interno

15 qualità del servizio

di ottenere dati da un'entità remota (ad es., a scopi di monitoraggio) e di effettuare cambiamenti all'entità remota (ad es., impostazioni) su quell'entità.

Un'analogia in chiave umana risulterà utile per comprendere l'infrastruttura necessaria per la gestione della rete.

Se si immagina di essere a capo di una vasta organizzazione che ha filiali sparse in tutto il mondo, il proprio lavoro sarà quello di assicurare che tutte le componenti della propria organizzazione operino senza difficoltà.
Come poterlo fare? Si possono raccogliere periodicamente dati dalle filiali in forma di rapporti e di varie misure quantitative di attività, produttività e budget. Occasionalmente, alcune informazioni potranno essere inviate direttamente dall'operatore di una filiale al proprio ufficio evidenziando che si è verificato un qualche problema nella filiale. I rapporti possono anche essere inviati per far notare che tutti i processi vengono eseguiti correttamente.
Analizzando poi tali rapporti si andrà a esaminare la situazione, positiva o negativa che sia e se ne trarranno le giuste conclusioni.
In caso di problemi si possono impostare due tipi di reazione:

- **intervento diretto alla risoluzione del problema:** si interviene sulla causa del problema
- **azione automatizzata in risposta all'evento scatenante:** al verificarsi di un dato evento di cui si conoscono la cause, viene attivata un'azione automatica finalizzata alla risoluzione del problema

In questo scenario è presente una struttura implicita per controllare l'organizzazione: l'amministratore, il sito remoto sotto controllo (la filiale), il proprio agente remoto (il manager della filiale), i protocolli di comunicazione (regole per trasmettere i rapporti) e i dati (il contenuto dei

rapporti e le misure quantitative di attività, produttività e budget). Come si vede, ciascuno di questi componenti nella gestione di un'organizzazione umana ha una controparte nella gestione della rete.

Identifichiamo ora tre componenti principali nell'architettura di gestione della rete [4]:

- un'entità di gestione
- i dispositivi da gestire
- un protocollo di gestione della rete

L'**entità di gestione** è un'applicazione, che tipicamente coinvolge un individuo, funzionante in una stazione centralizzata di gestione della rete nel NOC[16]. L'entità di gestione è il sito di attività per la gestione della rete; essa controlla la raccolta, l'elaborazione, l'analisi e/o l'esposizione delle informazioni di gestione. È da qui che partono le azioni per controllare il comportamento della rete, ed è qui che gli administrator della network interagiscono con i dispositivi della rete; in pratica è la NMS.

Un **dispositivo da gestire** è una parte dell'equipaggiamento di rete che risiede sulle network da gestire. Questa corrisponde alla filiale dell'analogia umana appena trattata. Un dispositivo da gestire può essere un host, un router, un bridge, ecc.
All'interno di un dispositivo da gestire ci possono essere molti oggetti da amministrare.

Questi sono parti reali di hardware all'interno del dispositivo (ad es. la scheda di interfaccia di rete) e i set di parametri di configurazione per le parti di hardware e software (ad es. un protocollo di instradamento intradominio come il RIP). Riprendendo in esame l'analogia sopra, gli

16 centro operativo di rete

oggetti da gestire possono essere equiparati agli uffici interni alla filiale. Questi oggetti hanno associate alcune informazioni che sono raccolte in una base di informazioni per la gestione, il MIB (Management Information Base) [5]. Il MIB, nell'esempio sopra, corrisponderebbe ai dati quantitativi (misure di attività, produttività e budget; quest'ultimo impostabile dalla NMS) scambiati fra la filiale e la sede. Infine, residente anch'esso in ciascun dispositivo da gestire, c'è un agente di gestione della rete (SNMP Agent), un processo funzionante nel dispositivo da gestire che comunica con l'entità di gestione, la quale compie azioni locali che corrispondono, sul tale dispositivo remoto, a comportamenti legati a detti comandi. L'agente di gestione della rete è equiparabile al manager della filiale della precedente analogia umana.

La terza parte di un'architettura è il **protocollo di gestione della rete**. Il protocollo funziona tra l'entità di gestione e i dispositivi da gestire, permettendo all'entità di gestione di chiedere lo stato ai dispositivi da gestire e indirettamente di agire su essi attraverso i suoi agenti.
Questi agenti possono usare il protocollo di gestione della rete per informare l'entità di gestione, del verificarsi di eventi eccezionali (ad es. guasti dei componenti, violazione delle soglie di prestazione, ...).
È importante notare che il protocollo di gestione della rete non gestisce la rete di per sé ma fornisce uno strumento con cui l'administrator può agire ("monitorare, provare, sondare, configurare, analizzare, valutare e controllare") sulla rete. Per capire meglio la funzione di un protocollo, si faccia riferimento al capitolo successivo.

2 PROTOCOLLI DI RETE

Generalmente possiamo definire un protocollo come un insieme di regole che definiscono il formato dei messaggi scambiati e che consente a due entità di comunicare tra di loro e di comprendere la comunicazione.
In informatica un protocollo, o meglio un protocollo di rete, racchiude delle norme che permettono a due o più entità di rete, di avviare e chiudere una connessione, di trasferire i dati da un punto ad un altro all'interno o all'esterno di una rete, di comprendere i dati che i vari nodi si interscambiano.
I protocolli collegano un client ad un server e viceversa.

Il client corrisponde alla macchina[17] che richiede la connessione, il server invece è la macchina che offre e fornisce i servizi ai richiedenti.
Questa comunicazione, come detto avviene grazie ai protocolli di rete. La connessione può iniziare in due modi:

- si scambiano pacchetti di sincronizzazione prima di spedire i dati reali; solo se il server accetta la connessione, il trasferimento dei dati può avvenire. Un esempio di questo genere è dato dall'handshaking[18] relativo al protocollo di trasporto TCP[6]
- il client inizia direttamente ad inviare i pacchetti[19] al server senza una procedura di sincronizzazione. Questo procedimento viene adottato dal protocollo di trasporto chiamato UDP[7]

La maggior parte delle applicazioni, tuttavia, ha bisogno di inviare i dati in maniera sicura e affidabile per cui l'handshaking serve proprio a questo compito. Si comprende come la connessione con TCP, ad esempio, sia più sicura ma anche più lenta perché scambia non solo dati reali, ma anche dati di servizio.

17 termine utilizzato per riferirsi ad un generico computer
18 procedimento di sincronizzazione tra client e server
19 Termine che indica l'unità di trasporto dei dati

UDP, per capire meglio, è il protocollo utilizzato per il trasporto dei dati riguardanti applicazioni in real-time (ad es. per le videoconferenze) o generalmente applicazioni che prediligono la velocità di trasmissione alla perdita di qualche pacchetto.

2.1 Elenco dei principali protocolli di rete

Vengono elencati di seguito, corredati da una breve spiegazione, i protocolli di rete maggiormente utilizzati. L'elenco dei protocolli che verrà fatto nel prossimi paragrafi non è casuale, si va infatti ad analizzare quei protocolli che vengono utilizzati dall'applicativo oggetto di questa tesi.
È necessario però illustrare anche il Modello ISO/OSI[20]. Tale modello è uno standard stabilito nel 1978 dall'ISO, che progetta una pila di protocolli in dislocati su sette livelli.
Questo modello rappresenta lo Standard per le reti di calcolatori e l'ISO avviò il progetto OSI[8], un modello standard di riferimento per l'interconnessione di sistemi aperti.

Il modello ISO/OSI è costituito da una pila (o stack) di protocolli attraverso i quali viene ridotta la complessità implementativa di un sistema di comunicazione per il networking. In particolare il modello ISO/OSI è costituito da strati (o livelli), i cosiddetti layer, che racchiudono uno o più aspetti fra loro correlati della comunicazione fra due nodi di una rete. I layers vanno dal livello fisico (quello del mezzo fisico, ossia del cavo o delle onde radio) fino al livello delle applicazioni, attraverso cui si realizza la comunicazione di alto livello.
Per meglio comprendere tali affermazioni si faccia riferimento al paragrafo seguente.

20 Open Systems Interconnection

2.1.1 *Illustrazione del Modelllo ISO/OSI*

Tale modello non è fisicamente visibile nei calcolatori, ma è solo un raggruppamento logico per meglio comprendere il funzionamento dell'architettura dei computer stessi. Tale riferimento assume la forma:

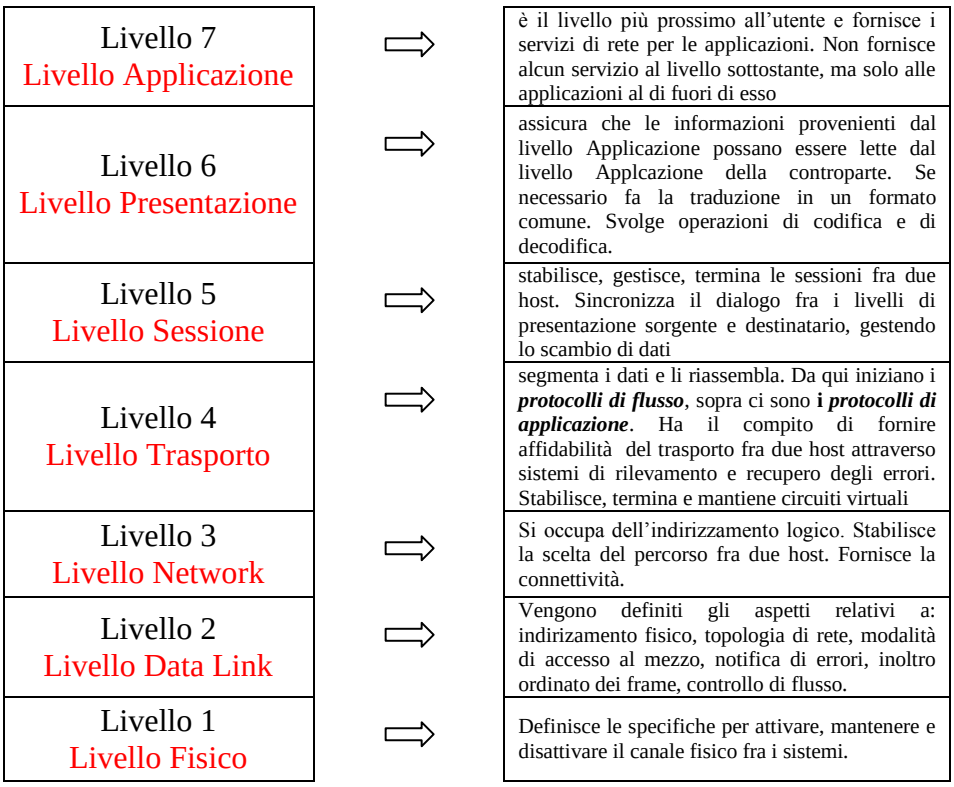

Figura 2.1 - Layer ISO/OSI

Il modello OSI definisce le funzioni di ciascun livello e il modo in cui le informazioni viaggiano su una rete; descrive anche il modo in cui le informazioni viaggiano da programmi applicativi e arrivano, attraverso un mezzo trasmissivo, agli applicativi del computer ricevente.

La suddivisione in livelli prende il nome di **suddivisione in livelli** o **layering**; ciò comporta dei vantaggi, quali:

- suddivide la comunicazione in parti più piccole e più semplici da descrivere e realizzare
- standardizza i componenti di rete al fine di agevolare lo sviluppo di componenti compatibili
- consente la comunicazione fra diversi tipi di hardware e software
- evita che le modifiche apportate all'implementazione di un livello influenzino gli altri livelli

Ciascun livello ha le proprie funzioni e fornisce servizi al livello immediatamente sovrastante.

2.1.2 IP

L'IP, (Internet Protocol), come dice il nome stesso, è il protocollo su cui si basa Internet. Esso si occupa di fornire un metodo di indirizzamento logico, di gestione, frammentazione e riassemblaggio per la trasmissione dati tra gli host della rete.

Il protocollo IP, nasce negli anni settanta grazie a una serie di ricerche fatte dalle università americane su richiesta del Ministro della Difesa, allo scopo di realizzare una rete in grado di trasportare diversi tipi di informazioni. L'IP protocol definisce una tecnica di trasmissione dati non orientata alla connessione (detta anche "connectionless") e senza riscontro (non c'è garanzia che i pacchetti giungano a destinazione e nella sequenza corretta). Esso prevede che le informazioni vengano strutturate in unità chiamate datagrammi IP (IP datagram), di lunghezza massima 65535 byte, suddivise in due aree: il campo dati ("data") che contiene il messaggio da inviare e l'intestazione ("header") che contiene le informazioni necessarie per instradare il pacchetto.

Questo protocollo appartiene al Livello di Rete, ovvero quello dei “famosi” indirizzi IP, ovvero quegli indirizzi che individuano univocamente un dispositivo dotato di una NIC[21], all'interno di una rete

2.1.3 TCP

Il TCP (Transmission Control Protocol) è uno dei principali protocolli della Suite di protocolli Internet. TCP è il protocollo di trasporto più utilizzato, su cui si appoggiano gran parte delle applicazioni Internet.

