

# Address Resolution Protocol (ARP) и Neighbor Discovery Protocol (NDP)

доц. д-р инж. Айдын Хъкъ

# ОСНОВНИ МОМЕНТИ

- Директно маршрутизиране
- Индиректно маршрутизиране
- ARP
- NDP
- Проблеми

# Address Resolution Protocol (ARP)

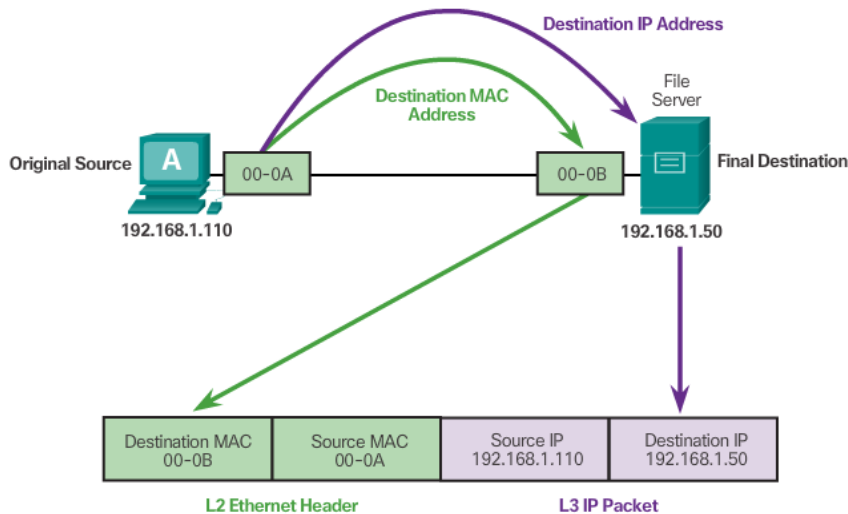
- ARP служи за намиране на физическия адрес (MAC, Token Ring, FDDI или IEEE 802.11, ATM ) на дадено устройство по неговия адрес от мрежовия слой (IPv4).
- Протоколът е дефиниран в RFC 826.
- Функциите на ARP за IPv6 се предоставят от Neighbor Discovery Protocol (NDP).

# Маршрутизиране

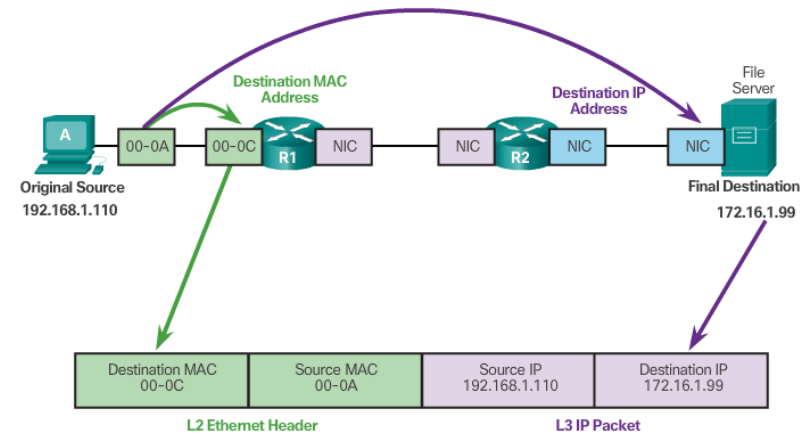
- Маршрутизиране – процес на доставяне на пакет от източник (сорс) до получател (дестинация), при който мрежовите устройства вземат решения за пътя на доставката с помощта на протоколи.
- Възможно е и задаване на статичен път.
- Всяко устройство има 2 адреса:
  - Физически (MAC) – за комуникация от NIC до NIC в сегмента.
  - Логически (IP) – за комуникация от оригиналния сорс до дестинацията.

# Директно / индиректно маршрутизиране

Communicating on a Local Network



Communicating to a Remote Network



MAC addresses are shortened for demonstration purposes.

- Директно - Дестинацията е в същия сегмент.
- Индиректно - Дестинацията е в друг сегмент на мрежата. Използва се конфигурираният default gateway.

