

# Protocolo ARP

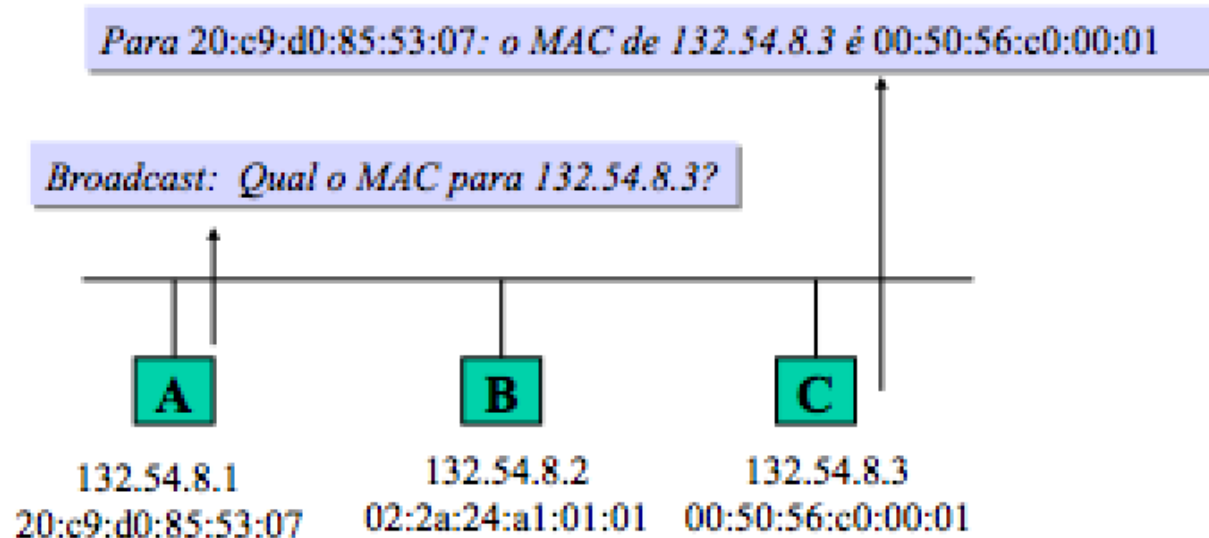
Prof. Marcelo Veiga Neves  
marcelo.neves@pucrs.br

# Problema

- Aplicações de usuários utilizam endereços IP para enviar dados para um host remoto
- Redes Ethernet utilizam endereços MAC enviar quadros para um host remoto
- Como o host descobre o endereço MAC a partir do endereço IP?

# Exemplo

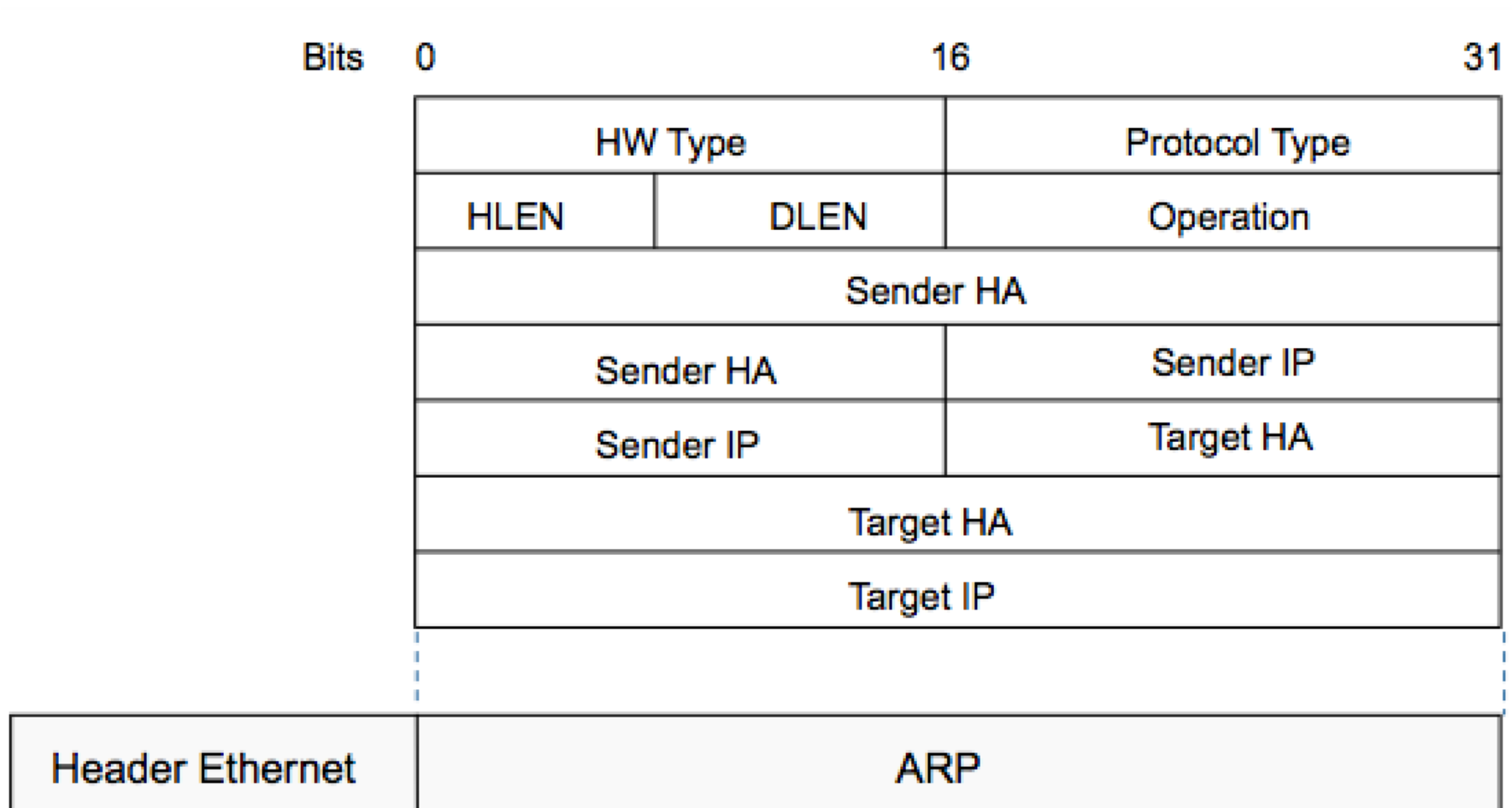
- A precisa enviar pacote IP para C
- A conhece apenas o IP do C
- Como descobrir o endereço MAC de C?



