Politechnika Krakowska

Katedra Automatyki i Technik Informacyjnych

Laboratorium Sieci Komputerowych

2012/2013

ARP

1. Wprowadzenie

1.1. Protokół ARP

Protokół ARP (ang. Address Resolution Protocol) umożliwia powiązanie adresów warstwy wyższej, np adresów logicznych IPv4 z odpowiadającymi im adresami fizycznymi interfejsów sieciowych. Protokół stosowany jest w sieciach ethernetowych, token ring jaki i sieciach FDDI (sieci światłowodowe).

Protokół umożliwia zarządzanie systemowi operacyjnemu tak zwanej tablicy ARP (jest to rodzaj pamięci cache) która jest wykorzystywana przy adresowaniu ramek ethernetowych. Jest to protokół pomocniczy w działaniu sieci, jego obecność nie jest konieczna w celu poprawnej komunikacji, można go zastąpić statycznymi wpisy w tablicy ARP, ale takie podejście jest niepraktyczne w przypadku dużej ilości hostów działającej w sieci. Niemniej takie rozwiązanie jest czasami stosowane w celu zwiększenia bezpieczeństwa sieci.

1.2. Działanie protokołu ARP

Działanie protokółu ARP opisuje poniższy algorytm:

1. Rozesłanie do wszystkich hostów działających w sieci lokalnej (z wykorzystaniem adresu rozgłoszeniowego) zapytania zawierającego adres IP hosta docelowego oraz adres fizyczny (MAC) i adres IP hosta źródłowego
2. Zapytanie jest obsługiwane tylko przez hosta którego adres sieci (IP) jest zgodny z podanym w zapytaniu. Host odpowiadający na zapytanie ARP tworzy odpowiedz zawierającą swój adres sieci (IP) i swój adres fizyczny (MAC), tworzona ramka adresowana jest na adres MAC hosta, który wygenerował zapytanie.
3. Odebrany komunikat ARP z adresem MAC dodawany jest do tablicy ARP systemu operacyjnego hosta i łączony z adresem IP hosta docelowego. Zarówno czas przechowywania adresu jaki i wymiar tablicy są ograniczone.

1.3. Format komunikatów ARP

Postać protokół ARP przedstawia rys 1 (na podstawie [1]), przy zastosowania go do 6 bajtowego adresu ethernetowego oraz 4 bajtowego adresu sieciowego

Rys 1. Postać komunikatu ARP sieci ethernetowej z adresacją IPv4 oraz 6 bajtowego adresu MAC

Typ adresu sprzętowego		Typ adresu protokołu
Długość adresu sprzętowego	Długość adresu protokołu	Operacja
Adres sprzętowy nadawcy (4 pierwsze bajty)		
Adres sprzętowy nadawcy (2 ostatnie bajty)		Adres protokołu nadawcy (2 pierwsze bajty)
Adres protokołu nadawcy (2 ostatnie oktety)		Adres sprzętowy celu (2 pierwszy bajty)
Adres sprzętowy celu (4 ostatnie bajty)		
Adres protokołu celu (4 bajty)		

Typ adresu sprzętowego, 2 bajtowe pole informuje o rodzaju stosowanego adresu sprzętowego (MAC), dla sieci ethernetowych wynosi „1"

Typ adresu protokołu, 2 bajtowe pole informuje o rodzaju adresu stosowanego w protokole warstwy wyższej, dla sieci IPv4 jest wypełniona wartością „0x0888"

Długość adresu sprzętowego, 1 bajtowe pole wyrażająca w bajtach rozmiar adresu sprzętowego

Długość adresu protokołu, 1 bajtowe pole określające w bajtach rozmiar adresu protokołu warstwy sieci

Operacja, 2 bajtowe pole służące do odróżnienia typu komunikatu, „1" - żądanie, „2" – odpowiedz

Adres sprzętowy nadawcy, Pole o długości określonej parametrem długość adresu sprzętowego, zawiera adres sprzętowy nadawcy komunikatu

Adres protokołu nadawcy, pole o długości określonej przez pole długość adresu protokołu, zawiera adres nadawcy

Adres sprzętowy celu, zawiera adres sprzętowy docelowego hosta

Adres protokołu celu, zawiera adres sieci wykorzystywany przez hosta docelowego

Pola **Adres sprzętowy celu oraz Adres protokołu celu** są polami długości określonej przez pola **długość adresu sprzętowego** oraz **długość adresu protokołu**

1.4. Enkapsulacja protokołu ARP

Komunikaty protokołu ARP przesyłane są w polu „dane" ramek ethernetowych, przedstawia to rys 2.

Rys 2. Enkapsulacja komunikaty ARP w ramce ethernetowej

Ramka ethernetowa	Nagłówki ramki	dane			CRC
komunikatu ARP		Typ adresu sprzętowego	...	Ostatnie 4 bajty adresu protokołu	

Ramka ethernetowa w polu typ wstawia tą samą wartość (0x0806) niezależnie czy transportowana jest informacja o żądaniu czy odpowiedzi ARP, aby zidentyfikować rodzaj komunikatu konieczna jest analiza pola **operacja** komunikatu.

2. Cel ćwiczenia

Celem ćwiczenia jest zapoznanie się z podstawowymi aspektami protokołu ARP.

3. Ćwiczenia

1. Proszę sprawdzić działanie polecenia „arp"

   Jakie informacje zawiera wynik? Do czego wykorzystywana jest tablica ARP?

2. Proszę sprawdzić jaki jest wynik polecenia „arp –v"

3. Sprawdź wartość zmiennej modułu jądra: */proc/sys/net/ipv4/neigh/[interfejs]/gc_stale_time*

   Jaką informację zawiera ta zmienna?

4. Proszę usunąć z tablicy arp wpis odpowiadający bramie domyślnej, a następnie przeanalizować (z wykorzystaniem filtrów) w programie Wireshark próbę uzyskania adresu fizycznego bramy przez hosta arp -d

   Z jakim (i dlaczego takim) adresem jest formowana ramka ethernetowa w każdym kroku?

   Jakie jest „zasięg" requestów protokołu arp?

   Jakie jest znaczenie pól w protokole? Czy są transmitowane jakieś zbędne informacje?

sudo wireshark + podanie hasła logowania

man arp

5. Analizując sesję z punktu 4, proszę odpowiedzieć na pytanie czy protokół ARP jest protokołem stanowym czy bezstanowym? Jakie zagrożenia wynikają z tego?

6. Korzystając z terminala i analizatora sieciowego zbadać kiedy dodawany jest wpis do tablicy ARP?

7. Proszę przeanalizować (w programie Wireshark) pierwszą ramkę ethernetową zawierającą pakiet ARP po przyłączeniu komputera do sieci. W tym celu proszę skorzystać z komend:

   sudo ifconfig eth0 down

   sudo ifconfig eth0 up

   Czym różni się ten komunikat ARP od wcześniej poznanych?

4. Bibliografia

[1] „Sieci komputerowe i intersieci" D. Comera

Instrukcja opracowana przez: