

# Redes de Computadores TCP/IP

Fabricio Breve

# Fundamentos

- Atualmente é o protocolo mais usado em redes locais
  - Principal responsável: Popularização da Internet
  - Mesmo SOs que antigamente só suportavam seu protocolo proprietário hoje suportam TCP/IP
    - WindowsNT com seu NETBEUI
    - Netware com seu IPX/SPX

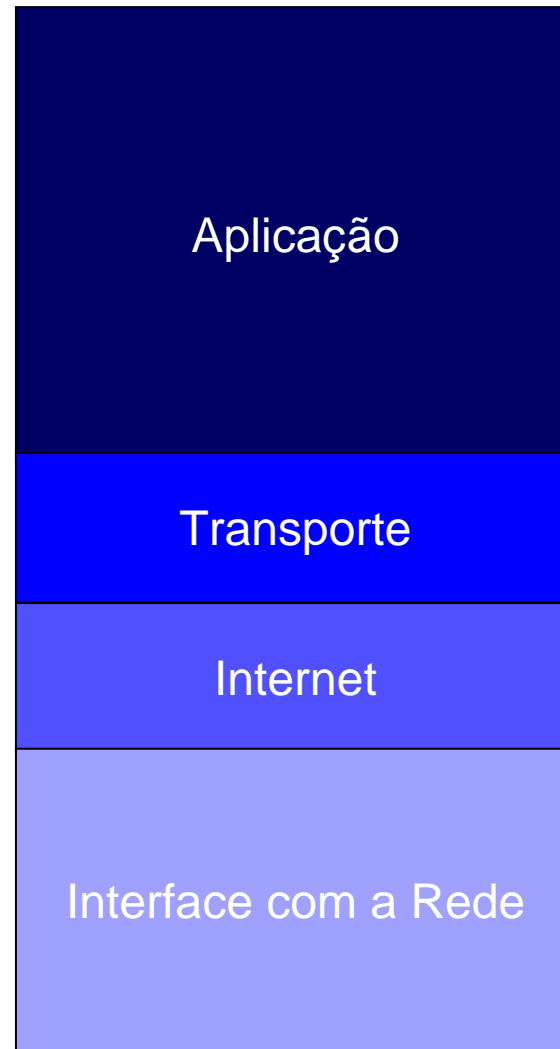
# Fundamentos

- É roteável, foi criado pensando em redes grandes e de longa distância, onde pode haver vários caminhos para chegar ao destino
- Arquitetura aberta
  - Qualquer fabricante pode adotar sua própria versão do TCP/IP em seu SO sem pagar direitos autorais
    - Todos os fabricantes acabaram adotando TCP/IP
    - Protocolo Universal

# Arquitetura TCP/IP



Modelo OSI



TCP/IP

# Arquitetura TCP/IP

- TCP/IP é na realidade um conjunto de protocolos
  - TCP: Transmission Control Protocol
  - IP (Internet Protocol)
    - Operam nas camadas de Transporte e Internet respectivamente
    - Não são os únicos

# Camada de Aplicação

- Equivale às camadas 5, 6 e 7 do modelo OSI
  - Faz a comunicação entre aplicativos e a camada de transporte
  - Os protocolos mais conhecidos:
    - HTTP (HyperText Transfer Protocol)
    - SMTP (Simple Mail Transfer Protocol)
    - FTP (File Transfer Protocol)
    - SNMP (Simple Network Management Protocol)
    - DNS (Domain Name System)
    - Telnet

