Università degli studi di Pisa

Sistemi di elaborazione dell'informazione:
gestione di rete

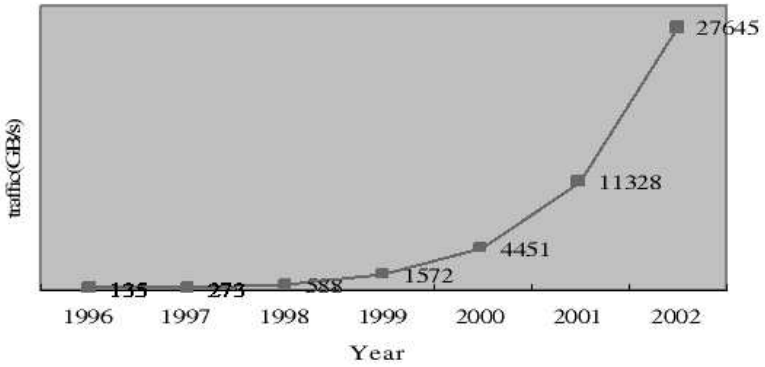
DEFINIZIONE DI UN MIB PER UNA SONDA DESTINATA ALL 'ANALISI DEL TRAFFICO DI SOTTORETI.

Michele Girolami
girolami@cli.di.unipi.it

Indice:

1-INTRODUZIONE

Il crescente sviluppo delle reti ha coinciso con una forte necessita' di monitorare ed analizzare il traffico prodotto , ovvero osservare e tenere traccia di cio' viene trasmesso su una rete.



Source: America's Network

Come si puo' osservare dal grafico precedente , negli ultimi 6 anni (1996-2002) il volume di traffico Internet e' aumentato enormemente .In una situazione di questo tipo risulta essenziale avere degli strumenti in grado di analizzare il traffico .
Secondo l'RFC 2063(Traffic Flow Measurement :Arichitecture), gli obiettivi della misurazione del traffico sono:

-comprendere il comportamento di reti esistenti
-pianificare una possibile espansione della rete
-quantificare le performance di rete
-verificare la qualita' dei servizi di rete
-attribuire l'uso della rete agli utenti

Nell'ottica di un'azienda raggiungere questi obiettivi coincide con un miglioramento generico delle prestazioni della propria rete ovvero con un migliore investimento delle risorse.Ecco perche' negli ultimi anni la ricerca nel campo della misurazione del traffico di rete ha fatto notevoli progressi.
Sflow(http://www.sflow.org/sFlowOverview.pdf) ha realizzato un grafico che mostra come negli ultimi 10 anni circa si sia passato da una misurazione del traffico fatta sul campionamento dei pacchetti di reti a 10Mbit ,fino ad un monitoraggio del traffico in ambiente switched su reti a 10Gb riducendo l'impatto sulle prestazioni.

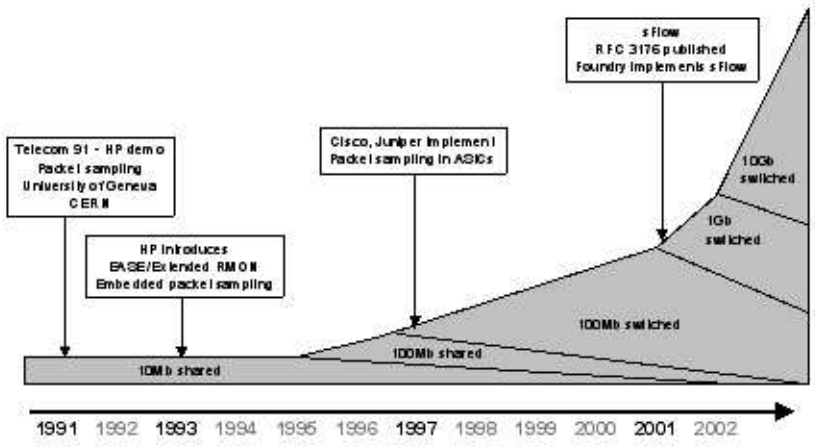


Figure 1 *History of Packet Sampling*

Un tipico modello architetturale per il monitoraggio di rete consiste nel predisporre una serie di apparati in grado ciascuno di compiere alcune attivita' utili alla produzione di statistiche crica l'andamento della rete.

1)Meter : il meter e' una sonda il cui compito e' quello di collezionare una serie di attributi , aggregarli insieme e mantenerli in un'apposita struttura dati(Flow Table) .Alcuni di questi attributi possono essere : numero di pacchetti con un certo source address e destination address, numero di pacchetti con un particolare protocollo ecc.
Le sonde vengono configurate dai manager (vd definizione successiva) , ed ogni sonda lavora con una propria configurazione settata.
I meters possono essere apparati di reti a se' stanti , oppure inegrati all'interno di router o switch. Uno degli aspetti critici del traffic measurement e' la collocazione di queste sonde , infatti posizionarle in punti non andatti porta ad una visione distorta dell'andamento di una rete.

2)Manager : un manager e' un'applicazione che gestisce e configura uno o piu' meters e meter-reader. Il manager sceglie una configurazione appropriata per il meter e provvede a comunicarla all'apparato.

3)Meter Reader : questa componente raccoglie i dati catturati dalla sonda , per passarli poi ad un' analysis application (vd. Definizione successiva).