# ARP

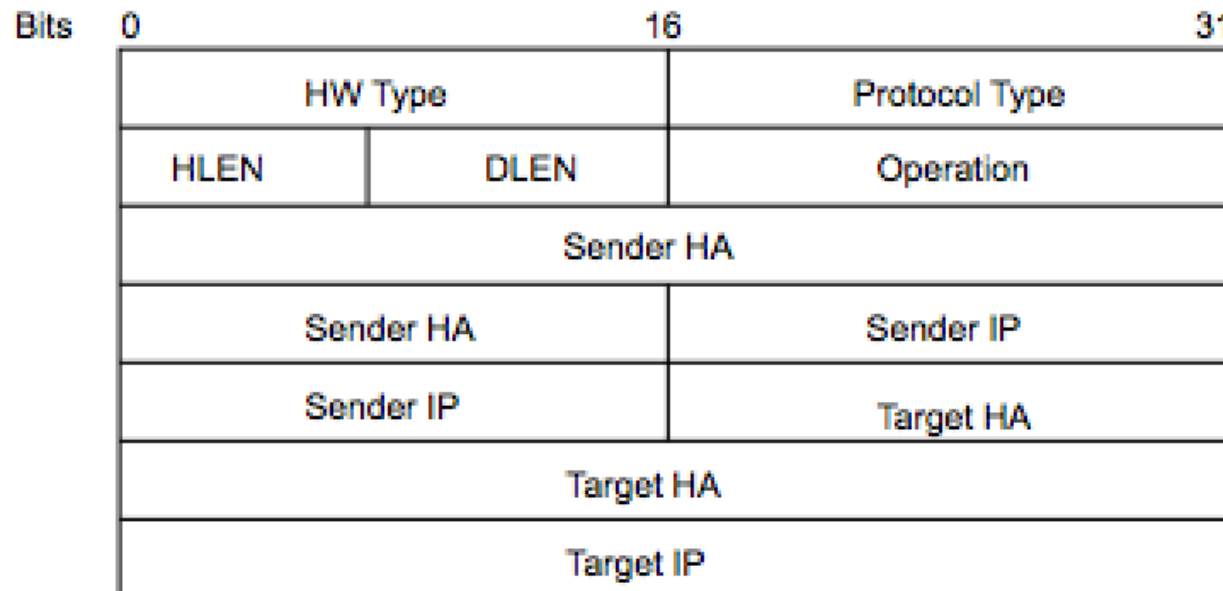
- ARP = Address Resolution Protocol
- Enviado diretamente sobre quadros Ethernet
  - EtherType: 0x0806
- Dois tipos de mensagens principais:
  - ARP request (envia para o endereço de broadcast)
  - ARP reply (responde para o host de origem)

