PORADNIKI

Wykrywanie snifferów przy użyciu pakietów ARP

WSTĘP

W sieciach lokalnych, bezpieczeństwo jest zawsze godne rozważenia. Kiedy jawny teks został wysłany do sieci, może być łatwo przechwycony przez dowolnego użytkownika sieci. Kradzież danych w sieci nazywa się sniffingiem. Przez sniffing sieci, użytkownik może uzyskać dostęp do poufnych dokumentów i spowodować zamieszanie w czyjejś prywatności. Wiele darmowego oprogramowania dystrybuowanego przez Internet dostarcza takiej możliwości. Pomimo łatwości sniffingu, nie ma dobrego sposobu na wykrycie takiego niegodziwego działania. Postaram się wyjaśnić mechanizmy używane przez PromiScan, oprogramowanie, które może efektowanie skanować sniffery w sieci. Sniffery działają przez odbieranie wszystkich pakietów będących wysłanymi do sieci. Aby to uzyskać, wszystkie sniffery muszą ustawić Network Interface Card (NIC) w swoich komputerach na tryb zwany "trybem odbierania". Wtedy NIC będzie odbierał wszystkie pakiety i przekazywał je do jądra systemu. Pakiety zgłoszenia Address Resolution Protocol (ARP) są używane do zapytania o adresy sprzętowe z adresów IP. Wykorzystamy ten rodzaj pakietów dla zweryfikowania czy NIC'i w sieci są ustawione na tryb odbierania .Pakiety zgłoszenia ARP są używane ponieważ są dostępne we wszystkich Ipv4 opartego na Ethernet. Kiedy NIC odbiera wszystkie pakiety, pakiety które przypuszczalnie nie dotarły do tego pC nie są dłużej blokowane przez NIC. Wszystkie pakiety są przekazywane do jądra systemu a jądro systemu może tworzyć błędy przez odpowiadanie na pakiety, które nie są przystosowane do odpowiedzi .Przy obecności powyższego mechanizmu, możemy tworzyć fałszywe pakiety zgłoszeniowe ARP i wysyłać je do każdego węzła w sieci. Pakiety zazwyczaj są blokowane przez NIC'i ale jeśli jakiś węzeł odpowiada na nie, wtedy istnieją NIC'i odbiorcze. Te PC z odbiorczymi NIC'ami są uruchomionymi snifferami .Zatem sniffery mogą być skutecznie wykrywane.

1. .... Zaczynamy

W sieciach lokalnych, akt sniffingu jest dużym wątkiem. Złośliwi użytkownicy mogą łatwo kraść poufne dokumenty i czyjąś prywatność przez sniffowanie sieci. Sniffing powoduje wtrącanie się w prywatność, ale może być zrobiony po prostu przez ściągnięcie darmowego sniffera z Internetu i zainstalowanie go na swoim komputerze. Jednak, na razie nie ma dobrego sposobu na wykrycie który komputer sniffuje w sieci. Tu wykorzystamy pakiety Address Resolution Protocol (ARP) dla skutecznego wykrywania złośliwych użytkowników, którzy sniffują biurową lub szkolną sieć.

2. Zasady sniffingu

Sieć lokalna zazwyczaj jest złożona z Ethernetu. W Ethernecie używa się protokołu IP (Ipv4), informacja jest wysyłana po kablu jawnym tekstem, chyba ,że używany jest program szyfrujący.Kiedy ktoś wysyła informację do sieci oczekuje ,że ktoś po drugiej stronie sieci odbierze tą informację. Niestety mechanizm Ethernetu daje nieautoryzowanym ldziom szansę kradzieży i przeglądania tych danych. Wiemy ,że sieci oparte o Ethernet działają przez wysyłanie komunikatów do wszystkich węzłów w sieci i oczekuje ,że tylko węzły uprawnione do tego będą odbierały ten komunikaty.W tym samym czasie, inne węzły po prostu odrzucają te komunikaty. Czy odbioeramy czy odrzucamy komunikaty jest to kontrolowane przez Network Interface Card (NIC). NIC nie odbiera wszystkich wszystkich pakietów w sieci chociaż jest połączony z Ethernetem; zamiast tego filtruje żądane pakiety, jakie określony komputer powinien odebrać. Tu będziemy wykorzystywać Hardware Filter NIC. Sniffing jest robiony porzez ustawienie NIC własnego komputera na określony tryb, tak ,że NIC będzie odbierał wszystkie dane przychodzące do niego bez względui czy jest miejscem przeznaczenia. Tryb NIC jest nazywany Trybem Odbierania.

