# Individuazione dei nodi promiscui su reti Token ring con l'ausilio di pacchetti ARP

ing. Roberto Larcher – webteca.altervista.org – febbraio 2004

# Introduzione

La possibilità di individuare i nodi di una rete locale che effettuano intercettazione, analisi e monitoraggio dei dati (*sniffing*) è stata oggetto di numerosi studi. Sebbene questi studi non abbiano permesso di sviluppare tecniche universalmente efficaci[1], nondimeno hanno fornito alcuni strumenti comunemente usati per le reti basate sulla tecnologia Ethernet.
Daiji Sanai nel suo white paper [1] "Detection of promiscuous nodes using ARP Protocol" illustra una di queste tecniche che si basa, appunto, sul protocollo ARP.
In questo documento viene presentato un metodo per utilizzare tale tecnica per cercare di individuare i nodi promiscui presenti nelle reti di tipo Token ring.

Il documento si compone di due parti: la prima richiama alcuni concetti di base dei protocolli di rete e delle tecniche di sniffing; la seconda illustra in dettaglio come sia spesso possibile rilevare i nodi settati in modo promiscuo su rete Token ring.

# Che cos'è il modo promiscuo?

La trasmissione dei dati su rete Token ring si basa sull'inoltro dei *frame* di informazioni dal mittente al destinatario attraverso tutti i nodi dell'anello: ogni nodo verifica se i dati contenuti nel singolo frame sono ad esso destinati, nel caso li inoltra al sistema operativo e in ogni caso li invia al nodo successivo[2]. Questa attività di filtro viene svolta dalla scheda di rete e, convenzionalmente, il componente che effettua tale attività viene indicato con il termine *filtro hardware*.

Il *filtro hardware* può essere impostato in modo da inoltrare al sistema operativo (o più in generale a rendere disponibili all'utente) i frame di informazioni destinati:

- all'indirizzo hardware univocamente assegnato alla scheda dal costruttore (modo unicast)
- a tutti i nodi presenti sulla rete (modo broadcast)
- ad un gruppo di indirizzi hardware (modo multicast)
- a tutti gli indirizzi hardware (modo promiscuo)

Oltre a questi indirizzi, le specifiche Token ring impongono di accettare degli speciali indirizzi hardware riservati[3]. Tali indirizzi prendono il nome di indirizzi funzionali (*functional addresses*) in quanto vengono utilizzati per gestire determinate funzioni proprie del protocollo.
Normalmente le attività di monitoraggio di rete e di *sniffing* necessitano di intercettare tutti i frame di informazione e quindi il filtro hardware della scheda di rete deve essere impostato in modo promiscuo.

---

[1] Rintracciare un nodo promiscuo implica la necessità di generazione di traffico da parte di quest'ultimo. Nel caso che in nodo sia abilitato alla sola ricezione (si pensi nel caso ethernet a un cavo dove non siano collegate le coppie di trasmissione) è impossibile ottenere risposte a qualsiasi richiesta.
[2] A tale proposito si veda la specifica del protocollo: [2] IEEE 802.5 "Token ring access method and Phisical Layer specification" – IEEE Computer Society - 1995
[3] Si veda ancora la specifica IEEE 802.5

## Individuazione dei nodi settati in modo promiscuo

Come ben illustra Daiji Sanai nel suo white paper, in linea di principio individuare i nodi settati in modo promiscuo è abbastanza semplice: si tratta di sollecitare una risposta da parte dei soli nodi settati in tale modalità. In altri termini, è sufficiente inviare sulla rete una richiesta di informazioni opportunamente preparata in modo che:

- sia ignorata dai nodi di rete settati in modalità normale
- sia accettata dai nodi di rete settati in modalità promiscua.

Uno dei protocolli più adatti allo scopo è il protocollo ARP.

