

Impiego e funzioni principali del LAN-Analyzer e del Wireless-LAN Analyzer

Pietro Nicoletti

www.studioreti.it



Nota di Copyright

- Questo insieme di trasparenze (detto nel seguito slides) è protetto dalle leggi sul copyright e dalle disposizioni dei trattati internazionali. Il titolo ed i copyright relativi alle slides (ivi inclusi, ma non limitatamente, ogni immagine, fotografia, animazione, video, audio, musica e testo) sono di proprietà degli autori indicati a pag. 1.
- Le slides possono essere riprodotte ed utilizzate liberamente dagli istituti di ricerca, scolastici ed universitari afferenti al Ministero della Pubblica Istruzione e al Ministero dell'Università e Ricerca Scientifica e Tecnologica, per scopi istituzionali, non a fine di lucro. In tal caso non è richiesta alcuna autorizzazione.
- Ogni altra utilizzazione o riproduzione (ivi incluse, ma non limitatamente, le riproduzioni su supporti magnetici, su reti di calcolatori e stampate) in toto o in parte è vietata, se non esplicitamente autorizzata per iscritto, a priori, da parte degli autori.
- L'informazione contenuta in queste slides è ritenuta essere accurata alla data della pubblicazione. Essa è fornita per scopi meramente didattici e non per essere utilizzata in progetti di impianti, prodotti, reti, ecc. In ogni caso essa è soggetta a cambiamenti senza preavviso. Gli autori non assumono alcuna responsabilità per il contenuto di queste slides (ivi incluse, ma non limitatamente, la correttezza, completezza, applicabilità, aggiornamento dell'informazione).
- In ogni caso non può essere dichiarata conformità all'informazione contenuta in queste slides.
- In ogni caso questa nota di copyright non deve mai essere rimossa e deve essere riportata anche in utilizzi parziali.



Il Lan-Analyzer

- Strumento che serve per analizzare e studiare il contenuto dei pacchetti che transitano in rete



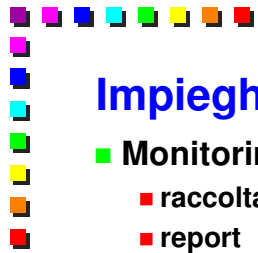
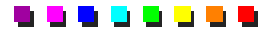
Tipi di Lan-Analyzer

- Di fascia alta (costi compresi tra 15 e 30 milioni di lire)
 - Basati su hardware dedicato
 - HP advisor, RAD, Fluke LanMeter
 - Basati su PC-Intel con interfaccia di rete dedicata
 - Sniffer® della Network Associates (ex Network General)
- Di fascia bassa (costi compresi tra 2 e 4 milioni di lire)
 - basati su software che decodifica pochi protocolli (IP, IPX, Netbeui, Appletalk, BPDU)
 - Observer (Network Instruments), Net-xray (Network Associates), Shomiti, Netmon SMS Microsoft



Impieghi e funzioni

- **Cattura dei pacchetti**
 - con eventuale impiego di filtri
- **Visualizzazione dei pacchetti catturati**
- **Decodifica ed analisi dei pacchetti**
 - può essere anche di tipo esperto
- **Trigger**
 - per far partire la cattura a fronte di un particolare evento
- **Generazione di traffico**
- **Gestione dei file di dati**



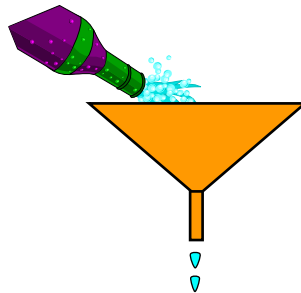
Impieghi e funzioni

- **Monitoring**
 - raccolta di statistiche
 - report
 - gestione allarmi



Cattura dei pacchetti

- Gli analizzatori di rete hanno una memoria finita e non è umanamente possibile analizzare una lunga lista di dati
- Bisogna ridurre al minimo la quantità dei pacchetti da catturare tramite l'impiego di filtri



Filtri in cattura

- I filtri possono essere basati su:
 - tipologia dei pacchetti:
 - good frame, bad CRC frame, short frame, collision frame
 - i protocolli
 - sugli indirizzi dei campi Source e Destination di livello MAC
 - se definiti entrambi si può verificare la comunicazione tra una coppia di macchine
 - su un particolare contenuto (pattern) all'interno di un pacchetto di cui si deve fornire anche l'Offset

Visualizzazione dei pacchetti

■ A seguito della cattura è possibile visualizzare il contenuto dei pacchetti

- può contenere il dettaglio di tutto il pacchetto o solo un sommario
- può essere visualizzata anche la sequenza dei byte con rappresentazione esadecimale
- l'analizzatore può aprire contemporaneamente 3 finestre:



- una contenente il riassunto del contenuto, un'altra contenente il dettaglio della decodifica ed l'ultima con sequenza dei byte in formato esadecimale

Filtri sulla visualizzazione

■ Nella fase di visualizzazione si possono attivare gli stessi tipi di filtri che si possono impiegare per la cattura