3. Podstawowe pojęcia związane z wykrywaniem Trybu Odbierania

Zamiast wysyłania nielegalnych pakietów, sieciowy sniffing występuje przez odbieranie wszystkich pakietów. Ponieważ nie koliduje to z ruchem w sieci, trudno wykryć takie zachowanie. Niemniej jednak, stan NIC w trycbie odbierania jst oczywiście inny niż w trybie normalnym. Pakiet , który jest przypuszczalnie filtrowane przez filtr sprzętowy jest teraz przekazywany do jądra systemu. Nasz sposób na wykrywanie węzła odbiorczego może być zademonstrowany na rzeczywistym przykładzie. Wyobraźmy sobie ,że jest zebranie w sali spotkań.Wtedy sniffing konferencji może być zrobione przez wstawienie jakiegoś ucha pod ścianamisali spotkań. Kiedy ją sniffujemy, chcemy podłsuchiwać wszystkie rozmowy prowadzone w sali spotkań.. Jednak, jeśli padnie na sali nazwa snifferki , "Miss XX?", wtedy sniffer może uczynić błąd odpowiadając "Tak?" Ta analogia brzmi trochę śmiesznie, ale może być zastosowane do sniffowania sieciowego. Ponieważ węzeł sniffujący odbiera wszystkie te pakiety, wliczając te ,które nie są dla niego przeznaczone, może popełnić błąd odpowiadając na te pakiety, które pierwotnie były filtrowane przez NIC. Dlatego też, nasze wykrywanie węzła odbiorczego jest wykonywane przez sprawdzanie odpowiedzi na pakiety ARP, kiedy żądania pakietów ARP są wysyłane do wszystkich węzłów w sieci.

4. Podstawy

1) Filtr sprzętowy
Najpierw, zacznijmy od różnic między NIC w trybie odbierania a w trybie normalnym. Wszystkie NIC'i w Ethernecie są przedstawiane przez 6 bajtowy adres sprzętowy. Wytwórca przypisuje ten adres tak ,że każdy adres jest unikalny w całym świecie. Teoretycznie, nie ma dwóch NIC'ów mających taki sam adres sprzętowy. Cała komunikacja w Ehernecie oparta jest na tym adresie sprzętowym. NIC jednak, może ustawiać różne filtry aby odbierać różne rodzaje pakietów. Poniżej mamy listę filtrów sprzętowych