## Il protocollo ARP

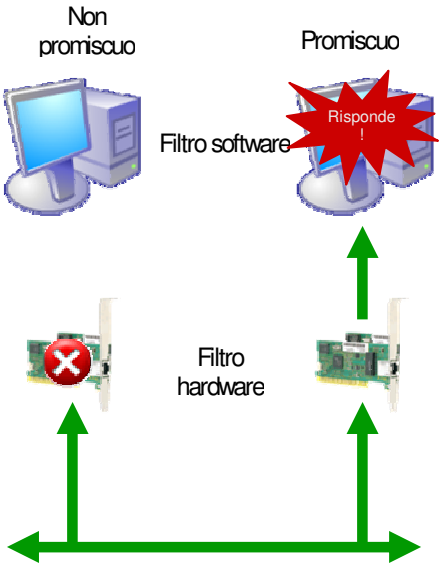
Le schede di rete, siano esse Ethernet o Token ring, sono identificate univocamente mediante un *indirizzo hardware* impostato dal costruttore. Tale indirizzo viene spesso indicato con il nome *MAC address* (Media Access Control) o, nel gergo proprio della tecnologia Token ring, *UAA* (Universally Administered Address). Tale indirizzo, attualmente di 48 bit, viene utilizzato per identificare il nodo mittente e il nodo destinatario di ogni *frame* di dati.
La grande diffusione del protocollo TCP/IP ha reso di fatto necessario l'utilizzo dello stesso anche nelle reti locali ed ha suscitato il problema della mappatura degli indirizzi IP sugli indirizzi MAC. Attualmente, infatti, il protocollo IP prevede un indirizzamento a 32 bit, contro i 48 bit degli indirizzi MAC. Il protocollo ARP si occupa, appunto, di effettuare questa mappatura.

Rimandando alla RFC corrispondente[4] per i dettagli, in questa sede è sufficiente richiamare il meccanismo di base che permette, dato un indirizzo IP, di reperire il corrispondente indirizzo MAC.
La modalità è la seguente: viene inviato a tutti i nodi della rete un messaggio (ARP_Request) in cui, specificando indirizzo IP e MAC del mittente ed indirizzo IP del destinatario, si richiede il MAC del destinatario.
A questo punto i ruoli si invertono: il nodo possessore dell'indirizzo IP desiderato risponde con un messaggio (ARP_Reply) che contiene i suoi estremi come mittente - IP e MAC - e come destinatario il mittente originario.
Si fa notare che il primo messaggio è indirizzato a tutti i nodi della rete (broadcast), mentre il secondo a un solo destinatario (unicast).

[4] [3] RFC 826: "An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission On Ethernet Hardware" – David C. Plummer – November 1982

## Come utilizzare ARP per individuare i nodi promiscui

Si è detto che quando un *frame* di informazioni giunge a una scheda di rete viene effettuato un test e, in funzione dello stato del *filtro hardware*, si determina se le corrispondenti informazioni debbano essere passate al sistema operativo.
Dal momento che nei nodi promiscui il *filtro hardware* è, sostanzialmente, disabilitato, tutti i pacchetti giungono ai componenti del sistema operativo che gestiscono i protocolli di livello superiore, quali, ad esempio, TCP/IP e quindi ARP (secondo computer in figura).




Questo non risulta essere vero se la scheda di rete non è settata in modo promiscuo (primo computer in figura).
Oltre al *filtro hardware* i sistemi operativi implementano comunemente un *filtro software* dal comportamento analogo.

Per ottenere una risposta al messaggio ARP_Request da parte di un nodo settato in modalità promiscua è quindi necessario creare tale messaggio con un indirizzo hardware che venga **rigettato dal filtro hardware settato in modalità non promiscua** e che venga **accettato in ogni caso dal filtro software** implementato nel sistema operativo[5].

## Una possibile soluzione per reti Token ring

Nel tentativo di individuare i nodi settati in modo promiscuo nelle reti Token ring, sono stati presi in considerazione gli indirizzi hardware modificati comunemente utilizzati nel caso di reti Ethernet.
Come verificato da appositi test, tali indirizzi non permettono di identificare i nodi promiscui nelle reti Token ring. Una possibile spiegazione a questo fatto è che le

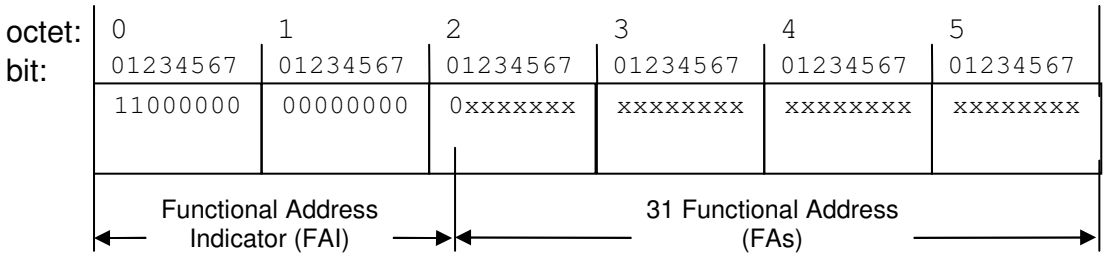
[5] Come già detto un ampio studio sull'argomento nel caso di reti di tipo Ethernet può essere trovato in [1] "Detection of Promiscuous Nodes Using ARP Packets" - Daiji Sanai – agosto 2001.