# Camada de Aplicação

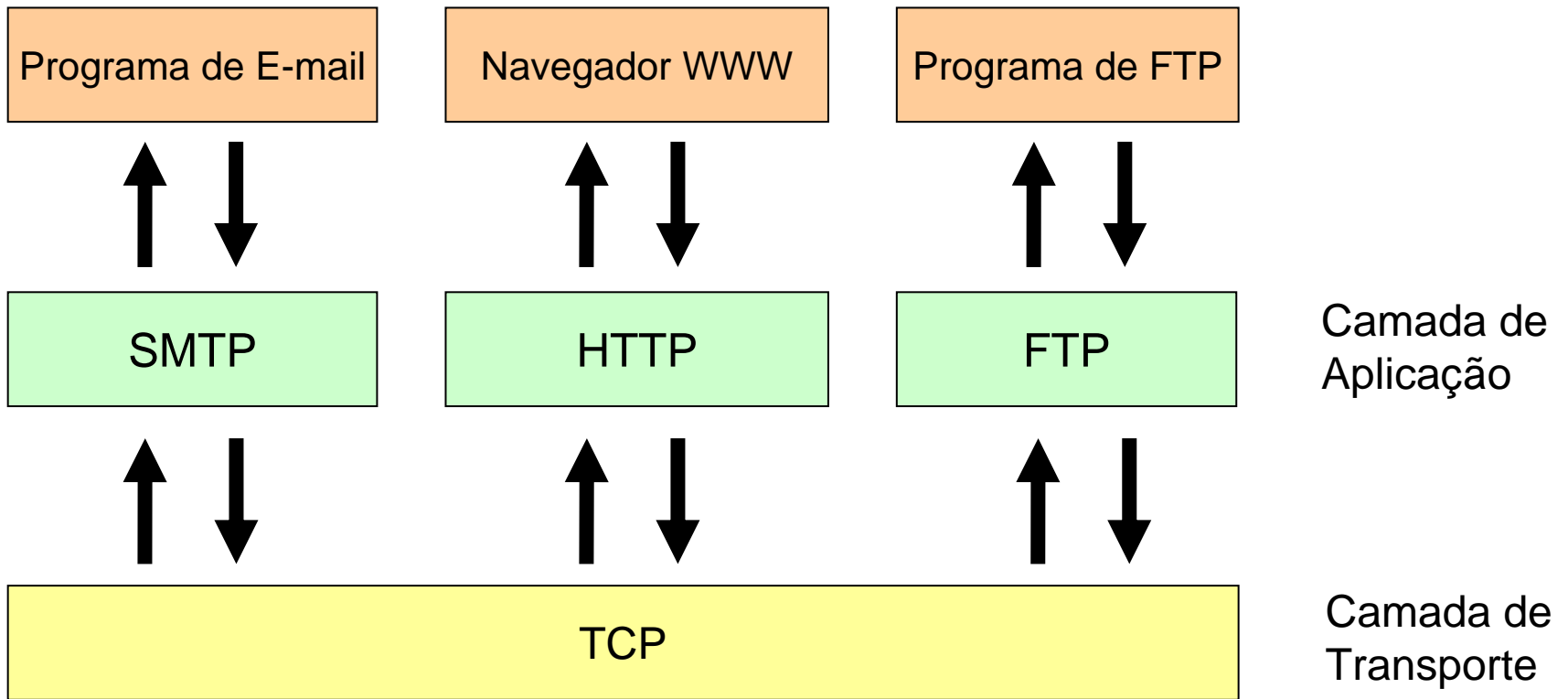
- Comunica-se com a camada de transporte através de uma *porta* (ou *porto*)
- Portas são numeradas e as aplicações padrão usam sempre a mesma porta
  - Exemplos:
    - SMTP utiliza a porta 25
    - HTTP utiliza a porta 80
    - FTP as portas 20 (dados) e 21 (informações de controle)

# Camada de Aplicação

- Uso de portas: permite ao protocolo de transporte (tipicamente o TCP) saber qual é o tipo de conteúdo do pacote de dados
  - No receptor, ao receber um pacote na porta 25 irá entregá-lo ao protocolo conectado a essa porta (tipicamente SMTP), que por sua vez irá repassá-lo para a aplicação (programa de e-mail)



# Funcionamento da camada de aplicação



# Camada de Transporte

- A camada de transporte do TCP/IP é um equivalente direto da camada de transporte (4) do modelo OSI
  - Responsável por pegar dados enviados pela aplicação e transformá-los em pacote para serem repassados para a camada de Internet
- Multiplexação: é possível transmitir dados das mais diferentes aplicações “simultaneamente”
  - Intercalamento de pacotes
    - Possível graças ao conceito de portas

# Camada de Transporte

- Nesta camada operam dois protocolos
  - TCP (Transmission Control Protocol)
    - Mais utilizado na transmissão de dados
  - UDP (User Datagram Protocol)
    - Não verifica se o dado chegou ou não ao destino
    - Mais usado na transmissão de informações de controle

# Camada de Transporte

- Recepção:
  - Pega os pacotes passados pela camada Internet
  - Coloca os pacotes em ordem e verifica se todos chegaram corretamente
    - Quadros podem seguir caminhos diferentes e chegarem fora de ordem
  - O protocolo IP (camada de Internet) não verifica se o pacote de dados chegou ao destino; ficando o TCP com essa tarefa (eventualmente pedindo uma retransmissão)