Il TCP è un protocollo corrispondente al Livello di Trasporto del modello di riferimento OSI, e di solito è usato in combinazione con il protocollo di livello rete IP (TCP/IP[9]).
Il TCP è nato anch'esso negli anni settanta come frutto del lavoro di un gruppo di ricerca del Dipartimento di Difesa statunitense. I suoi punti di forza sono l'alta affidabilità e robustezza. La sua popolarità si deve anche grazie ad una sua implementazione diffusa dalla Università di Berkeley in California sotto forma di sorgenti. La sua diffusione è stata facilitata dal fatto che è stato ed è un protocollo utilizzabile gratuitamente.
Le caratteristiche principali del TCP sono:

- la creazione di una connessione (protocollo orientato alla connessione o detto anche connection-oriented)
- la gestione di connessioni punto-punto
- la garanzia che i dati trasmessi giungano a destinazione in ordine e senza perdita di informazione (tramite il meccanismo di acknowlegment e ritrasmissione)

21 Network Interface Card, è un dispositivo hardware per lavorare con gli indirizzi IP

- attraverso il meccanismo della finestra scorrevole (sliding window), offre funzionalità di controllo di flusso e controllo della congestione, vitali per il buon utilizzo della rete IP, la quale non offre alcuna garanzia sulla consegna in ordine dei pacchetti, sul ritardo, sulla congestione.
- una funzione di multiplazione delle connessioni ottenuta attraverso il meccanismo delle porte.

2.1.4 UDP

L'UDP (User Datagram Protocol) è, come il TCP, uno dei principali protocolli della Suite di protocolli Internet. UDP è un protocollo del Livello di Trasporto. È usato di solito in combinazione con il protocollo IP.

A differenza del TCP, non gestisce il riordinamento dei pacchetti né la ritrasmissione di quelli persi. L'UDP ha come caratteristica di essere un protocollo di rete inaffidabile, privo di connessione (connection-less), ma in compenso molto rapido ed efficiente per le applicazioni "leggere" o time-sensitive. Infatti, è usato spesso per la trasmissione di informazioni audio o video. Dato che le applicazioni in tempo reale spesso richiedono un ritmo minimo di spedizione, non vogliono ritardare eccessivamente la trasmissione dei pacchetti e possono tollerare qualche perdita di dati, il modello di servizio TCP può non essere particolarmente adatto alle esigenze di queste applicazioni. Infatti l'UDP è un protocollo che grazie ai pochi controlli effettuati risulta inviare più velocemente i dati rispetto a TCP e ne congestiona in misura minore la rete in quanto non ci sono pacchetti di conferma (ACK).

L'UDP fornisce soltanto i servizi basilari del livello di trasporto, ovvero:

- multiplazione delle connessioni, ottenuta attraverso il meccanismo delle porte
- verifica degli errori mediante una checksum, inserita in un campo dell'intestazione del pacchetto.

UDP è un protocollo stateless, ovvero privo di stato, questo vuol dire che non mantiene lo stato della connessione dunque rispetto a TCP ha informazioni in meno da memorizzare. Un server dedicato ad una particolare applicazione che sceglie UDP come protocollo di trasporto può supportare molti più client attivi. E' un protocollo di trasporto di tipo connectionless, per la trasmissione dati tra due host.

I vantaggi nell'utilizzo di UDP sono infatti la velocità e la minore congestione di rete rispetto a TCP (non ci sono pacchetti di conferma) e la possibilità di trasmettere in multicast (invio di un pacchetto ad un gruppo di host) e broadcast (invio di un pacchetto a tutti gli host di un segmento di rete).

2.1.5 ARP

L'ARP[10] (Address Resolution Protocol) è un protocollo di Livello Rete. È un protocollo, che come dice la sua stessa definizione, risolve gli indirizzi di rete.

Si premette che gli indirizzi IP, chiamati indirizzi logici, sono assegnati indipendentemente dagli indirizzi fisici (detti anche indirizzi MAC address[22]) di una macchina.

I router utilizzano gli indirizzi logici, ma è bene sottolineare come due macchine qualsiasi possono comunicare solo se conoscono gli indirizzi fisici

22 Media Access Control address, sono indirizzi di 48 bit in hex univoci a livello mondiale, assegnato ciascuno ad un NIC

di rete; sorge quindi il problema di associare agli indirizzi IP logici a quelli fisici per ogni ogni interfaccia di rete.
Per risolvere tale problema esiste il protocollo ARP:

- una macchina, a partire dall'indirizzo IP, usa un messaggio broadcast (ARP request) per trovare l'indirizzo fisico di un'altra macchina (Figura 3.1 a)
- tra tutte le macchine che ricevono l'ARP request, quella a cui corrisponde l'indirizzo IP risponde inviando il proprio indirizzo fisico alla macchina che ha inoltrato la richiesta (Figura 3.1 b).

La figura seguente mostra il protocollo ARP:

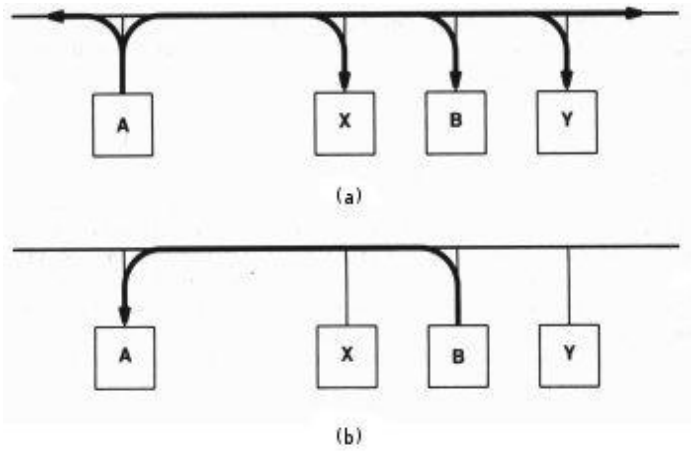

Figura 2.2 – Funzionamento protocollo ARP

2.1.6 RARP

Il RARP[11] (Reverse Address Resolution Protocol) è un protocollo di Livello Rete e serve per risolvere un indirizzo fisico in un indirizzo IP. Questo sistema consente ad un host di conoscere il proprio indirizzo IP

all'accensione chiedendolo, in modalità broadcast agli altri host connessi alla rete. In genere la richiesta arriva ad un server RARP che contiene l'indirizzo di risposta nei propri file di configurazione.

Nella figura seguente è mostrato il protocollo RARP:

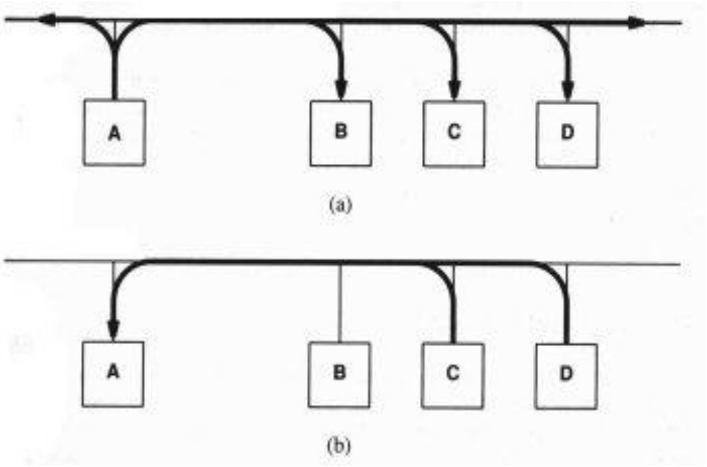

Figura 2.3 - Funzionamento protocollo RARP

2.1.7 ICMP

L'ICMP[12] (Internet Control Message Protocol) è un protocollo di Livello Rete e viene associato ad IP. Si ricorda che il protocollo IP, di per sé, non contiene nessuno strumento per poter riscontrare, da parte della stazione destinazione, la perdita di un pacchetto o il collasso di una rete. Si tratta quindi di un meccanismo attraverso il quale i router e gli utenti comunicano per sondare eventuali problemi o comportamenti anomali verificatisi in rete.

L'ICMP consente una comunicazione straordinaria tra routers ed hosts permettendo lo scambio di segnali di errore o di controllo attraverso le interfacce software dell'internet, senza però arrivare fino al livello degli

applicativi; esso è una parte necessaria ed integrante dell'IP ed è contenuto nell'area dati di un datagramma IP.

L'ICMP include messaggi di “source quench”, che ritardano il rate di trasmissione, messaggi di “redirect”, che richiedono ad un host di cambiare la propria tabella di routing, e messaggi di “echo request/reply”, che l'host può usare per determinare se la destinazione può essere raggiunta (il classico comando ping).

2.1.8 IPX/SPX

L’IPX/SPX[13] (Internetwork Packet eXchange/Sequential Packet eXchange) è un protocollo creato da Novell per le proprie reti, diventato uno standard durante i primi anni novanta. In realtà si tratta di due protocolli distinti, abbastanza simili da poter lavorare insieme in quello che viene considerato come un unico protocollo.

Il protocollo IPX prepara i pacchetti e li inoltra nella rete. Il protocollo SPX controlla invece se il computer destinatario sia collegato, che i pacchetti arrivino integri e se vi siano giunti. Offre la possibilità di interfacciare diversi segmenti di rete e sottoreti; attraverso i router comunicava con reti Novell, in cui veniva ampiamente utilizzato. In realtà il protocollo IPX è stato sostituito con l'avvento della suite TCP/IP. Il funzionamento congiunto di questi due ultimi protocolli è paragonabile a quello dei protocolli IPX/SPX.

2.1.9 DMI

Il DMI (Desktop Management Interface) è una specifica formulata dal Desktop Management Task Force che abilita le comunicazioni tra varie entità di software permettendo la gestione locale o remota di un PC. Ci sono tre tipologie di entità:

- **Component Instrumentation:** è il software che comprende i dettagli di una componente software o hardware di un computer. Un produttore di PC o componenti hardware, fornisce anche il supporto per quel tipo specifico di prodotto. Questo supporto, fornisce informazioni sul prodotto, convertendole in una forma canonica e passandole al Service Provider
- **Management Applications:** fornisce informazioni sulla macchina locale o remota, interrogando il Service Provider, il quale fornisce le informazioni al PC che le richiede, prendendole dall'entità Component Instrumentation. L'applicazione di gestione (Management Application) presenta poi queste informazioni all'utente sulla macchina locale
- **Service Providers:** un Service Provider è il fulcro che permette la comunicazione tra la Management Application e la Component Instrumentation.

2.1.10 MPLS

MPLS[8] (MultiProtocol Label Switching) è il nome dato dall'IETF[23] ad uno standard tecnologico oggi emergente e largamente accettato per la convergenza delle reti e dei servizi che offre l'opportunità di superare le barriere tra le diverse tecnologie e di ridurre la complessità ed i costi delle comunicazioni. Tale nuova tecnologia viene utilizzata quindi, anche per migliorare e velocizzare il routing.

MPLS non può essere considerato un protocollo di rete a tutti gli effetti in quanto non esistono terminali di rete MPLS ma, come detto sopra, è piuttosto da considerare come una tecnologia che all'interno delle reti potenzia il trasporto del traffico e rende possibili dei servizi particolari. Infatti esistono degli apparati di rete che gestiscono pacchetti con MPLS.

Si può fare una precisazione, anche se non universalmente riconosciuta, differenziando il significato di routing e commutazione:

- **routing:** è il processo di ricerca dell'indirizzo IP di destinazione eseguito in una tabella, e stabilisce la destinazione dei dati
- **commutazione:** usa come indice della tabella di routing un'etichetta presa dal pacchetto

Riguardo alla conformazione del pacchetto MPLS, si precisa che, siccome non c'era più spazio da dedicare ai campi MPLS nel pacchetto IP, ne sono stati aggiunti di nuovi. Fra questi campi, quattro per l'esattezza, c'è il campo **etichetta**, il più importante, il quale contiene un indice.

Questa è una tecnica di trasmissione dati utilizzata su reti a commutazione di pacchetto, tipicamente reti IP e alleggerisce i nodi intermedi dal compito di decidere per ogni pacchetto ricevuto la destinazione dove inviarlo in uscita.

23 Internet Engineering Task Force è una comunità aperta di specialisti interessati all'evoluzione tecnica e tecnologica di Internet

MPLS, architetturalmente, si colloca in una sorta di livello intermedio fra il livello Rete ed il livello Data Link dello Standard ISO/OSI.

Si chiama “multi-protocol” perché, teoricamente, è in grado di operare con qualunque protocollo di livello Rete, anche se lo si applica tipicamente ad IP.

Questa tecnologia è in grado di instradare più tipi di traffico (dati, voce, video) sullo stesso canale, consentendo di differenziare la banda di trasmissione in base al tipo di traffico e di aggirare le zone congestionate e i collegamenti interrotti garantendo alti livelli di prestazione.

2.1.11 SNMP

SNMP (Simple Network Management Protocol) è un protocollo che, come dice lo stesso nome, si occupa della gestione della rete. Questo protocollo è fondamentale per i software di gestione delle reti, infatti senza di esso molte informazioni non sarebbero individuabili, rendendo inutile l'utilizzo di tali applicativi.