4)Analysis Application : questa applicazione ha il compito di processare i dati raccolti dalla sonda , e provvedere a realizzare resoconti utili per " gli scopi di gestione , e per il network engineering. Alcuni esempi possono essere :
-Traffic flow measurement.
-Flow rate frequency distributions.
-Usage data."[1]

1 RFC: 2063 Traffic Flow Measurement:Architecture N.Brownlee, C.Mills, G.Ruth

2-DEFINIZIONE DI UNA SONDA

Come precedentemente detto una sonda e' un apparato di rete in grado di collezionare informazioni circa il traffico di rete .
Una sonda puo' essere un appararto indipendente quindi una macchina dedicata al collezionamento , oppure puo' essere integrata all'interno di altri apparati di rete(Router, Swicth) .

Il suo funzionamento puo' essere riassunto in 6 punti:

1)Arrivo dell'header di un pacchetto ed inoltro al PACKET PROCESSOR.

2)Il PACKET PROCESSOR inoltra l'header al PME (Packet Matching Engine, ovvero una Virtual Machine che confronta i pacchetti con regole impostate) ,il quale lo analizzera'.

3)Il PME confronta il pacchetto con l' insieme di regole attualmente utilizzate dalla sonda , quindi produce una un risposta che dice cosa fare con il pacchetto ricevuto.

4)Alcuni di questi pacchetti verranno scartati .

5)Altri invece vengono mantenunti dal PME che ritornera' una FLOW KEY (indice) che identifica il flusso al quale appartiene il pacchetto ricevuto.

6)La FLOW KEY serve per localizzare il flusso relativo al pacchetto ricevuto , se non e' presente un flusso per quel pacchetto allora verra' creato.

La sonda utilizza due strutture dati per mantenere informazioni circa i traffici:

Flow Table : array contenente una serie di Flow Entry
Flow Entry : una cella dell'array che descrive un flusso esistente.

Rule Table : array che contiene Rule Entry
Rule Entry : una cella dell'array che contiene un insieme di regole applicabili.

Si noti che sia la Flow Table , che la Rule Table sono dinamiche , ovvero possono crescere dinamicamente nel tempo. La Flow Table puo' aggiungere una entry se la sonda ha trovato un nuovo flusso, mentre la Rule Table puo' aggiungere una cella per caricare un nuovo set di regole.

2.1-I FLUSSI

Un flusso e' una sequenza di pacchetti aventi una serie specificata di attributi simili.
L'aggregazione per flussi e' un ottimo strumento per caratterizzare una sequenza di pacchetti, queste aggregazioni si possono fare su ogni tipo di attributo:

-Inidirizzo sorgente e destinazione del flusso , questi due parametri sono essenziali per inidividura uno specifico stream di pacchetti.
-Istante in cui il pck si e' visto per la prima e ultima volta in un flusso.
-L'indirizzo fisico dell'interfaccia di rete dalla quale proviene il flusso , o alla quale e'

destinato.
-protocollo utilizzato.

Un esempio di flusso puo' essere il traffico http dall'host 192.168.1.1 e indirizzo fisco aa:aa:aa:aa:aa:aa all'host 192.168.1.2 con indirizzo fisico bb:bb:bb:bb:bb:bb

Un flusso creato deve avere uno dei 3 stati seguenti:

1-Inattivo : la flow record relativa al flusso non viene piu' usata dalla sonda
2-Attivo : la flow record e' usata dalla sonda quindi subisce periodiche modifiche.
3-Idle : la flow record e' usata dalla sonda , ma per un certo periodo di tempo il PME non ha riscontrato pacchetti appartenenti a questo flusso.

Inoltre i flussi vengono generalmente considerati bidirezionale , ovvero un pacchetto da A->B con gli attributi x,y,z appartiene allo stesso flusso del pacchetto che viaggia da B->A con gli attributi x,y,z. Questo fatto complica un po' le cose , ovvero la soda sara' tenuta ad accorgersi di pacchetti di risposta e quindi non dovra' creare un nuovo flusso.

2.2-LE REGOLE

Una regola e' una condizione da testare ogni volta che la sonda riceve un pacchetto , ogni sonda contiene un insieme di regole applicabili , sara' compito del manager comunicare al meter quale insieme di regole utilizzare ; questo fatto permette alla sonda di essere flessibile alle varie esigenze di chi sta controllando la rete.