# Работа на ARP

- ARP изпраща запитване (ARP Request) в локалната мрежа и търси MAC адреса на собственика на IP адреса получател.
- Хостът, разпознал IP-то си, изпраща MAC-а си като отговор (ARP Response).
- MAC адресът на получателя се кешира в таблица (ARP Table), за да може при бъдеща комуникация ARP автоматично да асоциира IP-то с MAC адреса.

# ARP таблица

```
C:\Users\Veneta Aleksieva>arp/a
```

```
Interface: 192.168.1.7 --- 0x16
```

Internet Address	Physical Address	Type
192.168.1.1	24-df-6a-b9-8a-5a	dynamic
192.168.1.3	88-c9-d0-bf-4d-a3	dynamic
192.168.1.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

```
Wireless LAN adapter Wireless Network Connection:
```

```
Connection-specific DNS Suffix . : vivacom-ads1
Description . . . . . : Intel(R) Dual Band Wireless-AC 3165
Physical Address. . . . . : 08-D4-0C-A8-D9-AA
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : fd24:df6a:b98a:5a00:b134:89da:eef6:4b3(Preferred)
Temporary IPv6 Address. . . . . : fd24:df6a:b98a:5a00:6907:77a3:94a5:95a9(Preferred)
Link-local IPv6 Address . . . . . : fe80::b134:89da:eef6:4b3%22(Preferred)
IPv4 Address. . . . . : 192.168.1.7(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Sunday, July 30, 2017 3:04:55 PM
Lease Expires . . . . . : Tuesday, August 01, 2017 1:24:32 PM
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 235459596
DHCPv6 Client DUID. . . . . : 00-01-00-01-1F-8A-73-32-08-D4-0C-A8-D9-AA
DNS Servers . . . . . : 8.8.8.8
NetBIOS over Tcpip. . . . . : Enabled
```

- Съдържа двойки IPv4-МАС адреси.
- Ако дестинационният IPv4 адрес е в същата мрежа като сорсовия IPv4 адрес, хостът ще търси в ARP таблицата дестинационния IPv4, за да разбере неговия МАС адрес.
- Ако дестинационният IPv4 адрес е в различна мрежа, хостът ще търси в ARP таблицата IPv4 адреса на конфигурирания default gateway , за да разбере неговия МАС адрес.
- Ако се намери IPv4, се ползва МАС адреса като дестинационен в локалния сегмент.
- Ако не се намери IPv4, се изпраща ARP request.

# ARP Request

Capturing from Wireless Network Connection

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help



Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	HuaweiTe_b9:8a:5a	Broadcast	ARP	42	Who has 192.168.1.4? Tell 192.168.1.1
2	1.023937	HuaweiTe_b9:8a:5a	Broadcast	ARP	42	Who has 192.168.1.4? Tell 192.168.1.1
3	1.945679	HuaweiTe_b9:8a:5a	Broadcast	ARP	42	Who has 192.168.1.4? Tell 192.168.1.1

> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0  
> Ethernet II, Src: HuaweiTe\_b9:8a:5a (24:df:6a:b9:8a:5a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
> Address Resolution Protocol (request)

```
0000 ff ff ff ff ff ff 24 df 6a b9 8a 5a 08 06 00 01 .....$. j..Z....
0010 08 00 06 04 00 01 24 df 6a b9 8a 5a c0 a8 01 01 .....$. j..Z....
0020 00 00 00 00 00 00 c0 a8 01 04 ..... ..
```

> Frame 3: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0  
> Ethernet II, Src: HuaweiTe\_b9:8a:5a (24:df:6a:b9:8a:5a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
✓ Address Resolution Protocol (request)  
    Hardware type: Ethernet (1)  
    Protocol type: IPv4 (0x0800)  
    Hardware size: 6  
    Protocol size: 4  
    Opcode: request (1)  
    Sender MAC address: HuaweiTe\_b9:8a:5a (24:df:6a:b9:8a:5a)  
    Sender IP address: 192.168.1.1  
    Target MAC address: 00:00:00\_00:00:00 (00:00:00:00:00:00)  
    Target IP address: 192.168.1.4

- ARP request е бродкаст.
- ARP request съдържа IPv4 адреса, на който се иска MAC адреса, IPv4 и MAC на сorsa.
- Полето Target MAC address е празно (00:00:00:00:00:00).