SNMP nasce nel 1989 e viene definito dalla Internet Engineering Task Force (IETF); da quel momento SNMP diventa uno standard industriale per controllare gli apparati di rete tramite un’unica applicazione di controllo. SNMP rappresenta una serie di funzioni e protocolli per la gestione di rete che comunicano tra di loro attraverso l’Internet Protocol (IP), infatti la prima implementazione avviene sul protocollo TCP/IP, ma in seguito verrà sviluppato anche su reti IPX e AppleTalk. Questo protocollo permette agli amministratori di rete di individuare ed in seguito isolare i componenti difettosi che si possono trovare su una rete, configurare i vari componenti in remoto e monitorare lo stato e le performance della rete.

SNMP è passato attraverso alcune revisioni:

- SNMPv1: rappresenta la prima versione, utilizza l'invio dei nomi di community (utilizzati come password) in chiaro
- SNMPv2: in questa versione, rispetto alla prima, sono state aggiunte nuove funzionalità tra cui la crittografia tramite MD5[24]
- SNMPv3: è lo standard finale, ma al momento raramente utilizzato

Come altri protocolli del livello Applicazione del modello ISO/OSI, SNMP utilizza normalmente l'UDP come protocollo di trasporto e un metodo di comunicazione client/server.

SNMP è composto da due parti:

- **Manager:** il manager è un'applicazione software che viene installata su un computer della rete che verrà utilizzato come stazione di controllo (NMS); i software che si trovano in commercio e anche in rete, gratuitamente, sono diversi e soprattutto si trovano per tutte le piattaforme più diffuse (UNIX, PC e Mac) in modo da non obbligare l'amministratore di rete ad orientarsi su una determinata piattaforma
- **Agent:** gli agenti risiedono sui dispositivi della rete (switch, router,…) e generano informazioni, come i vari indirizzi di rete del dispositivo oppure trasmettono statistiche sul traffico del nodo in cui sono installati. Le informazioni vengono memorizzate all'interno di MIB (Management Information Base).

Gli agenti proxy svolgono le stesse funzioni di un agente normale ma operano per conto di dispositivi su cui non è implementato SNMP.

24 è un algoritmo crittografico

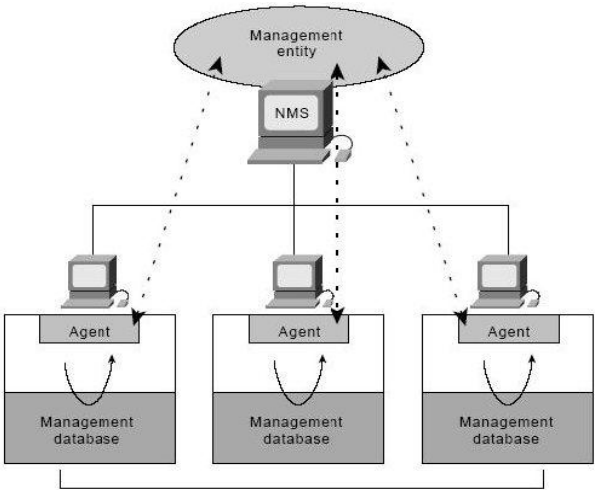

Figura 2.4 – SNMP: NMS e Agent

Come detto, il database che viene gestito dall'agente SNMP è più comunemente conosciuto come MIB (Management Information Base) ed è una raccolta di valori statistici e di controllo riferiti al dispositivo. SNMP permette di estendere questi valori standard con valori specifici per particolari necessità di un agente o di un utente sempre attraverso l'utilizzo dei MIB.

2.1.12 Precisazioni sul protocollo

Uno dei punti di forza del protocollo SNMP è la sua incredibile diffusione e la capacità di adattarsi a qualsiasi dispositivo che faccia parte di una rete di computer, infatti gli agenti SNMP si possono trovare su computer, bridge di rete, switch, router, modem e anche stampanti. Il motivo per cui SNMP è nato e per il quale tuttora è così diffuso è la sua interoperabilità. In più questo protocollo è flessibile ed estensibile in base alle necessità che si presentano. Siccome le funzioni degli agenti SNMP possono essere facilmente estese, per soddisfare le specifiche di ogni componente hardware,

SNMP dispone un grande numero di specifiche per la gestione non strettamente legata agli apparati di rete, ma anche ad esempio per la gestione di una stampante.

Logicamente, questo protocollo, come ogni altra cosa, ha oltre i punti di forza sopra elencati, anche dei punti di debolezza.

Prima di tutto, a discapito del nome Simple Network Management Protocol, SNMP è un protocollo molto complicato da implementare, per stessa ammissione dei progettisti. Un altro punto debole è l'efficienza del protocollo; infatti una parte di banda utilizzata viene in realtà sprecata con informazioni poco utili come per esempio la versione del protocollo che viene trasmessa in tutti i pacchetti o altre informazioni sui data descriptors inserite in ogni pacchetto. Il modo con cui il protocollo identifica le variabili (come le stringhe di byte, dove ogni byte corrisponde a un particolare nodo in una database MIB) comporta uno spreco di buona parte del messaggio.

Si può comunque affermare che la sua complessità non è importante per l'utente finale, in quanto non andrà mai a riprogrammare il protocollo, bensì lo utilizzerà in modo trasparente attraverso degli applicativi.

La completezza di questo protocollo e la sua capacità di adattarsi ad ogni dispositivo per realizzare tutte le funzioni di amministrazione di rete, portano alla conclusione che di fatto non esistono alternativa a SNMP; un altro aspetto da non dimenticare è il fatto che SNMP è oggi il metodo più efficace, e probabilmente il solo, per gestire network di grandi dimensioni.

Il protocollo SNMP assume che i canali di comunicazione siano connectionless, quindi utilizza come protocollo di Livello Trasporto, il protocollo UDP. Di conseguenza, il protocollo SNMP non garantisce l'affidabilità dei pacchetti SNMP.

2.1.13 *Messaggi SNMP*

Dopo aver descritto il protocollo SNMP, si procede alla descrizione dei principali comandi utilizzati da tale protocollo. Tali comandi sono stati creati per soddisfare ogni esigenza di un amministratore di rete:

- **get:** è una richiesta e come valore di risposta riceve il nome dell'oggetto interrogato. Questo comando si può suddividere in due comandi più specifici:
  - **get-request:** l'amministratore può richiedere valori specifici tramite il comando get per determinare le prestazioni e le condizioni di funzionamento del dispositivo. Molti di questi valori possono essere determinati esclusivamente analizzando i messaggi generati dal protocollo SNMP senza la necessità di creare un overhead facendo il login sul dispositivo o stabilendo appositamente una connessione TCP
  - **get-response:** questo comando viene utilizzato dal device di rete per rispondere alle richieste che gli vengono inoltrate tramite get, get-next e set
- **get next request:** la richiesta get-next richiede un altro nome o valore di un oggetto che si trova su un altro dispositivo, che abbia un nome SNMP valido. Questo comando viene utilizzato dagli amministratori per "navigare" sulla rete alla ricerca di tutti i dispositivi che supportano il protocollo SNMP. Questa operazione di ricerca parte dal manager di rete e viene reiterata da ogni nodo SNMP che incontra, sempre attraverso lo stesso comando, fino a quando non viene riscontrato qualche errore; a questo punto il manager è in grado di "mappare" tutti i nodi SNMP della rete di sua competenza

- **get bulk request:** questo comando serve ad accumulare in una unica transazione request/response molte informazioni relative ad un dispositivo. In pratica il get-bulk si comporta come una serie di interazione GetNext request/response, eccetto nel caso in cui sia sufficiente una singola interazione

- **set request:** questo comando mette a disposizione del manager un metodo per effettuare delle operazioni associate al dispositivo di rete come ad esempio disabilitare l'interfaccia, disconnettere degli utenti, pulire i registri, ... In sostanza il `set` permette di configurare e controllare in modo remoto il dispositivo tramite SNMP

- **trap message:** il comando trap viene generato dal dispositivo agente (quindi dal device di rete) in maniera asincrona quando deve segnalare o notificare un evento speciale al network manager. È un comando che quindi consiste in un meccanismo automatizzato, attraverso il quale i dispositivi di rete possono mandare delle comunicazioni sul loro stato ai network manager. Generalmente questa funzione viene utilizzata per notificare degli errori o stati di warning. Per ricevere i pacchetti trap è necessario configurare i vari dispositivi di rete in cui è installato il SNMP Agent.

Tutti questi messaggi viaggiano sulla rete incapsulati in PDU[25] e lo scambio di questi tra i dispositivi avviene tramite protocollo SNMP.

25 Protocol Data Unit, è il formato personalizzato per ogni livello ISO/OSI dello scambio di informazioni fra i vari layer

2.1.14 MIB

La lista dei valori che un oggetto può supportare è spesso chiamata SNMP MIB. Capita di frequente che si senta abusare di questo termine per descrivere ogni oggetto SNMP, mentre in realtà MIB è un tipo di database (virtuale) per la gestione di dispositivi nelle reti di comunicazione. Per l'esattezza non è un vero e proprio database, ma bensì una descrizione dell'informazione gestita, che viene rappresentata come una lista ordinata di valori. Un MIB comprende una collezione di oggetti in un “database” usato per gestire le entità (ad esempio router e switch) facenti parte di una rete. Gli oggetti di un MIB vengono definiti utilizzando un sottoinsieme della notazione Abstract Syntax Notation One (ASN.1) chiamato "Structure of Management Information Version 2 (SMIv2)"[14]. Il software che ne effettua il parsing viene chiamato compilatore MIB. Il database è di tipo gerarchico (ovvero strutturato ad albero) ed ogni entry viene indirizzata attraverso un identificatore di oggetto (object identifier).

Questo Object Identifier è l’identificativo univoco di un nodo dell’albero, infatti si esprime con la concatenazione degli identificativi dei nodi su tutta la gerarchia (fino alla radice). Questi valori, nella notazione simbolica, vengono separati da un punto (dot-notation) e sono associati ad un nome ufficiale (come ad esempio sysUpTime, che misura da quanto tempo è acceso il device dall’ultimo avvio, il cui numero identificativo è 1.3.6.1.2.1.1.3.0). Viene messo lo “0” finale per indicare che si accede ad una istanza dell’oggetto (Instance Identifier).

Si può facilmente intuire che è preferibile esprimere le varie funzioni con il rispettivo nome piuttosto che in dot-notation, un po’ come succede con gli indirizzi di Internet dove è preferibile memorizzare un nome piuttosto che un indirizzo IP.

Lo standard MIB include molti oggetti (valori) per misurare e monitorare le attività IP, TCP e UDP, l’instradamento IP, le connessioni TCP, le interfacce e il sistema in generale. Si veda ora un esempio di un oggetto

MIB:

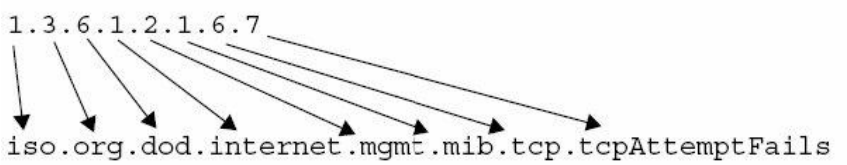

Figura 2.5 – Object Identifier MIB

Ogni oggetto dello SNMP è definito per avere un accesso particolare, “read-only”, “read/write”, “write-only” che determini se l'utente può leggere il valore dell'oggetto, leggere e scrivere il valore di un oggetto (usando il comando set) o soltanto scrivere il valore.

2.1.15 *Messaggi TRAP*

I messaggi TRAP sono dei messaggi che vengono inviati in maniera asincrona da un Agente verso il Manager per segnalare degli eventi particolari. I seguenti messaggi TRAP sono quelli che si possono incontrare più frequentemente:

- **ColdStart:** l’agente si è autonomamente avviato o riavviato e i dati potrebbero aver subito delle alterazioni
- **WarmStart:** l’agente si è autonomamente riavviato ma non c’è stata alcuna alterazione dei dati
- **LinkDown:** una interfaccia connessa è passata dallo stato link UP allo stato DOWN
- **LinkUp:** un’interfaccia connessa è passata in uno stato link UP
- **AuthenticationFailure:** il nome della community per accedere al dispositivo è errato

3 NETWORK NODE MANAGER 7.5

3.1 Introduzione a Hp OpenView NNM

Questo è il prodotto software finalizzato alla gestione delle reti, sviluppato dalla HP. Come detto precedentemente Network Node Manager (comunemente chiamato NNM) è uno, se non il primo, dei software più utilizzati dalle grandi imprese ed enti per monitorare reti di vaste dimensioni.

Bisogna premettere che NNM è un applicativo nato per ambienti Unix e poi è stato "adattato" a quelli Microsoft Windows.

Tale prodotto ha come finalità quella di monitorare le attività di rete di una determinata network o più network contemporaneamente.

Questa attività si basa sull'acquisizione di informazioni provenienti dai singoli nodi della rete.

Per fare ciò, di default il software utilizza il protocollo SNMP e quindi si basa sull'interazione SNMP Manager e SNMP Agent. L'acquisizione delle informazioni, con questo metodo può avvenire in due modi:

- attraverso **get request** da parte del Manager e successiva **get response** da parte dell'Agent
- attraverso l'attivazione di una **trap** nel nodo agente e quindi invio di informazioni al nodo manager

Le trap, come precedentemente descritto, sono delle eccezioni che vengono innescate al verificarsi di un dato evento preconfigurato nel MIB dell'Agent.