Una regola puo' essere vista come una tupla

$$R_i=(A_i,M_i,V_i,C_i,P_i)$$

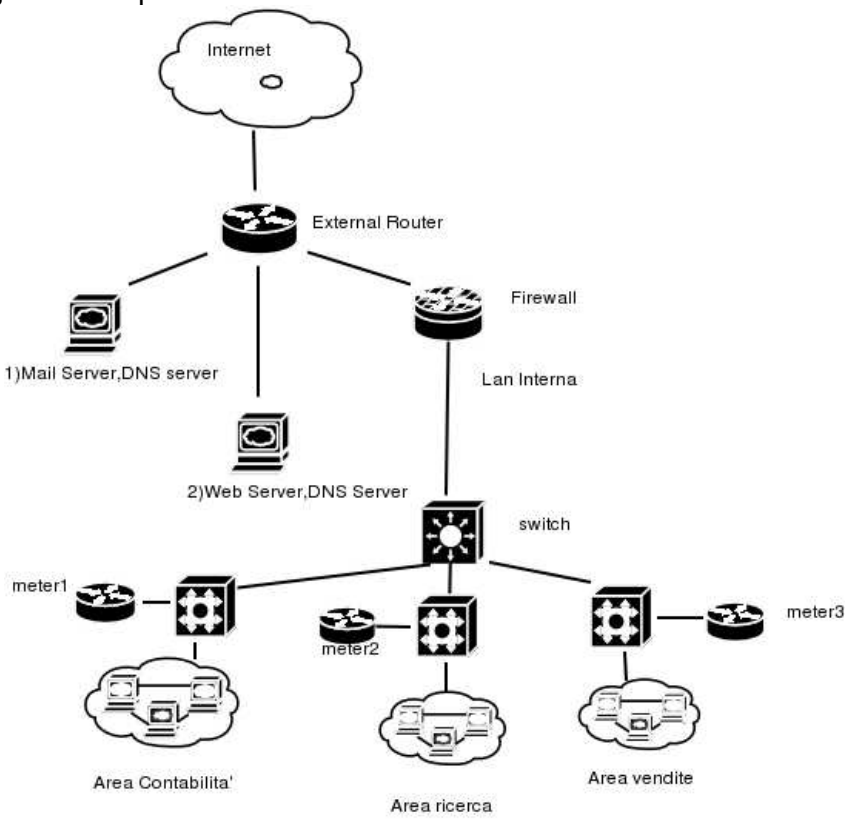
Per ogni regola si calcola il valore dell'attributo A_i con la maschera M_i e il risultato e' confrontato con il valore V_i. Se il due valori non sono identici , si passa alla regola successiva.Se invece i valori sono uguali si esegue l'azione C_i con i parametri P_i.

Come precedente detto il PME e' una virtual machine che prende in ingresso un insieme di regole, e decide quale azione prendere. Alcune azioni sono :

-ignore : si ignora il pacchetto e si aspetta il successivo
-fail : si e' verificato un errore nella fase di matching, quindi si aspetta il pck successivo.
-count : si salvano le informazioni utili sul pacchetto , il PME genera una indice (Flow Key) che servira' per aggiornare il flusso relativo al pacchetto.

3-CASO DI STUDIO

Questa sezione provvede a definire una possibile situazione in cui si presenta la necessita' di introdurre una sonda per il monitoraggio di una rete.
Qui di seguito viene presentato un modello di rete:



La ditta presa in esame , ha :
1)un server di posta elettronica con i seguenti servizi:
dns,smtp
2)Un server web che eroga i seguenti servizi:
dns,http,https,ftp

3)Un firewall per dividere la rete pubblica da quella interna, il firewall mette a disposizione per l'amministrazione solo un server ssh.
All'interno della LAN ci sono tre aree distinte e delimitate da un packet filter con ACL impostate.

Ogni area ha un suo compito nell'econimia della ditta e quindi un relativo tipo di traffico generato:

Area ricerca:e' l'area piu' attiva , ovvero quella che genera un maggior volume di traffico.
L'area e' delimitata da un packet filter che filtra il traffico da e per il settore ricerca , quindi in questo punto andra' collocata una sonda per intercettare tutto il traffico prodotto. Da questo settore ci si aspettano l'uso dei seguenti protocolli:

http,https,dns,ftp,ssh, telnet, smtp,scp,mysql,imap,pop3.

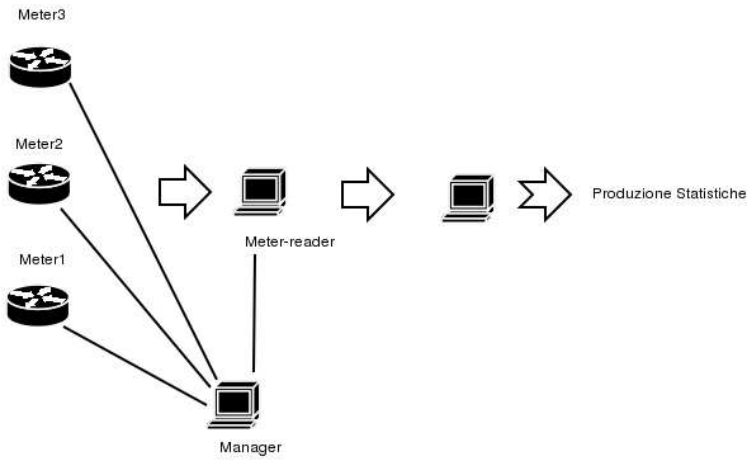
Area vendite : quest'area e' destinata alle vendite con il pubblico , quindi si prevede che generi assai meno traffico della precedente area e che utilizzi un numero di servizi molto ridotto qui andra' piazzata una seconda sonda , in particolare i servizi usati saranno :
http,ftp,https, smtp,pop3,imap

Area contabilita' :il suo scopo e quello di tenere aggiornata la contabilita' della ditta. Anche in questo caso , un packet filter si preoccupa di gestire il traffico , da e per il settore.
I servizi usati saranno
1)http, https, ftp,dns,mysql

I servizi elencati sfruttano la tecnologia Ip over Ethernet , quindi la sonda catturera' solo questo tipo di traffico.