# ARP Reply

Capturing from Wireless Network Connection

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
11	37.7519...	IntelCor_a8:d9:aa	HuaweiTe_b9:8a:...	ARP	42	Who has 192.168.1.1? Tell 192.168.1.7
12	37.7539...	HuaweiTe_b9:8a:5a	IntelCor_a8:d9:...	ARP	42	192.168.1.1 is at 24:df:6a:b9:8a:5a

> Frame 12: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0

> Ethernet II, Src: HuaweiTe\_b9:8a:5a (24:df:6a:b9:8a:5a), Dst: IntelCor\_a8:d9:aa (08:d4:0c:a8:d9:aa)

▼ Address Resolution Protocol (reply)

Hardware type: Ethernet (1)  
Protocol type: IPv4 (0x0800)  
Hardware size: 6  
Protocol size: 4  
Opcode: reply (2)  
Sender MAC address: HuaweiTe\_b9:8a:5a (24:df:6a:b9:8a:5a)  
Sender IP address: 192.168.1.1  
Target MAC address: IntelCor\_a8:d9:aa (08:d4:0c:a8:d9:aa)  
Target IP address: 192.168.1.7

0000 08 d4 0c a8 d9 aa 24 df 6a b9 8a 5a 08 06 00 01 .....\$. j..Z....  
0010 08 00 06 04 00 02 24 df 6a b9 8a 5a c0 a8 01 01 .....\$. j..Z....  
0020 08 d4 0c a8 d9 aa c0 a8 01 07 .....

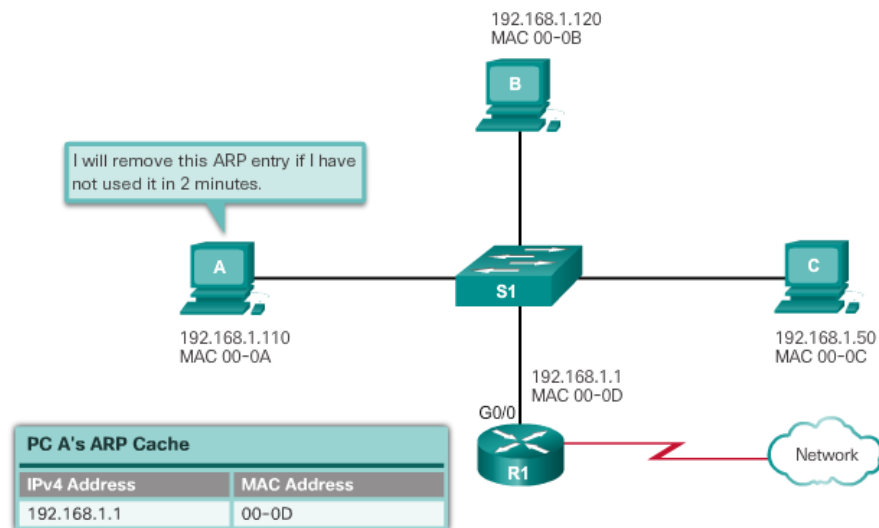
- ARP reply е уникаст, но поради бродкастния характер на средата се “чува” от всички в локалния сегмент.

# ARP в индиректно маршрутизиране

No.	Time	Source	Destination	Protocol	Length	Info
27	100.252...	IntelCor_a8:d9:aa	HuaweiTe_b9:8a:...	ARP	42	Who has 192.168.1.1? Tell 192.168.1.7
28	100.254...	HuaweiTe_b9:8a:5a	IntelCor_a8:d9:...	ARP	42	192.168.1.1 is at 24:df:6a:b9:8a:5a

- Ако дестинационния IPv4 адрес е в различна мрежа, хостът ще търси в ARP таблицата IPv4 адреса на конфигурирания default gateway, за да разбере неговия MAC адрес.
- Ако няма запис за IPv4 адреса на конфигурирания default gateway, се използва ARP процеса за определяне на MAC адреса на default gateway.