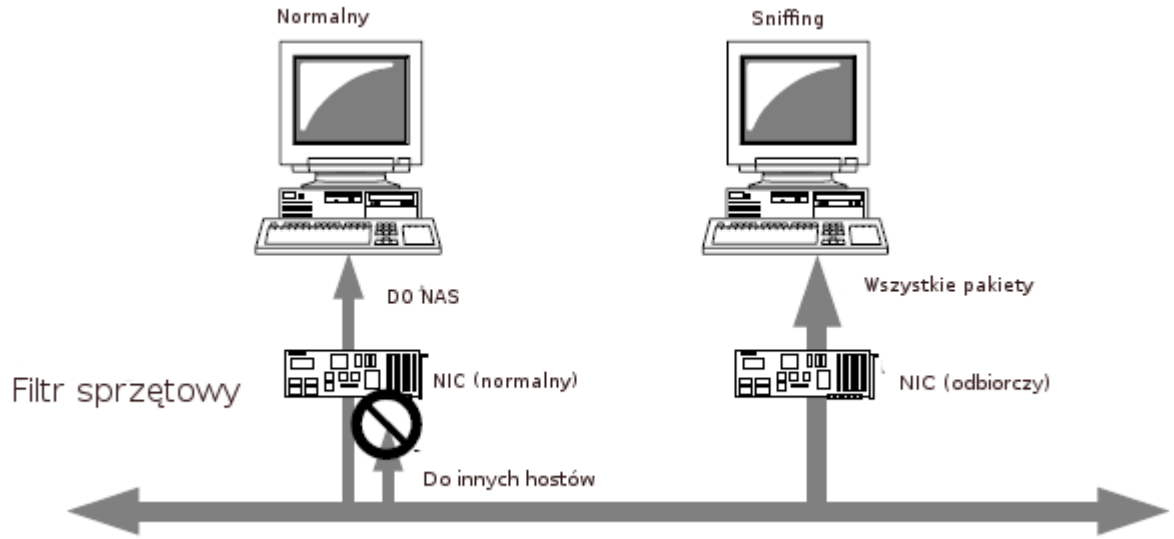
Unicast
Odbiera wszystkie pakiety mające taki sam adres przeznaczenia jako adres sprzętowy NIC'a

Broadcast
Odbiera wszystkie pakiety radiowe. Pakiety te mają adres przeznaczenia FF FF FF FF FF FF. Celem tego trybu jest odbieranie pakietów które przychodzą do prawie wszystkich węzłów istniejących w sieci

Multicast
Odbier wszystkie pakiety, które są szczególnie skonfigurowane dla odbierania grup adresów multiemisji. Tylko pakiety z sprzętowy adres multicast zarejestrowany uprzednio na liście multiemisji będzie odbierana przez NIC

Wszystkie multiemisje
Odbiera wszystkie pakiety multicast. Ponieważ ten tryb może również odpowiadać na inne wysokopoziomowe protokoły inne niż Ipv4 .Wszystkie multiemisje będą odbierały wszystkie pakiety które mają ustawiony własny bit grupy.

Odbieranie
Odbiera wszystkie pakiety w sieci bez sprawdzania adresu przeznaczenia



Filtr sprzętowy

Powyższy rysunek działania filtru sprzętowego kiedy jest w trybie normalnym i kiedy sniffuje. Zwykle, PC ustawia swój filtr sprzętowy NIC na adres unicast, broadcast i multicast1. One tylko odbierają pakiety , które mają swój adres przeznaczenia ustawiony na własny adres sprzętowy, adres broadcast (FF FF FF FF FF FF) a multicast1 (01 00 5E 00 00 01)

2) Mechanizm ARP

W Ethernecie łączonym przez adresy IP, pakiety są faktycznie wysyłane i odbierane w oparciu o adresy sprzętowe. Pakiety nie mogą być wysyłane przez użycie adresu IP. Dlatego też, Ethernet potrzebuje maechnizm, który konwertuje adresy IP na adresy sprzętowe. W tym czasie, są używane pakiety Address Resolution Protocol (ARP). Pakiety ARP należą do warstwy łączenia, który jest tą samą warstwą co IP, więc pakiety ARP nie wpływają na warstwę IP. Ponieważ adresy IP są zawsze dostępne w sieci IP, pakiety ARP stają się odpowiednimi pakietami dla testowania odpowiedzi węzłów kiedy wykrywamy węzły odbiorcze. W poniższym przykładzie zilustrujemy działania używające pakiet ARP dla rozwiązania adresu IP:

Komputer X z adresem IP 192.168.1.1 i adresem sprzętowym 00-00-00-00-00-01 chce wysłać komunikat do innego komputera Y z adresem 192.168.1.10. X najpierw złoży pakiet żądania ARP, który jest używany do zapytania o adres sprzętowy odpowiedniego 192.168.1.10. Pole adresu sprzętowego przeznaczenia pakietu ARP jest ustawiony na broadcast (FF-FF-FF-FF-FF-FF), tak ,że wszystkie węzły w sieci lokalnejk będą odbierały ten pakiet. Kiedy każdy PC w sieci odbiera ten pakiet, sprawdza czy adres IP pakietu ARP jest ten sam co jego własny. Jeśli się różnią, ten pakiet ARP jest ignorowany. Jeśli są takie same, wtedy PC odpowied na ten pakiet, wraz z jego własnym adresem sprzętowym i adres IP. W tym przypadku, Y wyśle pakiet odpowiedzi do X a X zbuforuje tą parę adresów sprzętowy / IP. Ponieważ X z powodzeniem zapytuje o adres sprzętowy Y, X może zaczynać wysyłać aktualne dane

5. Podstawy wykrywania węzła odbierania

Jak wspomniałem wcześniej, pakiety są filtrowane inaczej kiedy NIC jest ustawiony na ttryb odbierania niż na tryb normalny. Kiedy NIC jest ustawiony w trybie odbierania, pakiety które przypuszczalnie są filtrowane przez NIC są teraz przekazywane do jądra systemu. Przez zastosowanie tego mechanizmu, podchodzimy z nowym sposobem wykrywania węzłów odbierania:

jeśli skonfigurujemy pakiet ARP , tak ,że nie ma adresu broadcast jako adresu przeznaczenia, wysyła go do każdego węzła w sieci i odkrywa ,że niektóre węzły odpowiadają na niego, wtedy węzły te są w trybie odbierania. Teraz przejdziemy poprawną operacjężądanie / odpowiedź ARP. Na początku pakiet ARP generowany jest dla 192.168.1.10. Ten adres przeznaczenia jest ustawiony na adres broadcast taki ,że wszystkie węzły w sięci mogą go odbierać. Teoretycznie, tylko jeden węzeł z dokładnie takim samym adresem IP będzie na niego odpowiadał. Ale co z przeznaczeniem pakietu ARP, ustawionym na inny adres niż adres broadcast? Na przykład, co się stanie jeśli usatwimy adres przeznaczenia na 00-00-00-00-00-01? Kiedy NIC jest w trybie normalnym , pakiet ten jest rozpatrywany jako będący "pakietem innego hosta", więc jest odzrucany przez filtr sprzętowy NIC. Jednak, kiedy NIC jest w trybie odbierania, NIC nie wykonuje żadnych operacji filtrujących. Wtedy taki pakiet można przekazać do jądra systemu. Jądro systemu zakłada ,że to żądanie pakietu ARP ponieważ zawiera ten sam adres IP co PC, więc odpowiada na ten pakiet. I tu niespodzianka, jądro w rzeczywistości nie odpowiada na ten pakiet. Ten nieoczekiwany wynik pokazuje ,że istnieje jakiś filtr sortujący w oprogramowaniu, ponieważ pakiet jest w rzeczywistości filtrowany ponownie przez jądro systemu. W związku z tym przejdziemy do Filtra Programowego. Pójdziemy krok dalej, wykrywanie odbierania NIC może być uzyskane przez obserwację różnic między filtrem sprzętowym a filtrem programowym. Filtr sprzętowy zazwyczaj bokuje nieporawne pakiety (te nie przenoszone do jądra systemu). Więc jeśli pakiet może przejść przez filtr sprzętowy, może zwykle przejść również filtr programowy. Teraz chcemy złożyć pakiety , które będą blokowane przez filtr sprzętowy ale w tym samym czasie będą mogły przejść filtr oprogramowania Przez wysyłanie takich pakietów do węzła, NIC w trybie normalnym nie będzie odpowiadał. Zamiast tego jeślo NIC jest w trybie odbierania, odpowie.