# Formato do pacote



# Formato do pacote

- HW Type: especifica o protocolo da camada 2
  - Ethernet = 1
- Protocol Type :especifica o protocolo da camada 3
  - IPv4 = 0x0800



# Formato do pacote

- Operation
  - 1 - ARP request
  - 2 - ARP reply
  - 3 - RARP request
  - 4 - RARP reply

Bits	0	16	31
HW Type		Protocol Type	
HLEN	DLEN	Operation	
Sender HA			
Sender HA		Sender IP	
Sender IP		Target HA	
Target HA			
Target IP			

# Formato do pacote

- Sender HA: endereço MAC de origem
- Sender IP: endereço IP de origem
- Target HA: endereço MAC do destinatário
  - No ARP reply, esse valor é desconhecido
- Target IP: endereço IP do destinatário

Bits	0	16	31
HW Type		Protocol Type	
HLEN	DLEN	Operation	
Sender HA			
Sender HA		Sender IP	
Sender IP		Target HA	
Target HA			
Target IP			



# ARP Cache

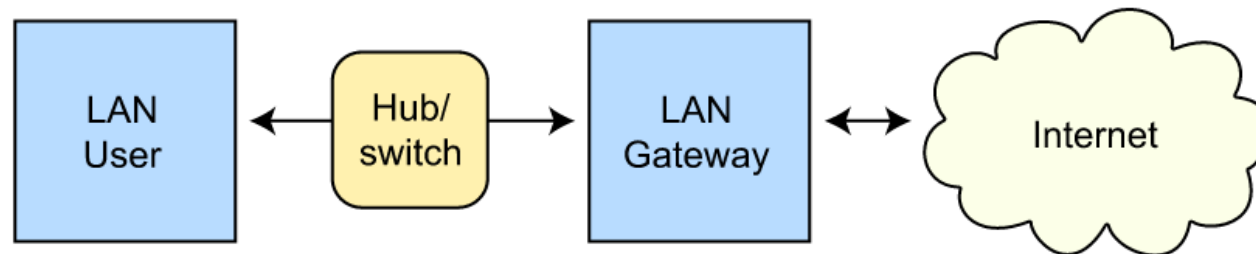
- Cada host mantém uma tabela com os endereços ARP conhecidos (ARP Cache)
  - Evita gerar tráfego desnecessário na rede
- Cada entrada da tabela tem um tempo de validade (normalmente 20 min)
  - Após esse período, o endereço é descartado
  - Próxima transmissão para esse IP necessitará uma nova troca de ARP request/reply
- Essa tabela também pode ser modificada pelo usuário
  - Ex: adicionar entrada estaticamente ou remover

# Casos particulares

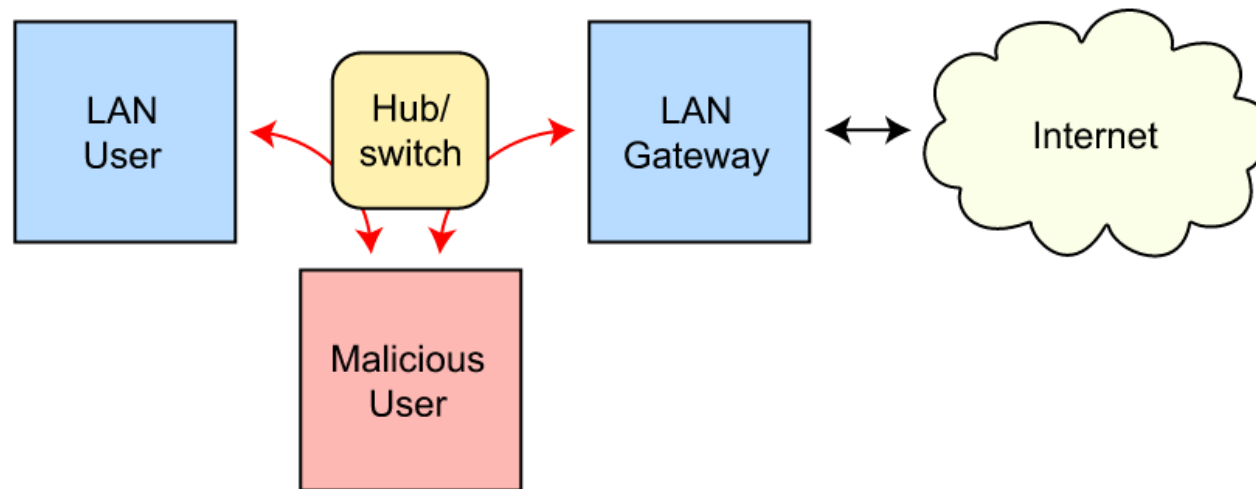
- Gratuitous ARP
  - Envio de ARP request o próprio IP
  - Host envia um Gratuitous ARP na inicialização
    - Exemplo: pode ser usado para detectar IP duplicado ou mudança da placa de rede
- ARP reply não solicitado
  - ARP spoofing
  - Migração de máquinas virtuais
- ARP request para um host inexistente
  - Timeout do protocolo de alto nível (ex: conexão TCP)