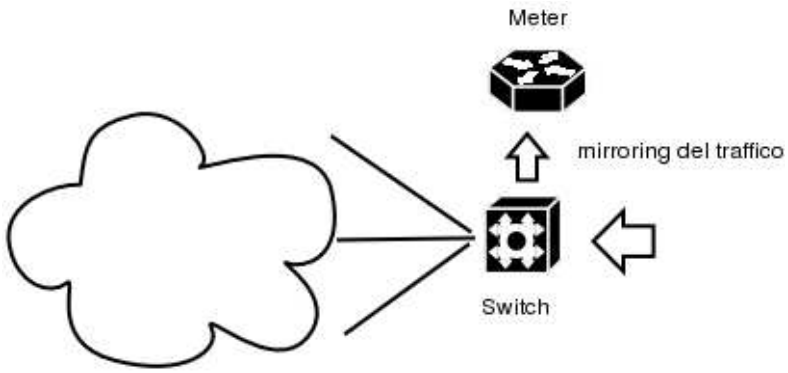
3.1-ARCHITETTURA DELLE SONDE

Le tre sonde catturano informazioni sui traffici delle tre aree, li aggregano in flussi e garantiscono l'accesso alla risorsa a tutti e soli gli utenti autorizzati , il meter-reader periodicamente andra' a prelevare i dati raccolti e li inviera' ad un'applicazione di analisi che produrra' statistiche riassuntive.Il Manager invece ha il compito di gestire sia i meters , che i meter-reader.
Le comunicazione tra i meter ,meter-reader e il manager , vengono fatte utilizzando il protocollo snmp.



3.2-DESCRIZIONE DELLA SONDA:

La sonda e' organizzata in tre parti, ogni sezioni provvede a definire variabili che gestiscono un particolare aspetto della sonda.
Assumo che la sonda riceva il segnale attraverso un meccanismo di Port Mirroring , ovvero uno switch copia tutto il traffico proveniente da una porta su di un 'altra



1)Controllo : questa sezione e' dedicata unicamente al controllo della sonda , qui sotto vengono descritte alcune variabili utili ad aquisire informazioni sullo stato della sonda e sulle interfaccie presenti a bordo della stessa.

--Le variabili relative allo stato della sonda e alle interfaccie di rete presenti vengono definite nel *mibII RFC 1213*

probeMIB: info generali sul MIB
sysDescr: Descrizione dell'apparato di rete.
sysUpTime: il tempo che e' trascorso dall'ultima volta che la sonda e' stata inizializzata.
sysConcact: fornisce un recapito per il gestore della sonda
sysName: fornisce un nome per la sonda
sysLocation : descrive la locazione fisica della sonda.
SysServices: variabile espressa come una bitmask che indica il/i servizo/i che fornisce la sonda , inizialmente e' uguale a 0 , per ogni servizio che la sonda implementa si setta un bit ad 1 .I livelli sono:

1 physical (e.g., repeaters)
2 datalink/subnetwork (e.g., bridges)
3 internet (e.g., IP gateways)
4 end-to-end (e.g., IP hosts)
5 applications (e.g., mail relays)

meterReaderTable : tabella che descrive i meter readers (MR) collegati alla sonda.Una sonda infatti puo' avere piu' meter reader collegati che aquisiscono informazioni.Questa tabella e' una sequenza di meterReaderEntry
meterReaderEntry :cella che descrive un MR
meterReaderIndex: indice del MR nella tabella
meterReaderPhysAddress :indirizzo fisico del MR
meterReaderAddress : indirizzo del MR.
meterReaderMaskAddress: maschera di rete del MR.
meterReaderLastRead : indica il tempo di ultimo accesso del MR alla sonda
meterRaederNote : informazioni extra.

ifTable: sequenza di ifEntry , per elencare e descrivere le interfaccie di rete presenti nella sonda.Una sonda infatti puo' avere piu' interfaccie di rete collegate .
IfEntry:cella che descrive le interfaccie di rete presenti sulla sonda :
ifDescr: descrizione dell'interfaccia(marca , chipset montato ..)
ifType: tipo dell'interfaccia , ovvero quale tecnologia usa
ifIndex : Indice dell'interfaccia di rete.
ifMtu: MTU dell'interfaccia, ovvero la dimensione massima di un datagram.
ifSpeed: velocita' dell'interfaccia espressa in bit/sec
ifPhysAddress: indirizzo fisico dell'interfaccia .Ad esempio se l'interfaccia di rete usa una teconologia ethernet l'indirizzo fisico sara' il mac-address.
ifAdminStatus: indica lo stato dell'interfaccia .Un'interfaccia si puo' trovare esclusivamente in uno dei seguenti stati: UP, DOWN ,TESTING.
ifInOctets :Indica il numero totali di ottetti ricevuti dall'interfaccia.
ifInUcastPkts: Indica il numero di pacchetti unicast ricevuti dall'interfaccia .
ifNUcastPkts: Indica il numero di pacchetti non unicast ricevuti dall'interfaccia.
ifInDiscards: Indica il numero di pacchetti ricevuti in ingresso "sintatticamente " corretti ,ma scartati dall'interfaccia.Una causa possibile puo' essere la saturazione del buffer di ricezione.
ifInErrors :Indica il numero di pacchetti ricevuti , ma malformati.
ifInUnknownProtos: Indica il numero di pck con protocollo sconosciuto
ifOutOctets : Indica il numero di otteti spediti
ifOutUcastPckts: indica il numero di pacchetti unicast inviati
ifOutNUcastPckts: indica il numero di pacchetti non unicast inviati
ifOutDiscards: Indica il numero di pacchetti da spedirte , ma scartati .Una possibile causa puo' essere la saturazione del buffer .
ifOutErrors :Inidca il numero di pacchetti che non possono essere spediti perche' contenenti errori.

2)Flussi : questa sezione provvede a descrive i flussi , in particolare la sonda mantiene un flowTable con flowEntries , ogni entry ha alcuni campi che descrivono il flusso .
flowTable : Tabella che contiene flowEntry che descrivono i vari flussi prodotti.
flowEntry: Cella che descrive un flusso prodotto , questa cella e' composta da vari campi:
flowIndex :Indica la posizione della cella all'interno della tabella dei flussi
flowStatus :Indica lo stato del flusso.Un flusso puo' trovarsi esclusivamente in uno dei seguenti stati : attivo,inattivo,idle.

--Insieme di variabili per descrivere la sorgente dei dati ricevuti , ovvero informazioni relative all' interfaccia di rete della sonda dalla quale proviene lo stream di dati(Una sonda puo' avere a bordo piu' interfaccie di rete) e informazioni relative al peer che ha inviato i dati.

flowSourcePhysType : Specifica il tipo dell'interfaccia sorgente della sonda, ovvero quale tecnologia utilizza la scheda di rete.
flowSourceInterface:indice dell'interfaccia di rete della sonda dalla quale proviene il flusso.
flowSourcePhysAddress : Indirizzo fisico della relativa interfaccia di rete da cui proviene il flusso
flowSourcePeerPhysAddress: Indica l' inidrizzo fisico del peer che ha prodotto il

flusso
flowSourcePeerAddress: Inidca l' indirizzo del peer che ha prodotto il flusso
flowSourcePeerMask: Indica la relativa maschera di rete.

--Insieme di variabili che descrivono la destinazione dei dati ricevuti , ovvero informazioni relative al peer destinatario per lo stream di dati. A differenza del precedente set di variabili , qui non e' necessario definire variabili per descrive la scheda di rete della sonda alla quale e' destinato il flusso di dati, infatti si assume che la sonda riceva passivamente il segnale(attraverso un meccanismo di port mirroring) senza fare il forwarding dei pacchetti.

flowDestPeerType: Indica il tipo di indirizzo del peer che ha prodotto il flusso.
flowDestPeerPhysAddress :Indica l'indirizzo fisico del peer destinatario del flusso.
flowDestPeerAddrss:Indica l'indirizzo del peer destinatario per il flusso
flowDestPeerMask: Indica la relativa machera di rete

flowRuleSet: Numero della regola che crea questo flusso

flowToOctect :Indica il numero di ottetti che transitano dalla sorgente alla destinazione per questo flusso.
flowFromOctect :Indica il numero di ottetti che trasnitano dalla destinazione alla sorgente per questo flusso

3)Regole , questa sezione si preoccupa di definire le regole sulla sonda. Anche in questo caso viene utlizzata una tabella per contenere gli insiemi di regole

ruleTable: tabella contenente insiemi di regole(RuleSets) , il meter puo' usare differenti insiemi di regole selezionati dal Manager.La tabella contiene delle ruleEntries che descrivono le regole da applicare.

ruleEntry : Cella che contiene informazioni circa le regole da utilizzare , e' composta da una sequenza di attributi:
ruleSet : Indica l'insieme di regole utililizzato
ruleParser: indica l'attributo da controllare ogni volta che il meter riceve dei dati.Questo valore indica quindi cio' che veine "osservato" per ritenere una regola verificata.Puo' assumere i seguenti valori:

sourceInterface
sourcePhysAddress
sourcePeerPhysAddress
sourcePeerAddress

--destinazione
destPeerPyhsAddress
destPeerAddress

ruleAction : Indica l'azione da prendere qualora la regola sia soddisfatta:
ignore : ignora

count tiene traccia dei dati
countPck incrementa di pacchetti
return ritorna
assign assegna un certo valore
goto passa ad un 'altra regola

ruleParameters : info extra sulla regola.

4)Trap: Questa sezione definisce le possibili trap che il meter puo' inviare (in seguito ad un particolare evento) ad un meter-reader.
ifDown : inviata quando una delle interfaccie di rete presenti sulla sonda va giu'.Il meter quindi non puo' piu' ricevere alcun tipo di segnale . *Contiene:ifIndex (indice dell'interfaccia).*

ifUp :inviata quando una delle interfaccie ritorna ad essere funzionanate .
Contiene: ifIndex (indice dell'interfaccia).

HighPckDropped: inviata quando la sonda sta scartando un eccessivo numero di pacchetti , questo puo' essere determinato da varie cause .*Contiene :ifIndex(indice dell'interfaccia che scarta i pck)*

NoMeterRaederFound : inviata quando la sonda non viene interpellata da nessun meter reader per piu' di un certo periodo di tempo .
Contiene :MeterReaderIndex(Indice del MeterReader)

L'albero ISO e' organizzato in 4 rami:
1)systemProbe in cui rientrano le variabili di controllo della sonda
2)flowProbe in cui rientrano le variabili di controllo dei flussi
3)ruleProbe in cui rientrano le variabili che controllano le regole per i flussi
4)trapProbe in cui rientrano le variabili che controllo le traps