6. Filtr programowy

Filtr programowy zależy od jądra systemu operacyjnego, więc zrozumienie jak działa filtr programowy jądra systemu jest konieczne. Ponieważ Linuks jest system otwartym, zajmiemy się mechanizmem jego filtra programowego. Jednak, ponieważ kod źródłowy Microsoft Windows jest nieopublikowany, mechanizm jego filtra programowego może być odgadywany przez eksperymenty.

1) Linux
W module Ethernet Linuksa, pakiety są klasyfikowane w zależności od adresu sprzętowego

Pakiety broadcast:
FF FF FF FF FF FF
Pakiety multicast:
Wszystkie pakiety mają grupę bitów ustawioną, z wyjątkiem pakietów broadcast
Pakiet DO NAS:
Wszystkie pakiety mają ten sam adres przeznaczenia jako adres sprzętowy NIC

Pakiety INNE HOSTY:
Wszystkie pakiety mają różne adresy przeznaczenia jako adres sprzętowy NIC

Zakładamy ,że wszystkie te pakiety z ustawiną grupą bitów są pakietami multicast. Odpowiedni pakiet multicast Ethernetu sieci IP jest w postaci 01-00-5E-xx-xx-xx i pierwotnie, apkiety multicast nie może być sklasyfikowany przez weryfikację grupy bitów. Jednak, to założenie ie jest błędne. Jest tak ponieważ 01-00-xx-xx-xx jest adresem multicast opartym o IP, ale adres sprzętowy NIC również jest używany przez inne protokoły górnopoziomowe. Spójrzmy na moduł ARP używany przez Linuks. Moduł ARP najpierw odrzuca wszystkie pakiety INNEHOSTY. Potem będzie odpowiadał na pakiety Broadcast, Multicast i DONAS.

Pakiety DONAS:
Kiedy NIC jest w trybie normalnym, wszystkie pakiety DONAS moga przechodzić przez filtr sprzętowy. Jak również może przechodzić przez filtr programowy, więc moduł ARP będzie odpowiadał na pakiety bez względu na to czy NIC jest trybie odbierania.

Pakiety INNEHOSTY:
Kiedy NIC jest w trybie normalnym, odrzuca pakiety INNEHOSTY. Nawet keidy NIC jest w trybie odbiorczym, filtr programowy odrzuca te pakiety. Więc nie będzie odpowiedzi na żądania ARP

Pakiety Broadcast:
W trybie normalnym, pakiety Broadcast przechodzą zarówno przez filtr sprzętowy i programowy. Więc będzie odpowiadał bez względu na tryb NIC

Pakiety Multicast:
W trybie normalnym, pakiety z adresem sprzętowym nie zarejestrowane na liście multicast są odrzucane. Ale jeśli NIC jest w trybie odbierania, ten rodzaj pakietów będzie przechodził filtr sprzętowy nawet jeśli adres sprzętowy nie jest zarejestrowany na liści multicast. I ,ze względu na fakt ,że filtr programowy nie odrzuca pakietów multicast, odpowiedzi będą uzyskiwane. W tym przypadku, ponieważ będą uzyskiwane różne wyniki kiedy ten sam pakiet jest wysyłany do NIC w trybie normalnym i trybie odbierania, ten rodzaj pakietów będzie używany dla wykrywania węzłów odbiorczych.

Pakiety grupy bitów:
Te pakiety nie są ani pakietami Broadcast ani Multicast, ale ustawioną grupą bitów. W trybie normalnym, filtr sprzętowy odrzuca ten rodzaj pakietów ale trybie odbierania, pakiety są przekazywane. A ponieważ ten rodzaj pakietów jest klasyfikowany jako pakiety multicast przez filtr programowy, moga one przechodzić filtr programowy. Ten pakiet grupy bitów może być używanny doo wykrywania węzłów odbiorczych.