# Изчистване на записи от ARP таблицата



```
C:\Users\Veneta Aleksieva>arp/?
```

Displays and modifies the IP-to-Physical address translation tables used by address resolution protocol (ARP).

```
ARP -s inet_addr eth_addr [if_addr]
```

```
ARP -d inet_addr [if_addr]
```

```
ARP -a [inet_addr] [-N if_addr] [-v]
```

-a Displays current ARP entries by interrogating the current protocol data. If inet\_addr is specified, the IP and Physical addresses for only the specified computer are displayed. If more than one network interface uses ARP, entries for each ARP table are displayed.

-g Same as -a.

-v Displays current ARP entries in verbose mode. All invalid entries and entries on the loop-back interface will be shown. Specifies an internet address.

inet\_addr Specifies an internet address.

-N if\_addr Displays the ARP entries for the network interface specified by if\_addr.

-d Deletes the host specified by inet\_addr. inet\_addr may be wildcarded with \* to delete all hosts.

-s Adds the host and associates the Internet address inet\_addr with the Physical address eth\_addr. The Physical address is given as 6 hexadecimal bytes separated by hyphens. The entry is permanent.

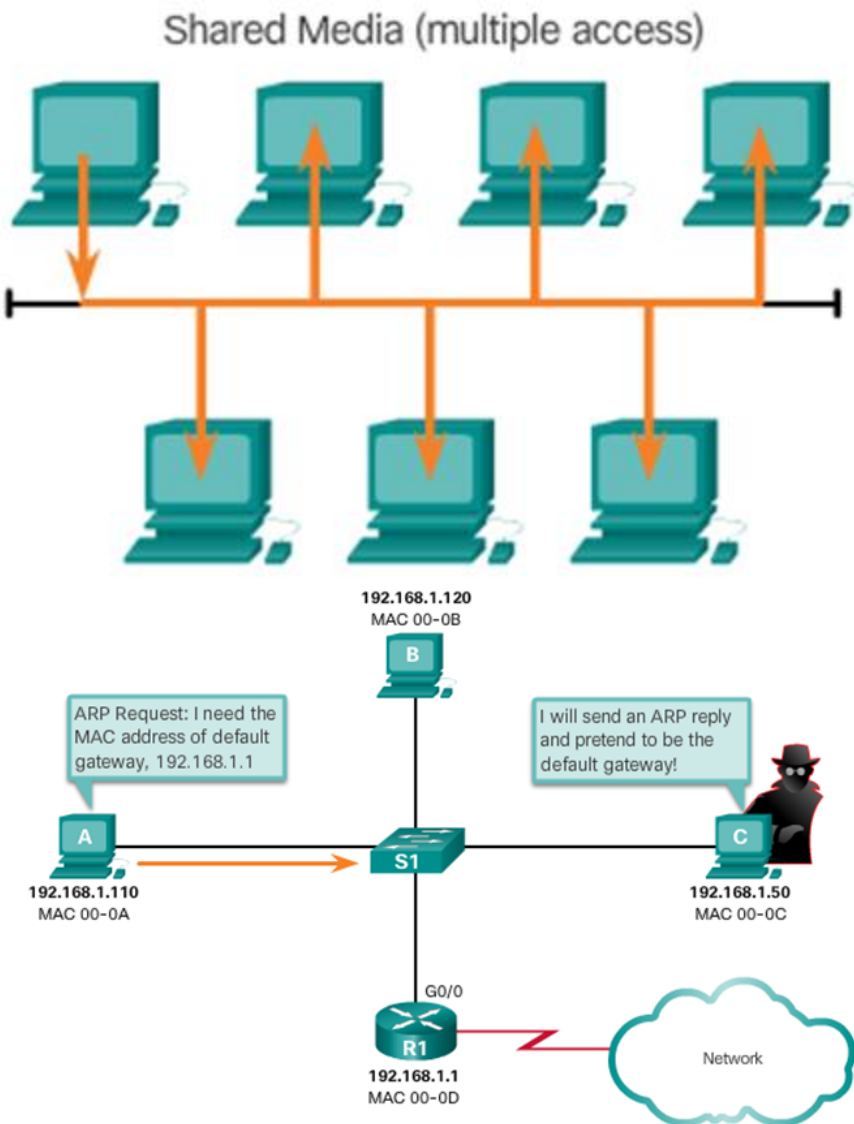
eth\_addr Specifies a physical address.