3.3-MIB

```
PROBE-MIB DEFINITIONS ::= BEGIN
IMPORTS
        MODULE-IDENTITY,
        NOTIFICATION-TYPE ,OBJECT-TYPE,
        Counter64,Integer32,TimeTicks, mib-2
                FROM SNMPv2-SMI
        TEXTUAL-CONVENTION
                FROM SNMPv2-TC
        ifIndex
                FROM IF-MIB;

probeMIB MODULE-IDENTITY
        LAST-UPDATED "0307091000Z"
        ORGANIZATION "University of Pisa"
        CONTACT-INFO
                "Michele Girolami , girolami@cli.di.unipi.it"
        DESCRIPTION "definizione di un Mib per la gestione di una sonda
                     destinata all'analisi del traffico di rete"
        ::={private 100}

--Definizione dei vari rami dell'albero

systemProbe         OBJECT IDENTIFIER ::={probeMIB  1}
flowProbe           OBJECT IDENTIFIER ::={probeMIB  2}
ruleProbe           OBJECT IDENTIFIER ::={probeMIB  3}
trapProbe           OBJECT IDENTIFIER ::={probeMIB  4}

--textual convention

PhysType ::=TEXTUAL-CONVENTION
        STATUS current
        DESCRIPTION
        "Indica il tipo della sorgente ,ovvere quale teconologia viene usata
        qui sotto sono riportati i 3 tipi che la sonda e' in grado di riconoscere."
        SYNTAX INTEGER{

        other(1), -- none of the following regular1822(2),
        hdh1822(3),
        ddn-x25(4), rfc877-x25(5),
        ethernet-csmacd(6),
        iso88023-csmacd(7),
        iso88024-tokenBus(8),
        iso88025-tokenRing(9),
         iso88026-man(10),
        starLan(11),
        proteon-10Mbit(12),
        proteon-80Mbit(13),
        hyperchannel(14),
```

```
                fddi(15),
                lapb(16),
                sdlc(17), ds1(18),
                -- T-1 e1(19),
                -- european equiv. of T-1 basicISDN(20),
                primaryISDN(21),
                -- proprietary serial propPointToPointSerial(22),
                ppp(23),
                softwareLoopback(24),
                eon(25)
                -- CLNP over IP [11] ethernet-3Mbit(26), nsip(27),
                -- XNS over IP slip(28),
                -- generic SLIP ultra(29)
                -- ULTRA technologies ds3(30),
                -- T-3 sip(31),
                -- SMDS frame-relay(32)
                }


PhysAddress ::= TEXTUAL-CONVENTION
                STATUS current
                DESCRIPTION
                "Specifica il valore dell'indirizzo fisico dei pacchetti ricevuti,ad esempio
                puo' essere un indirizzo MAC di 6 byte, gli indirizzi fisici ammessi.
                "
                SYNTAX OCTET STRING(SIZE (3..20))

PeerType ::=TEXTUAL-CONVENTION
                STATUS current
                DESCRIPTION
                "Descrive il tipo del Peer che sta inviando o ricevendo dati, i tipo
                ammessi sono:"
                SYNTAX INTEGER{
                ipv4(1),
                ipv6 (2),
                appletalk(3),
                nsap(4),
                ipx(5)  }


FlowAddress ::= TEXTUAL-CONVENTION
                STATUS current
                DESCRIPTION
                "Indica l'indirizzo del peer che sta inviando o ricevendo dati "
                SYNTAX OCTET STRING (SIZE (3..20))


Parser ::=TEXTUAL-CONVENTION
                STATUS current
                DESCRIPTION
```

```
                "Inidca l'attributo da testare all'interno di una regola.Sono stati inseriti
                attributi per testare una regola in base alla : sorgente , destinazione ,
                protocollo trasportato"
                SYNTAX INTEGER {
                null (0),

                --sorgente
                sourceInterface(1), --interfaccia della sonda dalla quale proviene lo strem
                sourcePhysAddress(2), --indirizzo fisico di una delle interfaccie della
                sonda
                sourcePeerPhysAddress(3), --indirizzo fisico del peer che ha generato il
                traffico
                sourcePeerAddress(4),  --indirizzo del peer che genera traffico

                --destinazione
                destPeerPyhsAddress(5), --indirizzo fisico del peer  destinatario del
                traffico
                destPeerAddress(6)  --indirizzo del peer destinatario del traffico


                }

Action ::= TEXTUAL-CONVENTION
                STATUS current
                DESCRIPTION
                "Elenco delle possibili azioni che si possono prendere ogni volta che una
                regola viene soddisfatta."
                SYNTAX INTEGER {
                ignore(1),              --ignora
                count(2),               --tiene traccia dei dati
                countPck(3),                    -- incrementa di pacchetti
                return(4),              --ritorna
                assign(5),              --assegna un certo valore
                goto(6)                 -- passa ad un 'altra regola
                }

--systemProbe

meterReaderTable OBJECT-TYPE
                SYNTAX SEQUENCE OF MeterReaderEntry
                MAX-ACCESS not-accessible
                STATUS current
                DESCRIPTION
                "Array che colleziona dati su meter reader collegati alla sonda;
                 l'array e' formato da MeterReaderEntry "
                ::={systemProbe 1}

meterReaderEntry OBJECT-TYPE
                SYNTAX MeterReaderEntry
                MAX-ACCESS not-accessible
                STATUS current
```

```
        DESCRIPTION
        "Entry con Informazioni sui meter-reader"
        INDEX {meterReaderIndex }
        ::={meterReaderTable 1}

MeterReaderEntry
        ::= SEQUENCE {
        meterReaderIndex                Integer32,
        meterReaderPhysAddress                  PhysAddress,
        meterReaderAddress              FlowAddress,
        meterReaderMaskAddress                  FlowAddress,

        meterReaderLastRead             TimeTicks,