Se i nodi in questione non supportano SNMP o non lo hanno abilitato, si passa all'acquisizione di informazioni attraverso il protocollo IP o IPX (quest'ultimo solo per Windows).

Generalmente si può affermare che NNM utilizza i seguenti protocolli per mantenere i canali di comunicazione con ciascun dispositivo gestito sulla rete:

- SNMP
- TCP/IP
- UDP
- IPX/DMI
- ICMP
- ARP/RARP

NNM è utilizzabile in tre differenti modalità:

1. NMS
2. console remota
3. via web; bisogna specificare due diverse tipologie di interfacce web:
    a) **Home Base:** è l'interfaccia accessibile a tutti gli utenti che ne conoscono l'indirizzo di rete
    b) **Web Launcher:** è l'interfaccia accessibile solo agli utenti autorizzati. In pratica è un sistema chiuso (login e password)

Tutte e tre queste modalità fanno capo allo stesso database; in pratica le informazioni vengono raccolte tutte in esso e poi a seconda dell'accesso scelto, vengono effettuate delle query al database stesso.

La seconda modalità, cioè quella attraverso l'utilizzo di una console remota, comprende l'utilizzo in remoto del software GUI (Graphical User Interface)

solo nel caso in cui ci si colleghi alla NMS; infatti tale applicativo è presente solo ed esclusivamente in questa macchina. L'altro caso di utilizzo della console remota comprende l'utilizzo dell'interfaccia web (Home Base o Launcher). Solo in un modo è possibile utilizzare contemporaneamente sia l'interfaccia web sia quella GUI, ovvero collegandosi in remoto o direttamente sulla NMS.

Logicamente, utilizzando un software commerciale e dovendo investire una cifra importante per l'acquisizione della licenza, si preferisce usare un server dedicato per un corretto utilizzo dell'applicativo.

Difficilmente si andranno ad utilizzare le varie interfacce direttamente dalla postazione server, ma si prediligerà, com'è logico, l'utilizzo da console remota.

3.2 Standard e Advanced Edition

È importante precisare che esistono due tipologie di licenze rilasciate da HP riguardo NNM:

- **Standard Edition**
- **Advanced Edition**

La Advanced Edition si distingue dalla Standard Edition principalmente per la disponibilità dell'**Extended Topology**. Quest'ultima è una modalità che prende in esame, come dice la parola stessa, la topologia estesa, ovvero va ad analizzare e visualizzare informazioni addizionali riguardo la connettività dei singoli dispositivi. Questa funzionalità viene solitamente usata per diagnosticare i problemi della network.

Fra le varie funzionalità di questa estensione vanno ricordate:

- la gestione di ambienti switched eterogenei di livello Data Link e routed di livello Rete del modello ISO/OSI
- visualizzazione di viste dinamiche attraverso interfaccia web
- utilizzazione di SPIs (Smart Plug-ins), i quali forniscono delle viste che sfruttano protocolli e tecnologie ai livelli più alti della rete, come OSPF[26] e HSRP[27]
- la visualizzazione di viste eseguite direttamente selezionando gli eventi che le riguardano

NNM, utilizzando SNMP, ha un MIB e ha anche un MIF (Management Information Format):

- **MIB:** è un "database" con i riferimenti ai relativi oggetti della rete e il relativo stato
- **MIF:** definisce la sintassi con la descrizione delle informazioni di gestione relativa ai componenti software e hardware che possono essere installati su un computer. I file MIF sono usati da DMI per riportare informazioni sulla configurazione di sistema

NNM reperisce automaticamente, dopo aver effettuato adeguati settaggi, informazioni circa oggetti MIB e eventi MIF, al fine di analizzarne il trend.

Tali informazioni, riguardo i trend, sono tutte visualizzabili in tempo reale o come storico delle informazioni; per quanto riguarda il GUI, tali analisi si possono effettuare nel menu `Options: SNMP MIB browser`.

Bisogna dire che NNM, per la raccolta di informazioni dai router deve necessariamente conoscere la **community name** del dispositivo considerato. Infatti è attraverso tale identificativo che è permesso alla NMS di

26 Open Shortest Path First, è un protocollo link-state sviluppato dall'IETF
27 Hot Standby Router Protocol, è un protocollo proprietario di Cisco ed è volto a garantire la fault tollerance fra i router Cisco

raccogliere tali dati.

3.3 Comunity name

La community name è una sorta di password di riconoscimento e deve essere identica in entrambi i dispositivi; se i dispositivi, all'inizio della loro connessione, riscontrano la stessa community e utilizzano entrambi la stessa porta per la trasmissione, la connessione può avvenire, altrimenti viene rifiutata. Di default la community è impostata a "public" e la porta di trasmissione è la 161[28].

A riguardo, nel GUI di NNM, si possono impostare le singole community in riferimento a ciascun nodo della rete che supporti SNMP o delle community multiple per un range di indirizzi in modo tale da non doverle impostare manualmente per tutti questi nodi. Il range di indirizzi a cui si fa riferimento viene detto **wildcard**.

Fra questi due modi di operare con le comunity name, vi è una principale differenza, oltre al fatto di non doverle impostare manualmente per ogni singolo nodo; nel primo caso il sistema andrà a provare la singola community per il nodo specificato, mentre nel secondo andrà ad analizzare il range di indirizzi provando le community in maniera sequenziale fino a trovare quella giusta; una volta trovata, le rimanenti non vengono processate.

Questo secondo metodo produce necessariamente un carico elaborazionale e un traffico di rete più elevato rispetto al primo metodo, anche se bisogna precisare che, se il server dove risiede il software di managing è dedicato, l'overhead generato risulta sopportabile.

28 Si precisa che tale porta di comunicazione è quella utilizzata da SNMPv1

Il file finalizzato all'utilizzo delle community impostate è `netmon.cmstr`.

La sintassi utilizzata in tale file ha la seguente forma:

```
"secret", "another secret" : 10.2.44.* : : 20 : 3
```

questo significa che sono state immesse due community string (secret e another secreet) per i nodi con range di indirizzo IP 10.2.44.0-255 e tutti i tipi di MAC address, due secondi di timeout (è espresso in decimi di secondo) con tre retry.

NNM prova poi le community name presenti in questo file.

Se le community name sono identiche, si può accedere al dispositivo e avere informazioni dettagliate, grazie all'utilizzo del protocollo SNMP.

Si ricorda che una volta acceduto al MIB del SNMP Agent, il SNMP Manager può effettuare operazioni di:

- get: vi sono due metodi per il get:
  - getrequest: legge i valori da una specifica variabile
  - getresponse: risponde ad una get request o ad una set request

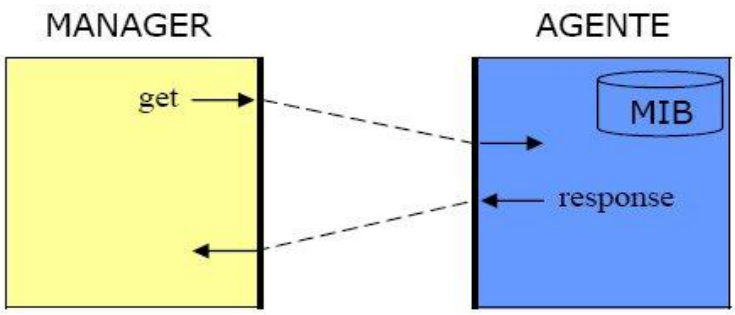

Figura 3.1– Comando get

- getnext: è una get request usata per accedere ricorsivamente sul MIB

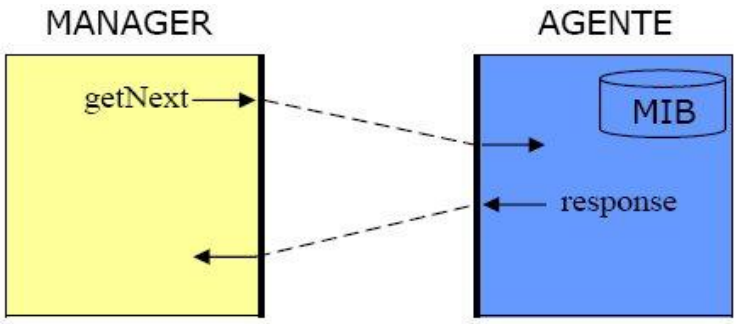

Figura 3.2 – Comando getNext

- getBulk: è una get request con la possibilità di specificare il numero di variabili da leggere

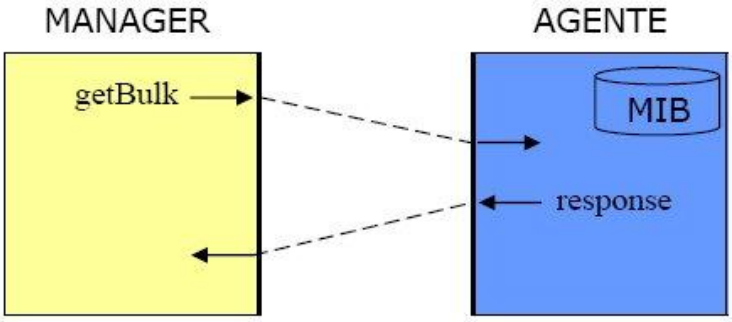

Figura 3.3 – Comando getBulk

- set: usata per impostare un valore in una determinata variabile

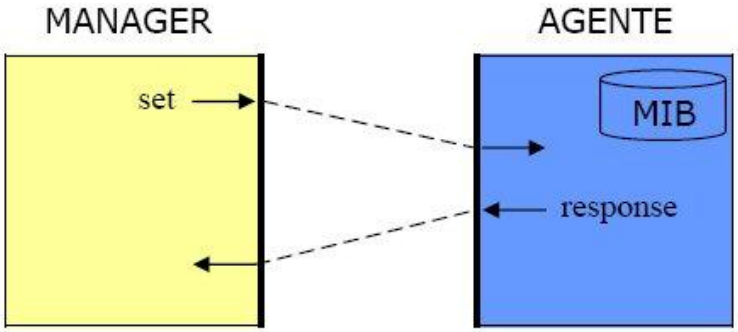

Figura 3.4 – Comando set

- trap: sono dei messaggi inviati dall'Agent senza la richiesta del Manager

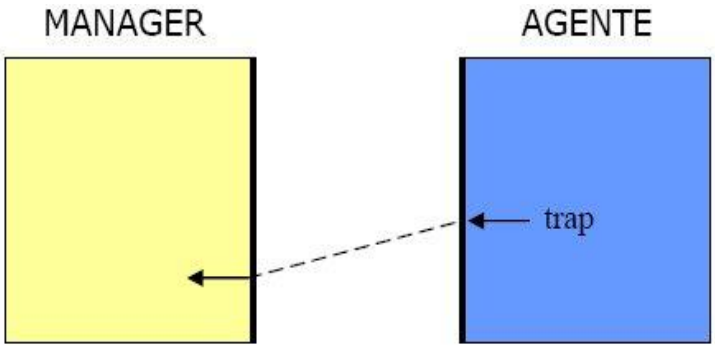

Figura 3.5 – Comando trap

3.4 Oggetti e simboli

Un oggetto può rappresentare un'entità logica (ad es. un gruppo, tutte le stampanti, tutti i pc, ...) o fisica (ad es. un router, un server, ...). Ogni oggetto è presente nel database di NNM e ha dei propri attributi. A questi attributi possono essere assegnati dei valori (es. l'attributo `seletion name` identifica univocamente l'oggetto all'interno del proprio name space).

Un simbolo è una rappresentazione grafica dell'oggetto.

Esistono due tipologie di oggetti:

- **icon symbol:** è un simbolo geometrico che rappresenta un nodo della rete e può avere al suo interno un'icona che specifica meglio il tipo specifico di simbolo
- **connection symbol:** sono i simboli dei link, ovvero i simboli che collegano due icon symbol

Entrambe i simboli possono svolgere una di due possibili azioni, ovvero:

1. **explod:** al doppio click del mouse sul simbolo si aprirà una nuova sottomappa contenente, se sono stati impostati, gli oggetti interni a tale simbolo (es. le interfacce all'interne di un router)

2. **execute:** al doppio click del mouse sul simbolo si può far corrispondere una determinata azione (es. l'avvio di un certo programma)

L'icon symbol è diviso in classi e sottoclassi (ad es. classe: Network; sottoclasse: Generic Network, IPNetwork, ...)