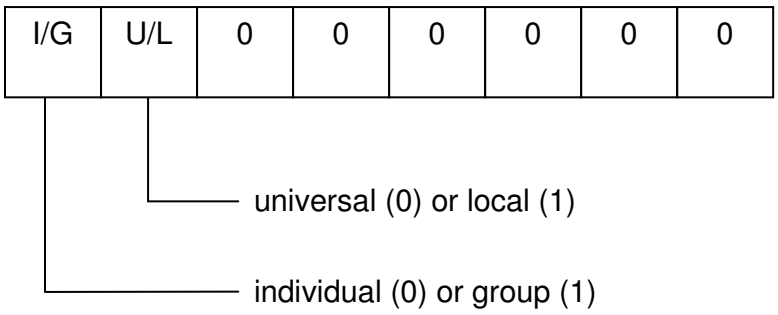
specifiche Token ring, oltre al classico indirizzo broadcast "FF FF FF FF FF FF" identificano anche l'indirizzo "C0 00 FF FF FF FF" come broadcast[6].
Risulta quindi intuibile come una modifica ai bit meno significativi (ad esempio nel caso di "FF FF FF FF FF FE"), solitamente utilizzata nel caso Ethernet, difficilmente potrebbe ingannare il filtro software, in quanto è plausibile che lo stesso effettui un test più approfondito che non il confronto dei soli primi bit.

Scartate quindi le modifiche agli indirizzi broadcast, l'attenzione si è spostata sugli indirizzi multicast e in particolare sulla modalità di trasmissione multicast su protocollo IP descritta dalla [4] RFC 1469: "IP Multicast over Token-Ring Local Area Networks" – T. Pusateri – Giugno 1993.

In tale documento viene proposto di riservare l'indirizzo funzionale "C0 00 00 04 00 00" per la trasmissione di pacchetti IP multicast nelle reti Token ring.

Come di può vedere in figura il generico indirizzo funzionale si compone di un prefisso, detto Functional Address Indicator di 17 bit, mentre i rimanenti 31 bit identificano la funzione che deve essere svolta.




In particolare, nel primo ottetto il bit 0 indica se l'indirizzo funzionale debba essere universale o locale, mentre il bit 1 indica se l'indirizzo funzionale debba essere individuale o di gruppo[7].

L'indirizzo C0 00 00 04 00 00, che la RFC 1593 suggerisce di utilizzare per la trasmissione multicast su IP, è quindi un indirizzo funzionale "locale di gruppo".

[6] Si veda la specifica del protocollo: IEEE 802.5 "Token ring access method and Phisical Layer specification" – IEEE Computer Society – 1995, paragrafo 3.2.4.1.3 Broadcast address.
[7] Si veda ancora la specifica del protocollo IEEE 802.5 "Token ring access method and Phisical Layer specification" – IEEE Computer Society – 1995, paragrafo 3.2.4.1.5 Functional addresses (FAs).

Le prime modifiche effettuate hanno portato a dei risultati immediati.

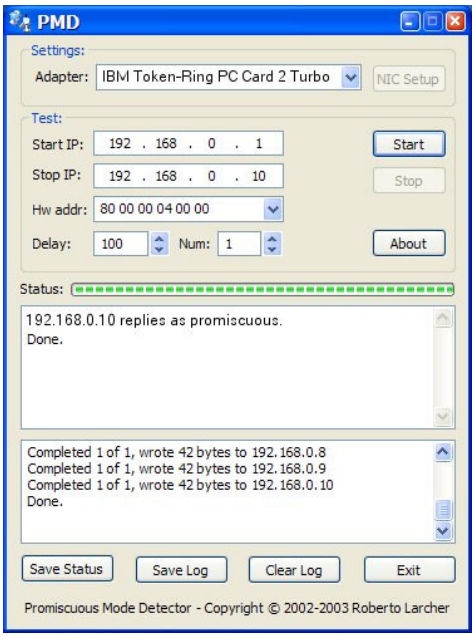
Lasciando invariato il bit 0 e ponendo a 0 il bit 1, si ottiene un indirizzo funzionale "universale di gruppo" che nei sistemi operativi testati[8] può essere efficacemente utilizzato per l'identificazione dei nodi promiscui.