        meterReaderNotes                OCTET STRING

        }

meterReaderIndex OBJECT-TYPE
        SYNTAX Integer32 (1..2147483647)
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
        "Indice del meter-reader collegato alla sonda"
        ::={meterReaderEntry 1}

meterReaderPhysAddress OBJECT-TYPE
        SYNTAX PhysAddress
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
        "Indica l'indirizzo fisico del meter-reader"
        ::={meterReaderEntry 2}


meterReaderAddress OBJECT-TYPE
        SYNTAX  FlowAddress
        MAX-ACCESS read-only
        STATUS   current
        DESCRIPTION
        "Indica l'indirizzo del meter-reader"
        ::={meterReaderEntry 3}

meterReaderMaskAddress OBJECT-TYPE
        SYNTAX FlowAddress
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
        "Indica la maschera di rete per il meter-reader"
        ::={meterReaderEntry 4}

meterReaderLastRead OBJECT-TYPE
```

```
                SYNTAX TimeTicks
                MAX-ACCESS read-only
                STATUS current
                DESCRIPTION
                "Indica il tempo di ultimo accesso del meter-reader alla sonda"
                ::={meterReaderEntry 5}


meterReaderNotes OBJECT-TYPE
                SYNTAX OCTET STRING (SIZE (4..20))
                MAX-ACCESS read-only
                STATUS current
                DESCRIPTION
                "Note varie sul meter-reader utili per un corretto funzionamento della
                        sonda"
                ::={meterReaderEntry 6}



--flowProbe

flowTable OBJECT-TYPE
                SYNTAX SEQUENCE OF FlowEntry
                MAX-ACCESS not-accessible
                STATUS current
                DESCRIPTION
                "Array contenente entries che descrivono i vari flussi generati "
                ::={flowProbe 1}

flowEntry OBJECT-TYPE
                SYNTAX FlowEntry
                MAX-ACCESS not-accessible
                STATUS current
                DESCRIPTION
                "Rappresenta una cella dell'array , quindi fornisce una descrizione
                del flusso"
                INDEX {flowIndex}
                ::={flowTable 1}



FlowEntry
                ::=SEQUENCE {

                flowIndex                       Integer32,
                flowStatus                      INTEGER,
                flowSourceInterface             Integer32,
                flowSourcePhysAddress       PhysAddress,

                flowSourcePeerType              PeerType,
                flowSourcePeerPhysAddress       PhysAddress,
```

```
        flowSourcePeerAddress           FlowAddress ,

        flowSourcePeerMask              FlowAddress,

        flowDestPeerType                PeerType ,
        flowDestPeerPhysAddress             PhysAddress,
        flowDestPeerAddress             FlowAddress ,
        flowDestPeerMask                FlowAddress ,

        flowRuleSet                                 Integer32,
        flowToOctect                                Counter64,
        flowFromOctect                              Counter64

        }

flowIndex OBJECT-TYPE
        SYNTAX Integer32 (1..2147483647)
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
        "indice della cella nell'array dei flussi"
        ::={flowEntry 1}

flowStatus OBJECT-TYPE
        SYNTAX INTEGER{attivo(1), inattivo(2),idle(3) }
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
        "Descrive lo stato del flusso"
        ::={flowEntry 2}

flowSourceInterface OBJECT-TYPE
        SYNTAX Integer32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
        "Indice dell'interfaccia di rete  dalla quale provengono i dati."
        ::={flowEntry 3}



flowSourcePhysAddress OBJECT-TYPE
        SYNTAX PhysAddress
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
        "Indica l'indirizzo fisico dell'interfaccia di rete della sonda"
        ::={flowEntry 4}

flowSourcePeerType OBJECT-TYPE
        SYNTAX PeerType
```

```
                MAX-ACCESS read-only
                STATUS current
                DESCRIPTION
                "Indica il tipo di tecnologia usata dal peer che produce traffico , la
                sonda e' in grando di riconoscere solo un sottoinsieme di teconlogie"
                ::={flowEntry 5}

flowSourcePeerPhysAddress OBJECT-TYPE
                SYNTAX  PhysAddress
                MAX-ACCESS read-only
                STATUS current
                DESCRIPTION
                "Indica l'indirizzo fisico del Peer cha ha prodotto il traffico"
                ::={flowEntry 6}

flowSourcePeerAddress OBJECT-TYPE
                SYNTAX FlowAddress
                MAX-ACCESS read-only
                STATUS current
                DESCRIPTION
                "Indica l'indirizzo del Peer che ha prodotto il traffico"
                ::={flowEntry 7}

flowSourcePeerMask OBJECT-TYPE
                SYNTAX FlowAddress
                MAX-ACCESS read-only
                STATUS current
                DESCRIPTION
                "Indica la machera di  rete adottata per il Peer che ha prodotto il traffico"
                ::={flowEntry 8}

 flowDestPeerType OBJECT-TYPE
                SYNTAX PeerType
                MAX-ACCESS read-only
                STATUS current
                DESCRIPTION
                "Indica il tipo di tecnologia usata dal peer che riceve traffico , la
                sonda e' in grando di riconoscere solo un sottoinsieme di teconlogie"
                ::={flowEntry 9}


flowDestPeerPhysAddress OBJECT-TYPE
                SYNTAX PhysAddress
                MAX-ACCESS read-only
                STATUS current
                DESCRIPTION
                "Inidca l'indirizzo fisico del Peer al quale e' destinato il traffico"
                ::={flowEntry 10}

flowDestPeerAddress OBJECT-TYPE
                SYNTAX FlowAddress
```