3.5 Managed e Unmanaged

In NNM gli oggetti, i quali sono raccolti nel database, possono essere:

- **managed:** sono quegli oggetti da cui si ricevono più informazioni; sono cioè quelli che hanno abilitato ed utilizzano SNMP per il trasporto delle informazioni alla NMS. Tali oggetti sono interessati attivamente dal monitoraggio e dal polling della rete. I simboli di tali oggetti assumono diverse colorazioni a seconda del loro stato
- **unmanaged:** danno poche informazioni; solo il posizionamento statico dell'oggetto nella rete e l'indirizzo IP/IPX. È utile per questo impostare per tali oggetti le trap per determinati eventi, in modo da ricevere informazioni da tale nodo solo nel momento in cui si verifichino le situazioni preimpostate. I simboli associati a tali oggetti assumono una colorazione simile al bianco

Figura 3.6 – Stato degli oggetti

Questa metodologia è molto utile, infatti grazie a essa si riesce a ridurre il numero di nodi managed della rete, così da poter apportare una carico minore sia per la macchina server che ospita il software NNM sia per il traffico di rete. Infatti gli oggetti managed comportano un maggior traffico di rete e un maggior carico del CPU e del RAM. Inoltre è importante per la licenza tener presente il numero di nodi managed; esistono a riguardo licenze con un numero massimo di nodi maneggiabili. Al raggiungimento del numero di nodi managed, come da licenza, NNM continuerà a scoprire nuovi nodi nella rete e poi li inserisce nel suo database, ma li imposterà tutti come unmanaged.

Si precisa comunque che NNM ha anche un limite massimo di nodi scopribili, oltre tale limite il discovery non mette più oggetti nel database.

3.6 Discovery e polling

Si analizzano ora due termini che hanno un ruolo centrale in NNM:

- **polling:** è un modo di interrogazione dei nodi per acquisire informazioni su tali oggetti
- **discovery:** è il metodo per l'acquisizione dei nodi della rete, ovvero il sistema va a vedere se ci sono nodi ad esso collegati e, se ne trova, li inserisce nel database

Sia il polling sia il discovery può essere impostato attraverso la configurazione relativa, che si trova nel menu `Network Polling Configuration IP/IPX` del GUI.

Esistono due protocolli su cui si può basare il discovery (escludendo quello relativo all'Extended Topology):

- **IP:** in questo caso il discovery si affida a SNMP per scoprire i nuovi nodi (nuovi nel senso che non sono presenti nel database). Usando tale protocollo, il processo di discovery si affida principalmente alle query SNMP per acquisire informazioni riguardo i nuovi nodi

- **IPX:** netmon, un processo descritto in seguito, utilizza versioni broadcast di vari protocolli IPX (IPX può essere utilizzato solo su ambienti Windows per quanto riguarda NNM) per scoprire i nodi che utilizzano SNMP. Una volta che il nodo è stato scoperto aggiunge informazioni addizionali riguardo il dispositivo. netmon stabilisce che un nodo IPX supporta IP solo se tale nodo supporta SNMP attraverso IPX. Logicamente i router o server IPX devono essere connessi alla NMS e devono essere in grado di rispondere a richieste diagnostiche IPX

Il discovery comporta un elevato dispendio di risorse per la macchina e è molto importante per la corretta gestione della rete. Esistono due tipi di dicovery:

- quello relativo solo all'Extended Topology

- il Full Discovery, ovvero che include anche l'ET (Extended Topology) oltre al normale discovery

Lo stato di apparati non IP o IPX è determinato via SNMP, basandosi sullo stato amministrativo ed operativo della porta esaminata.

Va ricordato che esistono due processi diversi per il polling:

- **netmon:** è il motore di polling più datato e svolge anche il discovery; lo svolge anche se si usa APA come processo di polling. Netmon utilizza una combinazione di richieste SNMP e ping ICMP trasmessi attraverso UDP e IPX per trovare i nodi della rete. Permette una limitata riconfigurazione dinamica.

- **APA (Active Problem Analizer):** è il nuovo motore di polling. Il processo relativo è l'`ovet_poll`. Usa il protocollo HSRP come default per i dispositivi scoperti nell'Extended Topology. Il polling di tale processo è basato sull'analisi dei path al livello due del modello ISO/OSI.

Riferendosi invece alle varie tipologie di polling effettuabili, possiamo identificarne cinque:

1. **status polling:** consiste nell'invio di un messaggio ICMP ad ogni nodo gestito (managed). L'intervallo di default è di quindici minuti fra un polling e l'altro, ma si possono comunque impostare intervalli di polling personalizzati anche per indirizzo o hostname

2. **configuration check polling:** raccoglie informazioni riguardo tutti i dispositivi controllati da NNM. Le informazioni riguardano l'aggiunta o la rimozione di un'interfaccia, il cambio di locazione, modifica del nome del nodo, cambiamento delle subnetmask, ... Riguarda cioè tutti i cambiamenti che avvengono relativamente ai vari dispositivi di rete. Di default tale operazione viene eseguita ogni ventiquattro ore. Tale polling non permette una personalizzazione particolarmente ampia, infatti la riguarda solamente la possibilità di variare l'intervallo di polling; i dispositivi che vengono interessati da tale operazione, non sono personalizzabili, ma riguarda o tutti o nessun dispositivo

3. **connector topology polling:** monitora gli hub e switch che sono connessi ad una rete

4. **new node discovery polling:** vengono controllate le ARP cache e le routing table disponibili. Queste informazioni vengono utilizzate per mantenere aggiornata la mappa e si applica indistintamente a tutti i dispositivi gestiti. Di default, tale polling avviene ogni sei ore. Anche in questo caso la personalizzazione riguarda indistintamente

tutti i dispositivi gestiti nella rete. Si possono personalizzare i parametri della ricerca relativamente agli oggetti con informazioni di livello Data Link, di protocollo IP o IPX

5. **secondary failure polling:** tale impostazione permette di regolare il tempo massimo in cui NNM ignora i dispositivi guasti. Di default è attivo, ma c'è la possibilità di non far ignorare nulla a NNM

Ritornando al discovery, si può affermare che netmon per trovare (discover) i nodi della rete, deve conoscere:

- la subnet mask del'Agent
- l'indirizzo di default del gateway nella routing table della NMS
- informazioni SNMP del default router (come minimo) e altri router della rete

Il DMI, analizzato in precedenza, è una strategia di management parallela al protocollo SNMP, ma completamente indipendente. Esistono tra le due metodologie delle similitudini:

- il client DMI è simile a quello SNMP della management station
- il DMI service provider è simile al server SNMP e deve essere attivo su ciascun dispositivo remoto
- il file MIF DMI (Management Information Format) è simile al file SNMP MIB e definisce la gestione delle informazioni che possono essere fornite dal servizio provider o richieste dal client (get/set).
- Il DMI event è simile alla trap SNMP

I messaggi che arrivano alla NMS vengono ricevuti dal processo

`ovcapsd`[29] e vengono poi convertiti in trap SNMP. Tali messaggi equivalenti vengono poi inviati all'Alarm Browser (analizzato nel prossimo paragrafo).

3.7 Alarm Browser

L'**Alarm Browser** è un insieme di messaggi che vengono ricevuti dalla Management Station in merito al verificarsi di determinati eventi. Di default vengono ricevuti tutti i messaggi dei vari eventi possibili, naturalmente inviati dai dispositivi nel caso del verificarsi dell'evento stesso (es. node down, subnet changed, ...). C'è la possibilità di limitare l'invio di tali messaggi disabilitando (unmanaged) il monitoraggio di un dispositivo e impostando l'invio di una trap alla management in caso del verificarsi di un evento predefinito.

Si precisa che è possibile filtrare i vari eventi attraverso l'impostazione dei campi presenti nel menu `View : Set filters`. A tale menu si può accedere dalla finestra `Alarm Categories` relativa agli allarmi, come dall'immagine seguente:

29 è un processo che testa i nuovi nodi scoperti dopo che sono stati inseriti nel topology databse

Figura 3.7 – Alarm Browser

Tutte le varie operazioni e viste riferite a NNM che coinvolgono gli oggetti fanno riferimento al database NNM. Tale database registra le informazioni che riguardano i nodi scoperti e è utilizzato dal processo `ovw` per generare automaticamente la mappa della rete.

Tale **mappa** è la rappresentazione logica della rete e non la sua rappresentazione fisica.

3.8 I Database di NNM

Il database NNM si serve di alcuni database che immagazzinano ciascuno, un determinato tipo di dati. L'elenco dei database utilizzati da NNM è il seguente:

- **Operational db:** è il database in cui vengono immagazzinate le varie operazioni effettuate fra i dati
- **Object db:** contiene informazioni semantiche circa i simboli sulla mappa
- **Map db:** contiene le informazioni di visualizzazione della

mappa, come ad esempio la disposizione dei simboli sulla mappa, la loro associazione con gli oggetti, la visualizzazione personalizzata per ogni utente, ...

- **Topology db:** gestisce informazioni critiche riguardo la gestione dei nodi IP. Include informazioni sullo stato degli oggetti, come ad esempio il time stamps, che indica l'ultima volta che l'oggetto ha subito una variazione e quando è previsto il prossimo avvio del polling

- **Event db:** in esso vengono immagazzinati gli eventi di Openview NNM come SNMP trap. Le informazioni contenute in tale database sono visualizzabili nell'Alarm Browser.

- **Trend db:** immagazzina i dati MIB e le informazioni di threshold che sono ottenute attraverso il servizio di `snmpCollect`. Tali informazioni possono essere visualizzate graficamente attraverso l'utilità `Grapher`.

- **Data Warehouse:** immagazzina dati esportati dal database di NNM in un database relazionale. Tali informazioni si possono esportare usando il menu `Tools : Warehouse`.

Un nodo che non comunica con altri nodi o gateway non viene visto da NNM, così bisogna che NNM invii ping ICMP di basso livello al fine di scoprire il nodo; in alternativa lo si può aggiungere manualmente.

Riguardo l'aggiunta di un nodo, si può precisare che NNM, nel momento in cui un nodo viene aggiunto, attraverso il menu `Edit : Add object`, dopo aver immesso il nome host e l'indirizzo IP, il software va a calcolarsi in automatico la subnet mask. Se tale nodo è già presente, viene visualizzato un messaggio che ci avvisa dell'esistenza di tale oggetto nel database.

Per capire meglio l'immissione manuale di un nuovo nodo in una mappa vengono inserite due immagini esplicative:

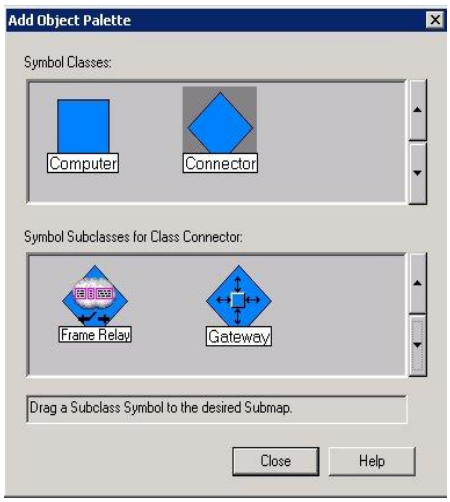

Figura 3.8 – Add Object 1/2

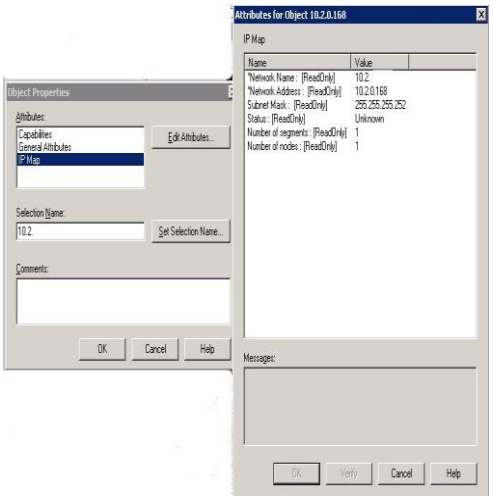

Figura 3.9 – Add Object 2/2

3.9 Mappe, sottomappe e livelli gerarchici

Per ciascuna sessione di NNM attiva si può aprire una singola mappa (**root map**); ciò vuol dire che se si vuol visualizzare un'altra mappa, si deve chiudere la precedente o avviare un'ulteriore sessione.

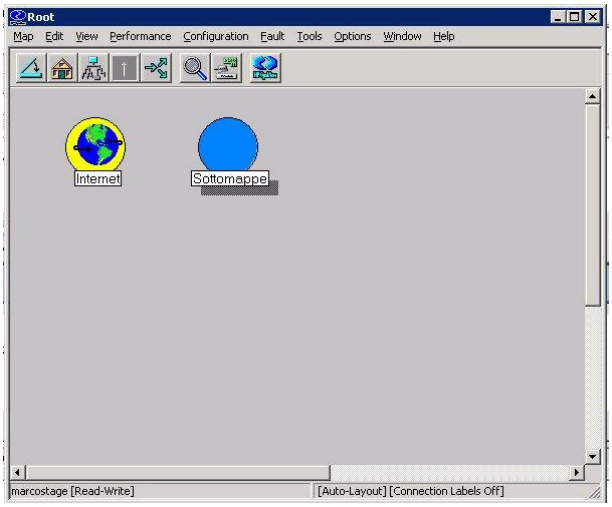

Figura 3.10 – Mappa

Non ci sono vincoli invece riguardo al numero delle sottomappe visualizzabili.