# ARP Spoofing

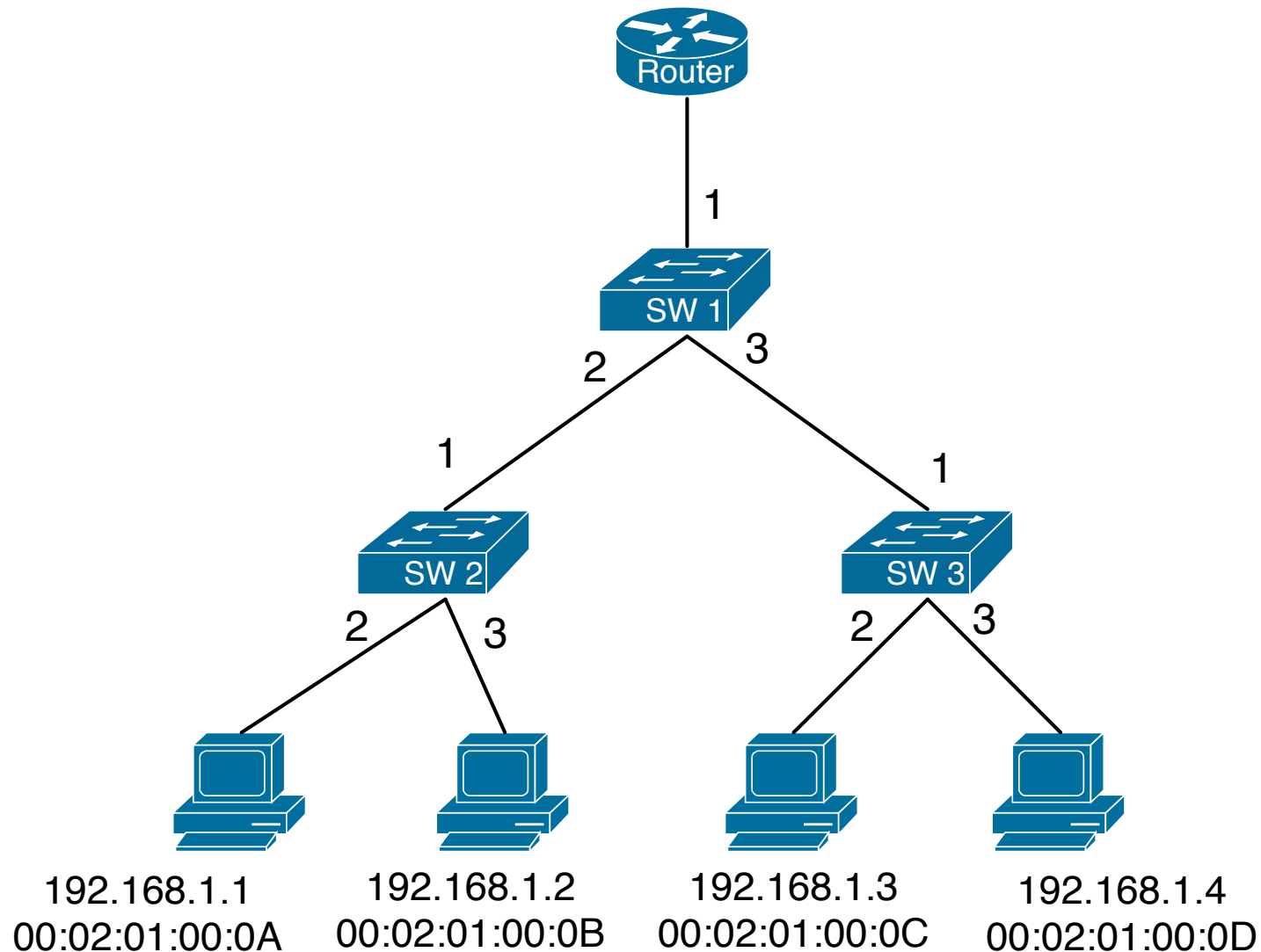
## Routing under normal operation



## Routing subject to ARP cache poisoning



Como enviar um frame Ethernet do 192.168.1.1  
para o 192.168.1.4?



# Referências

- Esse material foi baseado nos slides da Profa. Cristina Nunes (PUCRS) e no livro do Andrew Tanenbaun.
- Tanenbaun, A. Redes de Computadores, Quarta edição. Editora campus.