# Camada de Internet

- Equivale a Camada de Rede (3) do modelo OSI
  - Todas as explicações dadas sobre essa camada no modelo OSI são 100% válidas para a camada de Internet do TCP/IP
- Vários protocolos podem operar nessa camada:
  - IP (Internet Protocol)
  - ICMP (Internet Control Message Protocol)
  - ARP (Address Resolution Protocol)
  - RARP (Reverse Address Resolution Protocol)

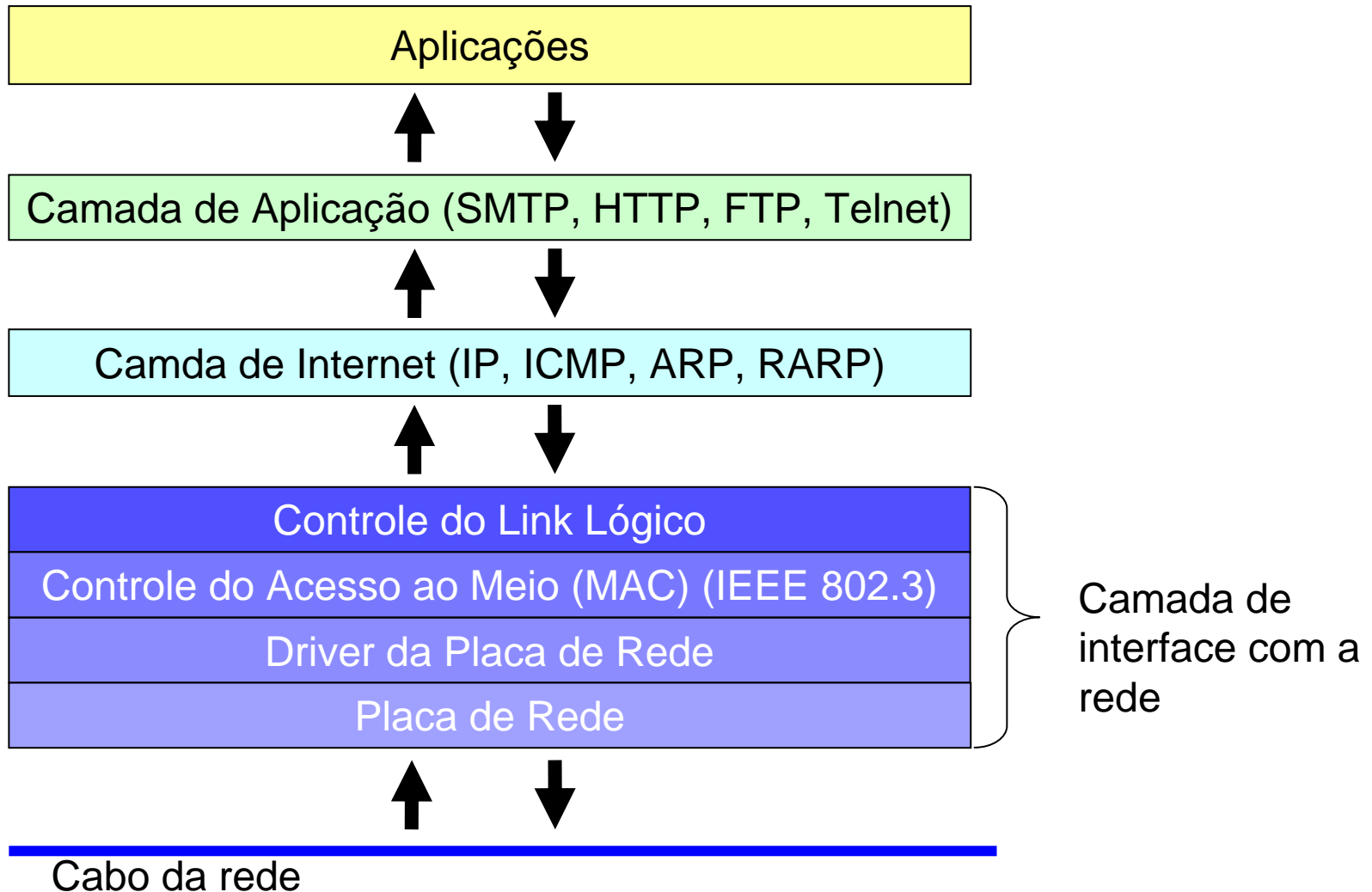
# Camada de Internet

- Pacote de dados recebido da camada TCP é dividido em pacotes chamados *datagramas*
  - Datagramas são enviados para a camada de interface com a rede, onde são transmitidos pelo cabeamento de rede através de quadros
- Não verifica se os dados chegaram ao destino, isso é feito pelo TCP
- Responsável pelo roteamento de pacotes
  - adiciona informações ao datagrama sobre o caminho que ele deverá percorrer