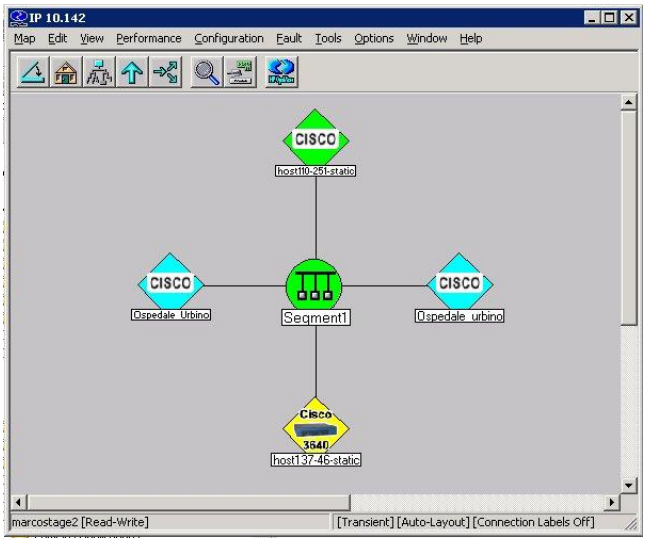

Figura 3.11 - Submap

Una precisazione molto importante da fare riguarda la classificazione gerarchica delle mappe. Esistono infatti, all'interno della **root map**, quattro livelli di sottomappe nelle quali vengono inseriti gli oggetti scoperti:

- **internet level:** IP Networks, gateways, routers e multi-homed workstation
- **network level:** segmenti a bus, stella, anello, gateways, routers, switches, hubs, bridges; se si ha un sistema windows si possono aggiungere anche: IPX networks, gateways e routers
- **segment level:** host, gateways, routers, hubs, switches, bridges; se si ha un sistema windows si possono aggiungere anche: IPX networks, gateways e routers
- **node level:** a questo livello sono presenti i dispositivi NIC

Un mezzo importante per verificare l'efficacia del discovery iniziale è l'`inventory report`. Attraverso tale strumento si possono visualizzare i nodi contenuti nel DB diviso per tipologia e organizzato in sottoreti.

Tale inventory report si può configurare attraverso l'uso del `web Reporting Interface`.

Se la mappa che viene visualizzata, non soddisfa le proprie aspettative, la si può personalizzare. La personalizzazione inizia sin dalla fase precedente il discovery, ovvero settando due tipi di impostazioni, ciascuna con un proprio fine. Va premesso che NNM nella fase di discovery parte da un nodo iniziale per poi aggiungere man mano i nodi che rispondono alle sue request. Così facendo, si ottiene un'espansione della mappa "a macchia d'olio". Le due impostazioni a cui si fa riferimento sono:

- **seed file:** tale file è codificato in ASCII e contiene una lista di network-level address o host name (non indirizzi IPX). Questo procedimento risulta molto utile nel caso in cui il proprio dominio contenga più reti. Con tale archivio si configura il processo netmon per generare la mappa partendo da più indirizzi IP invece che dal singolo nodo iniziale (tale singolo nodo rappresenta l'impostazione di default)
- **loadhosts Program:** nei domini che contengono pochi dispositivi SNMP si può velocizzare il processo di discovery creando un un file ASCII con la lista dei dispositivi che necessitano di essere aggiunti al database topologico e alla mappa. Così facendo si bypassa il discovery per tali nodi, ovvero tali dispositivi vengono messi nel database senza essere prima elaborati da tale processo. Con tale procedimento il discovery risulterà più veloce

Ci sono poi altre configurazioni aggiuntive finalizzate alla personalizzazione del processo di discovery:

- **IPX Hop Count:** si imposta un numero massimo di hop (massimo 16). Come hop vengono considerati i gateway, i router e i server

- **netmon.noDiscover:** è un file in cui si immettono liste di indirizzi IP o range IP per escluderli dal discovery, quindi anche dal database e dalle mappe. Durante il discovery, quando vengono valutati gli indirizzi dei vari device della rete, avviene il confronto con quelli presenti in questo file. Se le due stringhe confrontate risultano uguali, gli indirizzi corrispondenti vengono esclusi dall'immissione nel database. Questo è il metodo più semplice per limitare il traffico di rete

- **discovery filter:** è un'impostazione che va a filtrare ed escludere i dispositivi che non hanno le caratteristiche specificate nel filtro applicato. I filtri che possono essere impostati fanno riferimento al file `filters` nella cartella `install_dir/conf/c`. Questo "appesantisce" il carico elaborativo del processore in quanto deve elaborare il filtraggio per ogni singolo oggetto scoperto dopo aver raccolto tutti gli attributi dei device nel MIB. Le informazioni che non hanno una corrispondenza con il filtro vengono scartate e quindi non immesse nel database

- **oid_to_type**: è un file modificabile e specifica i tipi di dispositivo che vengono automaticamente impostati come unmanaged durante il discovery iniziale. Come detto, tali dispositivi vengono immessi nel database di NNM ma non vengono considerati per la raccolta di informazioni per il traffico generato

Sempre riguardo al discovery iniziale bisogna precisare che esiste un comando molto importante che permette di forzare netmon a recepire i nuovi filtri e a "ripulire" il database dalle informazioni esistenti permettendo di recepire tali nuovi filtri, riflettendoli in automatico sulla mappa. Questo comando è `ovtopofix`.

3.10 Ricerca dei nodi

Per essere veloci e precisi nell'individuare uno o più nodi si fa uso della ricerca degli stessi attraverso la finestra apposita che viene visualizzata dal menu `Edit: Find`. Una volta aperta la finestra, come da immagine seguente, si può impostare il criterio di ricerca in base all'attributo voluto.

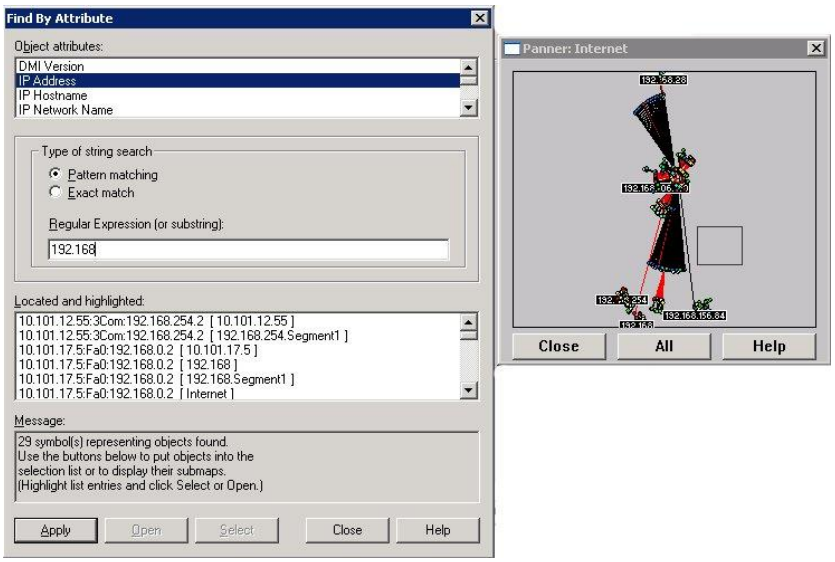

Figura 3.12 – Ricerca nodi

Gli attributi utilizzati per la ricerca sono molti, come ad esempio SelectionName, hostname, ifAlias, IPAddress, ...

Logicamente, a seconda dell'attributo prescelto si devono mettere differenti stringhe (ad esempio IPAddress 10.101.x.x, hostname Pippo, ...).

Una volta immesso il valore desiderato, si può procedere con la ricerca e nel caso vengano trovati degli oggetti corrispondenti nel database, verranno tutti visualizzati nella text box in basso, nella schermata di ricerca.

Tale affermazione può essere comprovata visionando l'immagine 3.12 sopra.

Questa funzione è molto utile, soprattutto se si lavora con migliaia di nodi; infatti è impossibile andare a trovare un nodo interno ad un segmento visualizzando solamente la sottomappa principale. In essa vengono visualizzati tutti i dispositivi sino ad arrivare ai segmenti di rete; ciò che è al loro interno è trasparente in tale sottomappa (ad esempio i computer, i server, ...). Per visualizzare tali dispositivi bisogna aprire delle sottomappe corrispondenti al segmento o network che li contiene. Per fare ciò in maniera veloce si utilizza la funzionalità di ricerca.

3.11 Web Launcher

Il Web Launcher è un programma che viene lanciato da web browser nella forma generica:

```
http://myserver/ovcgi/ovlaunch.exe
```

Dopo aver immesso tale indirizzo apparirà una finestra di autenticazione con login e password.

Immettendo le giuste stringhe si entra nella pagine bel Web Launcher che ha la seguente forma:

Figura 3.13 – Web Launcher

Con questa finestra, si può accedere a molte funzionalità del programma e la si può anche personalizzare a seconda dell'utente che vi accede.

Si possono ad esempio personalizzare i vari menu, le mappe visualizzabili e le impostazioni che l'utente può impostare. La cosa che è maggiormente utile è che per ogni utente si possono impostare personalizzazioni permanenti che non interferiscono con quelle degli altri user.

Con opportune modifiche al file `htpasswd` nel path `install_dir/www/etc` si possono aggiungere nome utente e password di un nuovo user, al fine di farlo accedere al Web Launcher. Si precisa che la password in tale file, per ciascun utente è criptata.

3.12 Home Base

L'Home Base, accennato in precedenza, è un applicativo accessibile da tutti gli utenti, anche quelli che non hanno accesso al Web Launcher, attraverso web browser. La URL generica di accesso a tale servizio è la seguente:

http://hostname:7510

Viene visualizzata una finestra del tipo:

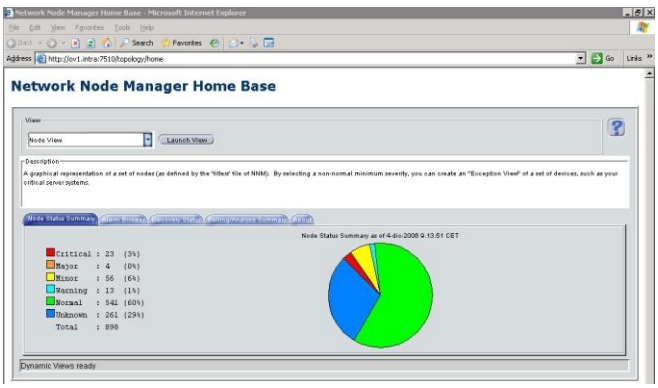

Figura 3.14 – Home Base

Questo è il servizio utilizzato per l'Extended Topology e quindi per le Dynamic View. É molto esaustivo e se tutte le configurazioni sono state fatte in modo adeguato nella GUI, questa visualizzazione risulterà molto esplicativa.

3.12.1 *Dynamic View*

Le viste dinamiche sono quelle viste grafiche, aggiornate dinamicamente, che fanno comunque riferimento allo stesso database del GUI.

Vi sono diversi ambiti in cui si applicano le viste dinamiche, ma ce n'è uno in particolare che è frutto della personalizzazione del manager; Node View.

In questo tipo di vista dinamiche si possono applicare i filtri creati dall'utente, oltre che quelli impostati direttamente da Hp.

In pratica in questo caso se ne fa un utilizzo congiunto con i filtri.

A titolo di esempio si può visualizzare un filtro relativo agli apparati di rete differenziato tra viste statiche e dinamiche, analizzando le figure 3.17 e 3.18.

3.13 Creazione di un filtro

Come prima cosa, per creare una sottomappa statica o dinamica, bisogna avere a disposizione dei filtri adeguati; se non ve ne sono bisogna crearli.

Per fare questo si è studiata la sintassi relativa alla creazione dei filtri che risulta essere:

```
// commento relativo al filtro (opzionale)

nomefiltro "illustrazione filtro" { argomenti coinvolti nel filtro e logica booleana }
```

In pratica, relativamente alla sintassi sopra si è andati a creare un filtro del tipo:

```
// Filtro degli apparati della rete quali Routers, IPRouters, Switches, Hubs e Pix FiltroApparati "Filtra solo gli apparati di rete"

{ isRouter || isBridge || isHub || isIPRouter }
```

Una volta creato il filtro, lo si può testare al fine di vagliare i risultati ottenuti dalla sua esecuzione.

Si precisa che i filtri possono essere applicati solo alle Mappe e non alle sottomappe statiche.