In particolare i nodi promiscui correttamente impostati per il normale utilizzo del protocollo IP vengono individuati preparando un opportuno messaggio ARP_Request avente come indirizzo MAC di destinazione "80 00 00 40 00 00".

## L'applicazione di test

Al fine di effettuare dei test è stato realizzato un apposito programma che, opportunamente rivisto e corretto, ha portato alla realizzazione dell'applicazione PMD (Promiscuous Mode Detector).

Si tratta di una applicazione Open Source[9], pertanto, in questa sede, se ne darà solo una descrizione di massima; per maggiori dettagli si rimanda all'esame del codice sorgente.




Come si può vedere dalla figura, si tratta di una applicazione per sistema operativo Windows.
L'interfaccia si compone di una prima parte che permette di:

[8] Le prove sono state effettuate per i sistemi operativi Microsoft di ultima e penultima generazione: Windows XP e 2000.
[9] L'applicazione è certificata OSI - Open Source Initiative. I sorgenti e la documentazione possono essere scaricati dal sito http://webteca.altervista.org

- selezionare la scheda di rete da utilizzare,
- determinare l'insieme di indirizzi da controllare,
- impostare il "falso" hardware da utilizzare,
- avviare / arrestare il test con gli appositi tasti.

Seguono poi due riquadri dove vengono presentati i risultati del test.

Il funzionamento dell'applicazione è il seguente: per ogni indirizzo IP dell'insieme selezionato viene inoltrato un messaggio di ARP_Request con le seguenti caratteristiche:

- indirizzo hardware del mittente reale,
- indirizzo hardware del destinatario (es.: 80 00 04 00 00 00),
- indirizzo IP richiesto: quello reale del destinatario,
- indirizzo IP del mittente: un indirizzo inventato, difficilmente presente in LAN[10].

Vengono poi intercettate le eventuali risposte che, viste le caratteristiche delle richieste, proverranno solo da nodi di rete settati in modo promiscuo e quindi avranno un impatto minimo sulla normale operatività della rete locale.
I possibili nodi promiscui vengono evidenziati nei riquadri dei risultati.

Il programma utilizza le librerie WinPcap del Politecnico di Torino, le librerie pcap per la cattura dei pacchetti e la libreria Libnet di Mike Shiffman per la scrittura dei pacchetti.
Ovviamente il programma può essere utilizzato anche su reti Ethernet.

## Ringraziamenti

Desidero ringraziare tutti coloro che mi hanno aiutato durante questo progetto. In particolare Gianluca Varenni del Politecnico di Torino e Dennis Kaer Jansen per il test dell'applicazione in ambiente Ethernet e Marco Favaretto per la revisione della bozza di questo white paper.
Infine, ringrazio particolarmente Daiji Sanai. Il suo lavoro sulle schede Ethernet mi ha fornito le informazioni di base per effettuare questo studio.

[10] Attualmente per la determinazione dell'indirizzo IP si fruttano due caratteristiche proprie di Ipv4, che prevede indirizzi IP da 32 bit, e dei microprocessori Intel, che lavorano con codifica *little endian.*
Detto quindi IP l'indirizzo IPv4 della macchina di test, si utilizza IP+1. In effetti date le caratteristiche appena citate se IP = 192.168.0.100 allora IP+1 = 193.168.0.100, che non essendo un indirizzo riservato per le reti private, difficilmente sarà presente in LAN.

# Bibliografia


[1] Detection of Promiscuous Nodes Using ARP Packets
Daiji Sanai – agosto 2001.

http://www.securityfriday.com/promiscuous_detection_01.pdf

[2] IEEE 802.5 “Token ring access method and Physical Layer specification”
IEEE Computer Society – 1995

http://standards.ieee.org/getieee802/802.5.html

[3] RFC 826: “An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission On Ethernet Hardware”
David C. Plummer – Novembre 1982

http://www.faqs.org/rfcs/rfc826.html

[4] RFC 1469: “IP Multicast over Token-Ring Local Area Networks”
T. Pusateri – Giugno 1993.

http://www.faqs.org/rfcs/rfc1469.html