if\_addr If present, this specifies the Internet address of the interface whose address translation table should be modified. If not present, the first applicable interface will be used.

- Таймерът на записа IPv4-MAC щом изтече, записът се премахва от ARP таблицата.
- Таймерът се конфигурира. По подразбиране е 2 минути.
- Някои записи от ARP таблицата могат да се изтрият ръчно.

# Проблеми с ARP

- ARP бродкастите могат да задръстят преносната среда, ако всички устройства се включат едновременно и таблиците им са празни.



# И още...Reverse ARP

- Не се използва в съвременни мрежи, т.к. Има DHCP.
- Използва се от клиентска машина в локална мрежа, която изпраща своя MAC адрес до RARP сървър, за да поиска своя IPv4 адрес от ARP таблицата му.
- Мрежовият администратор създава таблица в RARP сървъра, която се използва за свързване на MAC адреса към съответния IP адрес.

# И още... Inverse ARP

- Вместо да използва Layer-3 адрес (IP адрес) за намиране на MAC адрес, Inverse ARP използва MAC адрес за намиране на IP адрес.
- Inverse ARP е точно обратното на ARP.
- Обратният ARP е заменен от BOOTP и по-късно DHCP.
- Inverse ARP се използва единствено за конфигурация на устройството в ATM мрежи и DLCI във frame relay.

# И още...Proxy ARP

- Позволява на устройства, които са в разделени мрежови сегменти, свързани от маршрутизатор в една IP мрежа, да преобразуват IP адрес в MAC адреси.
- Когато устройствата не са в една и съща мрежа на Data Link слой, но са в една и съща IP мрежа, те се опитват да предават данни едно на друго, сякаш са в локалната мрежа. Рутерът, който разделя устройствата, няма да изпрати бродкаст, т.е. адресите не могат да бъдат получени. Прокси ARP е активиран по подразбиране, така че „прокси рутерът“, който се намира между локалните мрежи, отговаря със своя MAC адрес, сякаш е рутерът, към който е адресиран бродкаста.
- Когато изпращащото устройство получи MAC адреса на прокси рутера, то изпраща съобщенията си до прокси рутера, който на свой ред ги изпраща до дестинационното устройство.

# И още... Gratuitous ARP

- Когато компютърът се стартира (мрежовата интерфейсна карта е включена) за първи път, той автоматично изпраща своя MAC адрес към цялата мрежа с Gratuitous ARP.
- След Gratuitous ARP MAC адресът на компютъра е известен на всеки комутатор и позволява на DHCP сървърите да знаят къде да изпратят IP адреса по този MAC, ако бъде поискан.
- Gratuitous ARP работи с Gratuitous ARP request, така и Gratuitous ARP reply.
- Gratuitous ARP е полезен за откриване на IP конфликт в мрежата.
- Gratuitous ARP се използва за отсуича за актуализиране на ARP таблицата и бридж таблицата му (port - MAC address).



# Neighbor Discovery Protocol (NDP)

- Neighbor Discovery Protocol (NDP) работи с IPv6.
- Работи като ARP и Internet Control Message Protocol (ICMP), както и протоколите за откриване на рутер и пренасочване на рутер, използвани в IPv4.
- Той работи на Data Link слой.
- Отговаря за събирането на различна информация, необходима за мрежова комуникация.
- Inverse Neighbor Discovery (IND) позволява на хостовете да определят и рекламират IPv6 адрес, съответстващ на даден MAC адрес, подобно на Reverse ARP за IPv4.

# Въпроси ?

Благодаря за вниманието !