2) Windows
Windows nie jest systemem operacyjnym open source, więc nie możemy zanalizować zachowania jego filtru programowego przez zbadanie jego kodu źródłowego. Zamiast tego wykonamy eksperymenty testujące filtr programowy Windows. Użyjemy siedmiu rodzajów adresów sprzętowych:

Adres broadcast FF-FF-FF-FF-FF-FF:
Wszystkie węzły powinny odbierać ten rodzaj pakietów i odpowiadać ponieważ jest to adres broadcast. Zwykle pakiety żądania ARP używają tego adresu

Fałszywy adres broadcast FF-FF-FF-FF-FF-FE:
Adres ten jest fałszywym adresem broadcast ze zgubionym ostatnim bitem 1. Jest to sprawdzenie czy filtr programowy sprawdzi wszystkie bity adresu i czy odpowie na nie

Fałszywy broadcast 16 bitowy FF-FF-00-00-00-00:
Adres ten jest fałszywym adresem brodcast w którym tylko pierwszse 16 bitóq jest takich samych jak adres broadcast. Może być to zaklasyfikowane jako adres broadcast i odpowiada kiedy funkcja filtru tylko sprawdza peirwsze słowo adresu broadcast.

Fałszywy broadcast 8 bitowy FF-00-00-00-00-00:
Adres ten jest fałszywymy adresem broadcast w którym tylko pierwsze 8 bitów jest takich samych jak adres broadcast. Może być to zaklsayfikowane jako adres broadcast i odpowiada kiedy funkcja filtru sprawdza tylko pierwszy bajt adresu broadcast.

Adres grupy bitów 01-00-00-00-00-00:

Jest to adres tylko z ustawioną grupą bitów. Jest to sprawdzenie czy adres ten jest rozpatrywany jako adresmulticast, jak w Linuksie

Adres multicast 0 01-00-5E-00-00-00

Adres multicast 0 zazwyczaj nie jest używany. Więc użyamy tego przykładu adresu multicast nie zarejestrowanego na liście multicastów NIC. Filtr sprzętowy powinien odrzucić ten pakiet. Jednak, pakiet ten moze być nieprawidłowo zaklasyfikowany jako adres multicast kiedy filtr programowy nie do końca sprawdził wszystkie bity. Jadro systemu zatem moze odpowiedzieć na taki pakiet kiedy NIC jest ustawiony w tryb odbierania.

Adres multicast 101-00-5E-00-00-01:

Adres multicast 1 jest adresem , który wszystkie hosty w sieci lokalnej powinny odebrać. Innymi słowy ,filtr sprzętowy będzie przepuszczał ten rodzaj pakietów domyślnie. Ale jest możliwe , że NIC nie obsługuje trybu multicast i nie odpowiada. Więc jest to sprawdzenie czy host obsługuje adresy multicast.

7. Wykrywanie odbierania

Wyniki wskazują ,że możemy użyć pakietów ARP do określenia węzłów odbierania, czy systemy to Windows czy Linux .Zatem, w podobny sposób te metody wykrywania mogą być stosowane w sieci lokalnej. Oto ta procedura:

1) Chcemy sprawdzić czy maszyna z adresme IP (A) jest w trybie odbierania, składamy pakiet ARP. Pakiet ARP ma następujący format:

Ethernetowy adres przeznaczenia	FF FF FF FF FF FF
Ethernetowy adres nadawcy	00 11 22 33 44 55
Typ protokołu (ARP =0806)	08 06
Przestrzeń adresu sprzętowego (Ethernet=01)	00 01
Przestrzeń adresu protokołu (IPv4=0800)	08 00
Długość w bajtach adresu sprzętowego	06
Długość w bajtach adresu protokołu	04
Opkod (żądanie ARP=01, odpowiedź ARP=02)	00 01
Adres sprzętowy nadawcy tego pakietu	<Własny adres urządzenia NIC>
Adres protokołu nadawcy tego pakietu	<Własny adres IP kmputera>
Adres sprzętowy celu tego pakietu	00 00 00 00 00 00
Adres protokołu celu	<Adres IP (A) >

- Adres ethernetowy miejsca przeznaczenia jest adresem przeznaczenia pakietu Ethernet. W tym przypadku, jest to adres sprzętowy NIC celu. Pakiet przeznaczenia ARP powinien być ustawio na adres broadcast FF FF FF FF FF FF, ponieważ chcemy aby wszystkie hosty odbierały ten pakiet. I chcemy aby aby tylko jeden host odpowiedział na niego jeśli adres IP odpowiada na jeden pakiet ARP jaki jest żądany.Ale chcemy złożyć pakiet , który jest przypuszczalnie blokowany przez filtr sprzętowy i aby przejśc filtr programowy, będziemy używać zamiast tego adresu FF FF FF FF FF FE
- Adres Ethernet nadawcy jest adresem sprzętowym nadawcy. Na przykład, 00 11 22 33 44 55 jest sześciobajtowym adresem sprzętowym
- Typ protokołu to 08 06 kiedy jest to pakiet ARP
- Adres sprzętowy przestrzeni to 01 kiedy używany jest Ethernet
- Przestrzeń adresu protokołu to 08 00 kiedy używany jest protokół IPv4
- Długość bajtowa adresu sprzętowego jest to długość w bajtach adresu sprzętowego. W tym przypadku to 06
- Długość bajtowa adresu protokołu jest to długość w bajtach adresu IPv4. W tym przypadku

jest to 04

- Opkod to 00 01 kiesy jest to pakiet żądania ARP
- Adres sprzętowy nadawcy tego pakietu jest to adres sprzętowy PC, na przykład może być wysłanedo 00 11 22 33 44 55
- Adres protokołu nadawcy tego pakietu to 00 00 00 00 00 00 ponieważ jest aktualnie nieznany (Celem pakietu żądania ARP jest zapytanie się o to pole)
- Adres protokołu celu to 4 bajtowy adres IP węzła który jest sprawdzany czy jest w trybie odbierania

2) Potem składamy ten pakiet, możemy wysłać go do sieci
3) Teraz ten pakiet jest blokowany prze filtr sprzętowy maszyby docelowej. Jednakże jeśli ta maszyna jest w trybie odbierania, pakiet ten przejdzie filtr sprzętopwy a filtr programowy będzie odpowiadał. Jeśli odbierzemy odpowiedź, wtedy maszyna ta jest w trybie odbierania.

8. Wykrywanie węzła odbierania

Aby wykryć wszystkie węzły odbiorcze obecne w sieci lokalnej, zastosujemy techniki opisane w punkcie 7 do wszystkich węzłów w sieci sekwencyjnie. Jeśli istnieje jakaś maszyna która nie może być osiągalna dla pakietów ARP, wtedy ta metoda wykrywania odbierani nie może być zrealizowana

9. Wyjątki

Prezentuję kilka wyjątków kiedy wykrywanie odbierania nie może być zastosowane:

1) Stare NIC'i

Pewne stare NIC'i nie obsługują listy multicastów. Na przykład 3COM EtherlinkIII nie obsługuje tych list. Pakiety są możliwe do uzyskania przez filtr programowy bez sprawdzania przez filtr sprzętowy. Ze względu na fakt ,że pakiety jakie wysyłamy mają ustawioną grupę bitów, nie jest możliwe dla tego rodzaju NIC'ów odróżnienie między pakietem wykrywania odbierania a pakietem multicast. Jeśli taka sytaucja się wydarzy, powinno się zastosować nowszy NIC.

2) 3Com NIC

Kiedy NIC serii 3Com 3c905 jest zainstalowany na maszynie z Linuksem, ustawiony jkest domyślnie tryb multicast, więc nie możliwe jest dla nas odróżnienie trybu multicast od trybu odbierania. Wystąpienie tego wyjątku jest spowodowane tym ,że sterownik dostarczony przez Linuks nie obsługuje listy multicast'ów a NIC ma domyślny tryb multicast.