3.13.1 *Test del filtro*

Per fare ciò si utilizza il comando `ovfiltertest -f` nomefiltro. Di seguito viene fornito uno screenshot a riguardo:

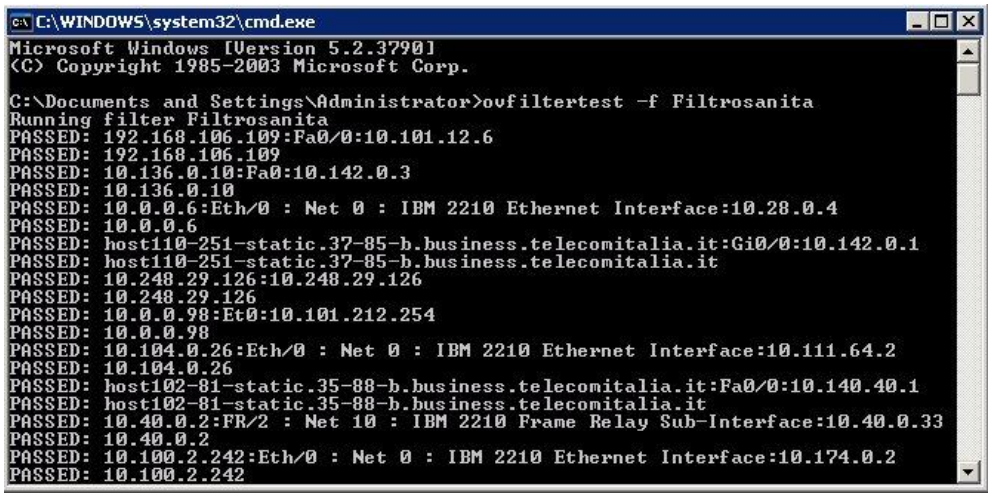

Figura 3.15 – Comando ovfiltertest

Eseguendo tale comando si possono visualizzare tutti quei dispositivi che passano il filtro e vengono cioè potenzialmente visualizzati. Si precisa potenzialmente, perché tale comando, come si intuisce dal suo stesso nome è un test. Se invece c'è un errore nel filtro, viene visualizzato un messaggio di errore, come il seguente:

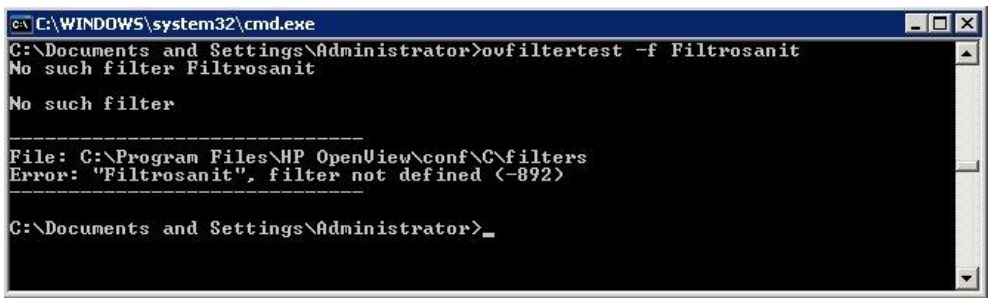

Figura 3.16 – Errore da comando ovfiltertest

3.13.2 *Visualizzazione grafica del filtro*

Una volta appurato che il filtro fa ciò che era nel proprio intento, si procede alla sua applicazione.

Questa può avvenire in due modi:

1. applicando il filtro all'interfaccia GUI; si ricorda che i filtri in tale interfaccia possono essere elaborati solo dalle mappe e non dalle sottomappe. Infatti se si accede al menu

   `Map : Properties -> Applications -> IP Map -> Edit`

   si possono inserire i filtri. Una volta inserito il filtro il software necessita di una verifica e perciò bisogna premere il tasto `verify`. Se tale verifica va a buon fine, verrà abilitato anche il tasto `Ok`. Premuto tale tasto, la finestra apertasi dopo la pressione del tasto Edit, di cui sopra, ritornerà attiva e in questa si potrà procedere all'applicazione del filtro attraverso la pressione del tasto apply. Il risultato sarà il seguente (logicamente il numero e lo stato dei nodi filtrati può variare a seconda dei nodi filtrati della propria rete gestita):

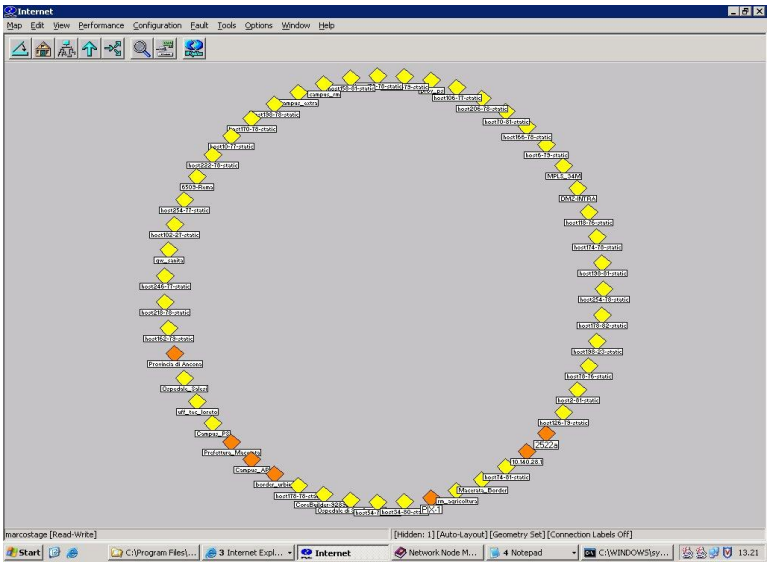

Figura 3.17 – Filtro su GUI

2. una volta verificato che il filtro funziona correttamente si può accedere all'Home Based e selezionare il tipo di viste dinamiche Node View, dal menu a tendina. Confermata la scelta apparirà una nuova finestra dalla quale poter selezionare i campi `Show Nodes, Status>=, IP range`. Il primo campo ci fa vedere un elenco di

filtri; sono tutti quei filtri abilitati e presenti nel file filters cui si è detto prima. In questo modo la visualizzazione sarà più comprensibile, in quanto facente parte di una vista dinamica e non statica come quella del GUI . La Dynamic View risulterà simile a questa:

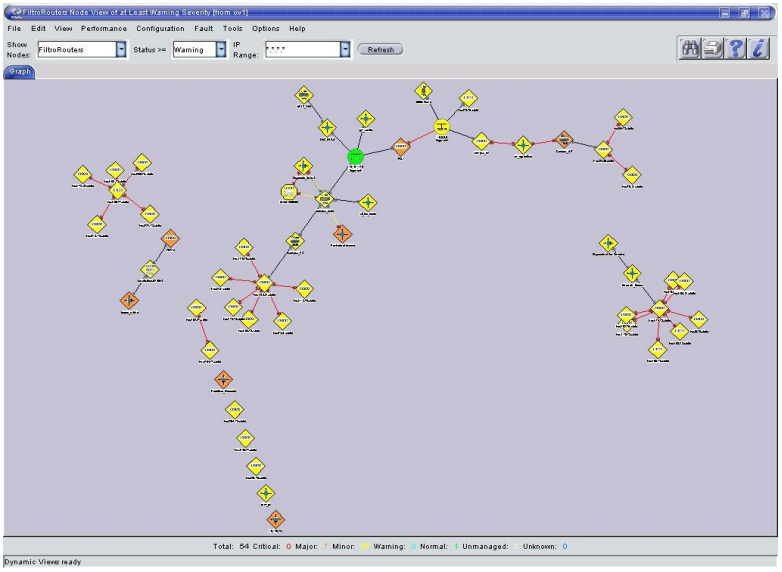

Figura 3.18 – Filtro su Home Base

Il secondo campo invece fa riferimento allo stato dell'oggetto, ovvero oggetti che hanno uno stato dello stesso livello o maggiore di quello selezionato, verranno visualizzati.

Il terzo campo è relativo all'ampiezza degli indirizzi su cui applicare la vista.

La differenza che prima risalta agli occhi, è la presenza di gran parte dei link nella vista dinamica e la totale assenza degli stessi nella vista statica del GUI. Si ricorda che le Dynamim View fanno riferimento al discovery dell'Extended Topology. Il processo interessato a questo discovery è l'`ovet_ disco`.

3.14 Sistema di rete

Viene ora preso in esame un sistema di reti complesso su cui è stato installato l'applicativo e su cui si sono attuate le politiche di monitoraggio personalizzato.

Tale sistema è strutturato, nel seguente modo:

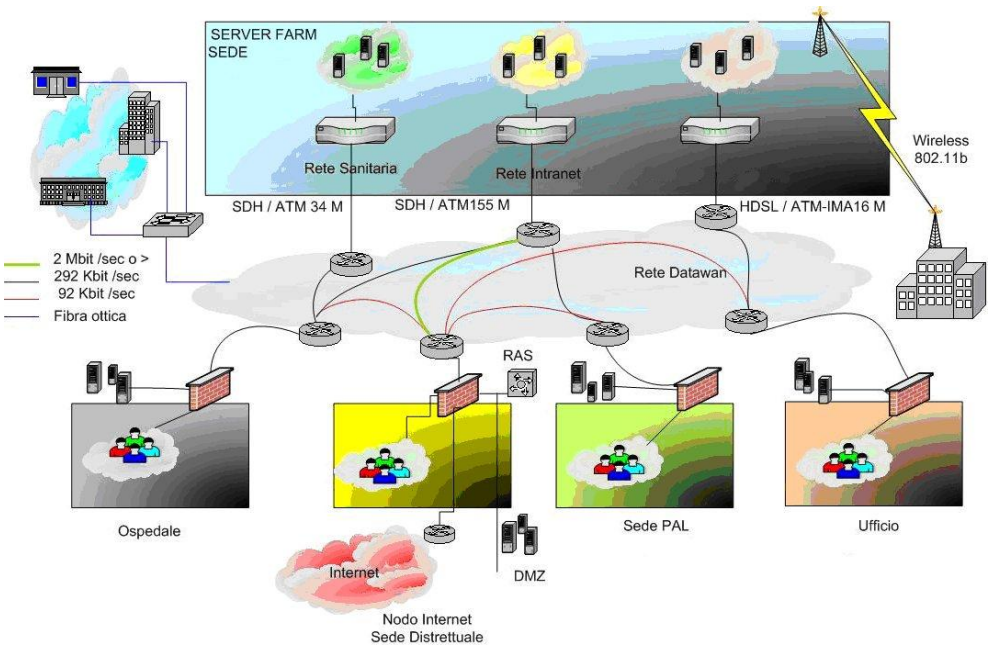

Figura 3.19 – Rete complessa generica

Come si può vedere dall'immagine sopra, la generica rete è composta da diverse reti, tra loro interconnesse. Se si guarda con attenzione si può notare che nella parte superiore c'è il vero "cuore" dei servizi della rete, ovvero la Server Farm. Questa è un insieme di server e dispositivi di controllo per la condivisione delle risorse di rete, finalizzata al rilascio dei servizi agli utenti che li richiedono. È presente in questa Server Farm anche un insieme di database di riferimento per gli applicativi remoti.

Per dare una migliore illustrazione del Server Farm, si veda la seguente immagine:

Figura 3.20 – Server Farm

Questa fa riferimento ad una generica infrastruttura proprietaria di rete geografica nel territorio per il collegamento delle PAL (Pubbliche Amministrazioni Locali), Enti, Organizzazioni e del Sistema Sanitario al fine di promuovere lo sviluppo dei sistemi di interoperabilità, ed applicativi e favorendo lo sviluppo della Società dell'Informazione tra Pubbliche Amministrazioni, con l'obiettivo di migliorare i servizi verso il Territorio

Per quanto riguarda le regole d'accesso alle porte di rete, si precisa che sono state standardizzate con l'adozione di un piano di indirizzamento e di regole di accesso ai servizi.

Si è provveduto ad implementare un piano di indirizzamento per reti private, utilizzando la classe 10.0.0.0[13] e strutturando la suddivisione dell'intero spazio in 32 aree di 512 blocchi di 1024 indirizzi ciascuno identificate con una numerazione da 0 a 31.

A ciascuna area geografica è stato assegnato una specifico blocco di indirizzi, si tratta quindi di assegnazione di indirizzi statici, al fine di monitorare e gestire meglio il sistema nel suo complesso.

All'interno di ciascuna area si è ulteriormente provveduto a suddividere gli indirizzi disponibili in sottoreti di distribuzione ed accesso di tipo condiviso o punto - punto; mentre alle Amministrazioni è stato assegnato un range di indirizzi sulla base della esigenze concordate secondo le seguenti tipologie: sottoreti locali di piccole sedi (256 indirizzi); sottoreti locali di grandi edifici

(1024 indirizzi); sottoreti locali sedi di dominio (4096 indirizzi).

All'interno del range assegnato ogni gruppo d'utenti ha predisposto il proprio piano di indirizzi.

Per ogni distretto è stato creato uno spazio di indirizzi per un'area DMZ.

Una DMZ (demilitarized zone) è un segmento isolato di LAN (una sottorete) raggiungibile sia da reti interne che esterne che permette, però, connessioni esclusivamente verso l'esterno: gli host attestati sulla DMZ non possono connettersi alla rete aziendale interna.

Una DMZ può essere creata attraverso la definizione di politiche distinte su uno o più firewall e a tal proposito si afferma che nell'area DMZ di ogni sede di distretto è installato un firewall per l'uscita Internet dei soggetti che ricadono esclusivamente all'interno dell'area.

3.15 Politiche di monitoraggio

Si descrive ora il concetto di politiche di monitoraggio che è l'argomento centrale di questa tesi e che necessita, per la sua comprensione ed attuazione della comprensione di tutti gli argomenti illustrati nei capitoli e paragrafi precedenti.

Definire una politica di monitoraggio vuol dire definire delle regole e delle scelte finalizzate al raggiungimento di determinati obiettivi.

Nel sistema di rete preso in esame in questa tesi, tali obiettivi riguardano la costruzione di filtri finalizzati alla limitazione del dominio amministrativo oggetto della gestione. Sono stati creati inoltre dei filtri che permettono un monitoraggio personalizzato per ciascun utente, limitandone la visualizzazione di nodi o reti in relazione al livello di autorizzazione con cui

si è avuto accesso.