MAX-ACCESS read-only
STATUS current
DESCRIPTION
"Indica l'indirizzo del peer a cui e' destinato il traffico"
::={flowEntry 11}

flowDestPeerMask OBJECT-TYPE
SYNTAX FlowAddress
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"Indica la machera di sottorete del peer a cui e' destinato il traffico"

::={flowEntry 12}

flowRuleSet OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"Inidica il numero della regola che ha prodotto quueso flusso"
::={flowEntry 13}

flowToOctect OBJECT-TYPE
SYNTAX Counter64
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"Indica il numero di ottetti che transitano dalla sorgente alla destinazione per questo flusso "
::={flowEntry 14}

flowFromOctect OBJECT-TYPE
SYNTAX Counter64
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"Indica il numero di ottetti che trasnitano dalla destinazione alla sorgente per questo flusso "
::={flowEntry 15}

--ruleProbe

ruleTable OBJECT-TYPE
SYNTAX SEQUENCE OF RuleEntry
MAX-ACCESS not-accessible
STATUS current

DESCRIPTION
"Tabella contenente insiemi di regole rappresentati dalla ruleEntry , il meter puo' usare differenti insiemi di regole selezionati dal Manager.Ogni cella contiene un indice (ruleIndex, ovvero la posizione che occupa nella tabella), un parser(ruleParser ovvero l'attributo da controllare ogni volta che si ricevono dati), un'azione da prendere(rule Action), e delle note aggiuntive(ruleParameters)"
::={ruleProbe 1}

ruleEntry OBJECT-TYPE
SYNTAX RuleEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"Cella che contiene informazioni circa le regole da utilizzare"
INDEX {ruleIndex}
::={ruleTable 1}

RuleEntry ::= SEQUENCE{
ruleIndex Integer32,
ruleParser Parser,
ruleAction Action,
ruleParameters Integer32
}

ruleIndex OBJECT-TYPE
SYNTAX Integer32 (1..2147483647)
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"Indica l'indice all'interno della rule table"
::={ruleEntry 1}

ruleParser OBJECT-TYPE
SYNTAX Parser
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"Indica l'attributo da analizzare quando quando si ricevono dati"
::={ruleEntry 2}

ruleAction OBJECT-TYPE
SYNTAX Action
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"Indica il valore relativo all'azione da predere quando la regola e' soddisfatta"
::={ruleEntry 3}

```
ruleParameters OBJECT-TYPE
        SYNTAX Integer32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
        "Note aggiuntive sulla regole"
        ::={ruleEntry 4}

--trapProbe

ifDown NOTIFICATION-TYPE
        OBJECTS {ifIndex}
        STATUS current
        DESCRIPTION
        "Trap inviata dal meter a meter-reader quando una delle interfaccie a
        bordo della sonda assume un comportamente anomalo(rottura).
        Vengono in inviati alcune variabili relative all'interfaccia interessata,
        per poterla localizzare "
        ::={trapProbe 1}


ifUp NOTIFICATION-TYPE
        OBJECTS {ifIndex}
        STATUS current
        DESCRIPTION
        "Trap inviata dal meter al meter-reader quando una delle interfaccie
        presenti sulla sonda torna a funzionare correttamente . Anche in questo
        caso vengono riportate informazioni circa lo stato e la desrizione
                dell'interfaccia."
        ::={trapProbe 2}

highPckDropped NOTIFICATION-TYPE
        OBJECTS{ifIndex}
        STATUS current
        DESCRIPTION
        "Questa trap viene generata quando il meter scarta un eccessivo numero
        di pacchetti rispetto a quelli ricevuti.Vengono aggiunte informazioni
        circa i pacchetti ricevuti, e l'interfaccia che scarta questi pacchetti.
        Una possibile casua , potrebbe essere una configurazione errata della
        scheda di rete."
        ::={trapProbe 3}

noMeterRaederFound NOTIFICATION-TYPE
        OBJECTS {meterReaderIndex}
        STATUS current
        DESCRIPTION
        "Trap generata quando uno dei meter-reader collegati alla sonda ha un
        tempo di ultimo accesso troppo elevato , questo potrebbe significare che
        il meter-reader non e' piu' presente , oppure che si sta verificando
        un malfunizionamento."
```

```
::={trapProbe 4}
END
```

4-LAVORI FUTURI

Per motivi di tempo ,questo documento non tratta le parti relative alla definizione del Manager, Meter Reader e delle Applicazioni di Analisi.Questi tre parti risultano tuttavia essenziali per poter monitorare una rete e produrre le relative statistiche.

5-BIBLIOGRAFIA

J.Schönwälder, L.Deri "Sistemi di Elaborazione dell'informazione:Elementi di Gestioone di Rete" v.3

RFC 2063 : "Traffic Flow Measurement:Architecture"

RFC 2720 : "Traffic Flow Measurement:Meter MIB"

RFC 3176 : "InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks"

RFC 1213 : "Management Information Base for Network Management of TCP/IP-based internets:MIB-II"

RFC 2578 : " Structure of Management Information Version 2 (SMIv2)"

Traffic Monitoring using sFlow® (www.sFlow.org)

James F. Kurose, Keith W.Rose "Internet e Reti di calcolatori", McGraw-Hill ,Italy , 2001