- a volte i filtri su base protocollo sono molto più ricchi, come numero di protocolli supportati, rispetto alla fase di cattura
- i filtri possono essere basati anche sui sintomi di un'anomalia

La decodifica dei pacchetti

- Fornisce l'interpretazione delle informazioni binarie contenute nel pacchetto

```

BPDU: Root Identifier      = 7D00.00E01E3E28AC
BPDU:  Priority            = 7D00
BPDU:  MAC Address        = 00E01E3E28AC
BPDU:
BPDU: Root Path Cost      = 500
BPDU:
BPDU: Sending Bridge Id   = 7FFF.00E01EEC3C84.8002
BPDU:  Priority            = 7FFF
BPDU:  MAC Address        = 00E01EEC3C84
BPDU:  Port                = 8002
BPDU: Message Age         = 1.000 seconds
BPDU: Information Lifetime = 20.000 seconds
BPDU: Root Hello Time     = 2.000 seconds
BPDU: Forward Delay       = 15.000 seconds
    
```

Decodifica ed analisi dei pacchetti

- Gli analizzatori più evoluti sono in grado di decodificare i pacchetti fino al livello 7
 - quelli più economici si fermano in genere al livello 3
 - certi problemi di rete causano delle anomalie che sono rilevabili solo a livello 4 (ritrasmissioni eccessive)
- I sistemi esperti sono in grado di fornire informazioni circa le possibili cause di un determinato evento

Trigger

■ Fa partire la cattura dei pacchetti a fronte di:

- eventi applicativi: esempio la ritrasmissione di un file
- eventi di livello 4:
 - connessione rotta
 - richiesta di ritrasmissione
 - login fallito, ecc...



Trigger

■ Fa partire la cattura dei pacchetti a fronte di:

- eventi di livello 3:
 - indirizzo duplicato
 - router storm
 - errata tabella di routing
 - conflitto di subnet, ecc...
- eventi di livello 2
 - eccessivo carico di traffico
 - tempesta di broadcast
 - errori del livello fisico: bad CRC, short frame, Oversize frame

Generazione di traffico

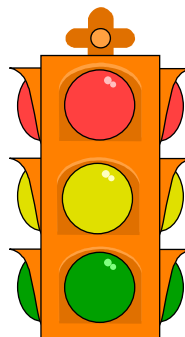
■ Single frame mode:

- si invia un pacchetto contenente dei dati predefiniti
- il pacchetto può essere inviato a tutte le stazioni (broadcast) o ad una particolare macchina
- la lunghezza del pacchetto è definibile
- si può definire l'occupazione percentuale della banda che si vuole causare o il ritardo tra i pacchetti
- si può definire un numero massimo di pacchetti da trasmettere oppure si può trasmettere ininterrottamente

Generazione di traffico

■ Buffer mode:

- si utilizza un pacchetto o insieme di pacchetti precedentemente catturati e salvati su un file per generare del traffico



Gestione dei file di dati

- I dati catturati possono essere salvati in un file
- Si può caricare in memoria un file di dati relativo ad una precedente cattura per analizzare i pacchetti a posteriori
- Si può stampare la visualizzazione di un pacchetto su stampante o su file
 - la stampa su file genera un file di testo in formato txt o prn

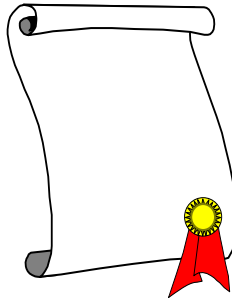
Statistiche

- Le statistiche possono riferirsi a:
 - occupazione della banda in termini di:
 - pacchetti singlecast, multicast e broadcast
 - pacchetti corretti o errati
 - ridistribuzione percentuale della banda per protocollo
 - statistiche globali o per singola stazione
 - si può avere uno storico di tipo globale o per singola stazione
 - le dimensioni dei pacchetti
 - le macchine top-talker



Report

- Si possono creare, salvare, stampare dei report, caricare dei report precedentemente salvati



Allarmi

- Si possono attivare degli allarmi a fronte del superamento di una soglia di:
 - numero di frame oversize
 - broadcast storm
 - utilizzo percentuale della banda
 - pacchetti errati



Le funzioni aggiuntive del Wireless-LAN Analyzer

■ Cattura e decodifica dei pacchetti di

- Management
 - Beacon, Association, Authentication, Probe ecc.
 - In particolare i pacchetti di Beacon contengono molte informazioni specifiche delle reti wireless
- Controllo
 - ACK, RTS, CTS, Power Save
- Data

Le funzioni aggiuntive del Wireless-LAN Analyzer

■ Filtri in cattura su base:

- canale, SSID,
- Tipologia dei pacchetti:
 - Management
 - Control
 - Dati senza crittografia WEP
 - Dati con crittografia WEP

■ Decodifica di pacchetti dati di cui si conosce la chiave WEP

■ Individuazione degli Access Point



Le funzioni di scanning del Wireless-LAN Analyzer

- Funzione di scanning dei canali per catturare i pacchetti trasmessi su canali differenti in diversi BSS
- Rilevazione di attività di rete sui vari canali
- Funzioni di site survey su un singolo canale o su tutti i canali