I nodi principali, inizialmente filtrati, riguardano apparati chiave per il corretto funzionamento delle reti e precisamente sono:

- **Router:** sono gli apparati di rete più importanti. Attuano delle politiche di instradamento e filtraggio dei pacchetti che si ripercuote anche sul traffico e sulla sicurezza della rete
- **Switch:** sono dispositivi importanti che indirizzano i pacchetti sui giusti segmenti di rete mantenendo la banda totale per ogni host ad esso collegato; si dice in questo caso che ogni host ha un accesso dedicato
- **Pix:** sono firewall fisici della Cisco
- **Bridge:** sono dei dispositivi di rete ch dividono i domini di collisione e che instradano i pacchetti verso il segmento di rete giusto
- **Hub:** sono dei repeater multiporta che rigenerano il segnale
- **Server DNS:** sono dei server che traducono gli indirizzi IP in nomi e viceversa
- **Firewall**: sono dispositivi finalizzati alla sicurezza della rete

Il caso del sistema di rete di cui ci si sta occupando ha comportato l'attuazione di determinate politiche di monitoraggio che di seguito vengono illustrate:

- riguardo al **discovery:** attraverso tale procedimento si è proceduto all'immissione di un particolare filtro (FiltroDiscovery) che ha permesso di includere solamente i nodi principali suddetti e che conseguentemente sono stati monitorati, escludendo fin dall'inizio quelli superflui (ad es. escludendo i computer). Questa scelta è stata implementata onde evitare di raggiungere il numero massimo di nodi

maneggiabili disponibili secondo la licenza in uso. La politica che è stata attuata ha riguardato l'impostazione dei seguenti parametri:

- intervallo di discovery: ogni sette giorni
- eliminazione dei nodi non più connessi: dopo una settimana dall'ultimo ricevimento di messaggi da tali nodi
- Utilizzo del FiltroDiscovery come filtro per l'esclusione dei nodi non principali

- riguardo al **polling**: di default il polling riguarda tutti i dispositivi scoperti nella fase di discovery. Questo comporta un elevato traffico di rete in quanto viene effettuato ogni quattro ore. Ciò si deve al fatto che in una rete si possono collegare o scollegare apparati, modificando quindi i percorsi della rete stessa.
  Si è andati a personalizzare il processo di polling in funzione dell'importanza dei nodi. In questo senso si è scelto di monitorare con maggior frequenza gli apparati chiave specificando i loro indirizzi di rete e impostando l'intervallo di polling in sessanta minuti; per gli altri nodi l'intervallo è stata impostato in sei ore. Le informazioni raccolte serviranno poi per visualizzare un grafico con lo storico o in tempo reale dei dati che vengono scambiati

- riguardo ai **filtri**: sono un ottimo strumento per visualizzare solo ciò che si desidera e a tal proposito ne sono stati costruiti e implementati alcuni ad hoc per ciascun utente che abbia accesso al sistema. In questo senso si è voluto limitare l'accesso di utenti non autorizzati alla visualizzazione di determinate aree di rete al fine di aumentare la sicurezza del sistema stesso. A tal proposito è stato possibile disabilitare alcuni comandi di menu che non rientrassero nell'ambito delle politiche di accesso.

  È stato possibile creare dei filtri che andassero a visualizzare dispositivi specifici per ogni utente come:

- `FiltroRouter`: filtra i router, switch, hub e bridge
- `FiltroProvincia`: seleziona le reti appartenenti ad una specifica provincia visualizzandone la mappa degli apparati relative
- `FiltroSanita`: seleziona e visualizza i nodi più importanti che fanno parte del sistema sanitario regionale
- `FiltroFirewall`: seleziona le reti che hanno al loro interno i firewall
- `FiltroPersNet`: filtra le reti più importanti che sono alla base del funzionamento di tutto il sistema di reti interconnesse
- `FiltroServer`: filtra le reti che hanno i server al loro interno
- `FiltroPrinter`: filtra le stampanti dell'intera rete

- riguardo l'**utilizzo di altri comandi**: utilizzando il comando `ovtopofix` è possibile fare il filtraggio degli oggetti presenti nel database seguendo eventuali nuove politiche di filtro impostate nel discovery. Il vantaggio di questo comando sta nel fatto che si può aggiornare il database e le mappe senza eseguire nuovamente il discovery, ma semplicemente andando ad analizzare e escludere le singole entry del database. L'attuazione di tale comando non è stata necessaria in quanto si è scelto di applicare il filtro per il discovery iniziale, escludendo fin dall'inizio i nodi non primari.
- riguardo gli **allarmi**: fra tutti gli eventi disponibili, che generano un allarme, sono stati impostatati quelli relativi al corretto funzionamento di un nodo. Si va a ricevere una notifica via email solo quando i nodi impostati non sono più attivi: questo succede quando vengono disabilitate tutte le interfacce di un nodo, cioè

quando il nodo non comunica più con la rete. La politica scelta per questa tipologia di eventi è stata implementata con l'aggiunta di uno script (msgsend.exe), per l'invio selettivo delle email con un oggetto e un testo che vengono predisposti secondo dei parametri impostati. Si veda di seguito un esempio chiarificatore:

Per inviare tali messaggi ai destinatari designati, si è proceduto nel seguente modo:

- dall'Alarm Browser si sono scelte le tipologie di eventi che si desiderava fossero inoltrate
- si è proceduto all'impostazione dell'invio della categoria di evento `OV_Node_Down` inserendo la stringa corrispondente nel campo `Command for Automatic Action`. La stringa è stata preceduta in tutti i casi da `msgsend.exe`. Questo significa che viene richiamato tale script e gli viene passata la seguente sequenza di caratteri:

  IP_$2_Node_Down Node_Down_Capabilities_$8_Root_Cause:_$9_$10

  Per capire meglio utilizziamo di seguito uno screenshot:

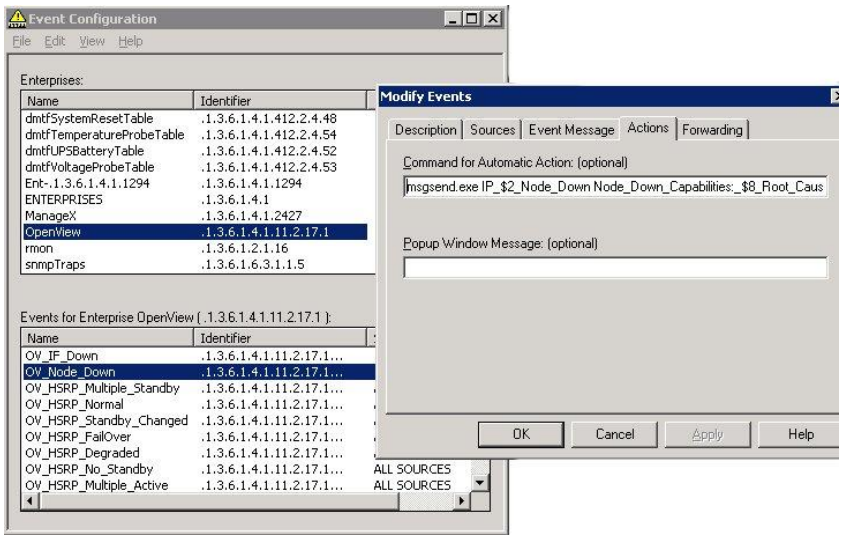

Figura 3.21 – Stringa msggsend.exe

I parametri di tale stringa hanno una propria corrispondenza nel database (ad es. $2 corrisponde alla colonna degli indirizzi IP situata nel database). Il simbolo "_" viene interpretato dallo script come uno spazio " ". Come si può notare, la stringa contiene un solo spazio, questo fa sì che lo script interpreti come oggetto dell'email il testo presente fra msgsend.exe e lo spazio suddetto; ciò che è messo dopo lo spazio viene interpretato come il testo dell'email. In questo testo viene elencato il tipo di problema riscontrato e ciò che lo ha causato.

In definitiva, la stringa sopra immessa corrisponderà al seguente messaggio email:

Oggetto: `IP 10.101.12.1 Node Down`

Testo:
```
Node Down Capabilities:
isIPRouter,isSNMPSupported,isRMON,isFra
meRelay,isSONET,isATM,isCDP,isOSPF,isBG
P4,isVRRP Root Cause: 88.35.101.24 Nu0
```

- accedendo ad un indirizzo email fra quelli impostati si vedrà tale messaggio con l'oggetto suddetto.

3.15.1 Esempio di monitoraggio

Si fornisce ora un esempio di monitoraggio in cui si è esaminato un nodo gateway e prendendo in esame i pacchetti IP ricevuti in un intervallo di tempo di cinque minuti.

Questo monitoraggio può essere visionato graficamente e assume la forma seguente:

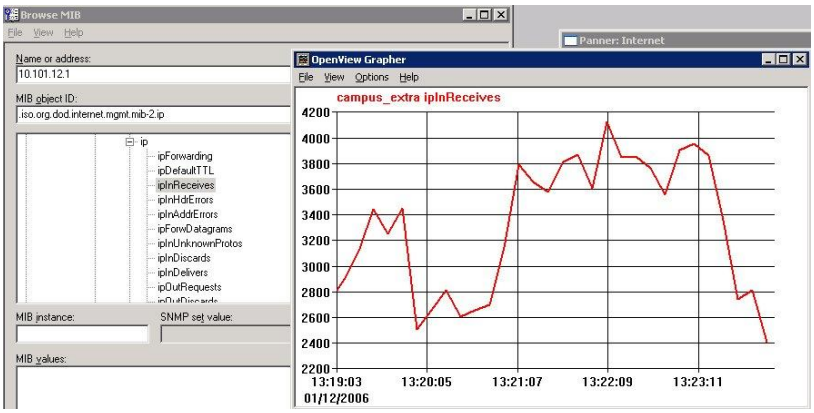

Figura 3.22 – SNMP MIB

Come si può vedere viene preso in esame il nodo 10.101.12.1 e attraverso l'immissione della corretta community name si possono avere, come detto, informazioni attraverso il protocollo SNMP. Queste informazioni aiutano l'administrator ad attuare variazioni sulle politiche di monitoraggio già esistenti o a prendere in esame un'eventuale installazione di nuovi collegamenti che garantiscano una banda maggiore al fine di non congestionare la rete.

Conclusioni

Analizzando il funzionamento del software di Network Management, HP OpenView Network Node Manager, e implementandone la costruzione di mappe dinamiche, filtri e configurazioni correlate ci si è resi conto che si è utilizzato un applicativo di ampia portata. Questo però comporta anche un grande dispendio di tempo finalizzato allo studio del prodotto, dei processi e dei comandi.

Le configurazioni non sono di semplice impostazione e richiedono, anch'esse, un impiego importante di tempo.

Per quanto riguarda le mappe statiche del GUI bisogna precisare che nella prossima versione di tale software, la 8.0, si è pensato di trasferire tutte le interfacce sul web, in modo da facilitare la visualizzazione dinamica delle mappe e altre peculiarità attualmente presenti solo su Home Base o Web Launcher.

Concludendo si può affermare che NNM è un applicativo molto potente e complesso che necessita di un adeguato studio e applicazione pratica sin dalle fasi iniziali.

Ringraziamenti

Desidero innanzitutto ringraziare tutta la mia famiglia, che nel percorso che mi ha portato sin quì mi ha dimostrato sempre amore e comprensione. Ringrazio per la disponibilità e gentilezza il mio relatore, Dott. Fausto Marcantoni, e in particolar modo la mia correlatrice, la Dot.ssa Maria Laura Maggiulli, che mi ha sempre aiutato nonostante i suoi numerosi impegni.
Desidero infine ringraziare i compagni e gli amici che mi sono stati vicini e in particolar modo Stefano, che anche nei momenti difficili mi ha sempre dimostrato la sua profonda amicizia.
Infine ringrazio tutte le persone che mi sono state vicine e che mi hanno incoraggiato e sostenuto per raggiungere questo obiettivo.

Bibliografia

[1] RFC 1321

[2] RFC 3139

[3] T. Saydam, T. Magedanz "*From Networks and Network Management into Service and Service Management*", Journal of Network and System Management, 1996

[4] Kurose J. F., Ross K. W. "*Internet e Reti di Calcolatori*", Seconda Ed., 2003

[5] RFC 2788 - Network Services Monitoring MIB

[6] RFC 793

[7] RFC 768

[8] ISO 7498

[9] RFC 1180

[10] RFC 826

[11] RFC 903

[12] RFC 792, RFC 1788, RFC 1345, RFC 2521

[13] RFC 1132

[14] RFC 1450, RFC 1451, RFC 1452

Altre fonti bibliografiche

Hewlett-Packard Development Company , *"Managing Your Network with HP OpenView Network Node Manager"* 2003

Hewlett-Packard Development Company, *"A Guide To Scalability and Distributionfor HP OpenView Network Node Manager"*

Tananbaum A., *"Reti di calcolatori"*, Quarta ed., 2003

Siti Internet

www.wtcs.org/snmp4tpc/jton.htm

www.iso.org

www.ietf.org

www.wikipedia.org

www.hp.com