# Camada de Interface com a Rede

- Equivale as camadas 1 e 2 do modelo OSI
- Responsável por enviar o datagrama recebido pela camada de Internet em forma de um quadro através da rede

# Funcionamento do TCP/IP



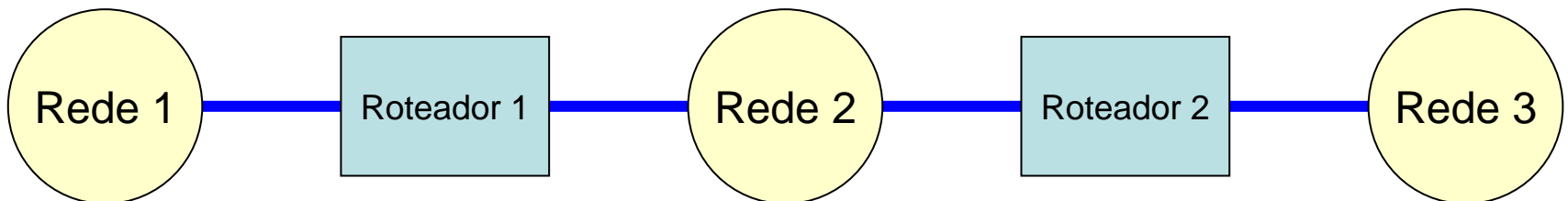


# Endereçamento IP

- TCP/IP é roteável, foi criado pensando na interligação de diversas redes (podem haver vários caminhos entre o transmissor e o receptor)
- Cada dispositivo conectado em rede necessita usar pelo menos um endereço IP
- Endereço IP permite identificar o dispositivo e a qual rede ele pertence

# Endereçamento IP

- As redes são interligadas através de dispositivos chamados *roteadores*
  - Quando um computador da rede 1 quer enviar um pacote de dados para um computador da rede 3, ele envia o pacote para o roteador 1, que então repassa esse pacote diretamente ao roteador 2, que se encarrega de fazer a entrega ao computador de destino na rede 3



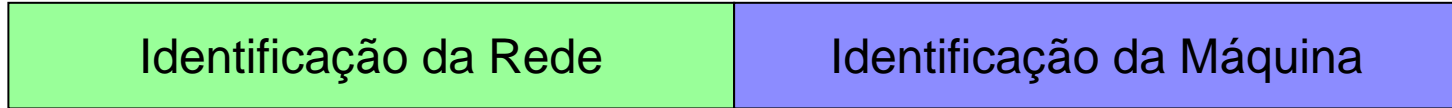
# Endereçamento IP

- A entrega é feita facilmente pelo roteador pois os pacotes possuem o endereço IP do computador de destino
  - Nesse endereço há informação de em qual rede o pacote deve ser entregue
  - O roteador 1 sabe que o destinatário não está na rede 2 e portanto o envia diretamente para o roteador 2

# Endereçamento IP

- Redes TCP/IP tem um ponto de saída chamado *gateway*
  - Todos os pacotes de dados recebidos que não são para aquela rede vão para o gateway
  - As redes subseqüentes vão enviando os pacotes a seus respectivos gateways até que cheguem ao destino
  - Isso é possível porque o endereço IP possui duas partes (próximo slide)

# Campo de um endereço IP



- O endereço IP é um número de 32 bits, representado em decimal em forma de 4 números de 8 bits separados por um ponto no formato a.b.c.d
  - Menor endereço possível: 0.0.0.0
  - Maior endereço possível: 255.255.255.255

# Endereçamento IP

- Teoricamente um endereço TCP/IP pode ter até 4.294.967.296 endereços IP ( $256^4$ )
  - Porém alguns endereços são reservados e não podem ser usados
- Logo esse limite máximo será atingido, por isso já foi padronizado o endereçamento usando 128 bits em vez de 32, chamado IPv6
  - Também chamado IP Next Generation (IPng) ou Simple Internet Protocol Plus (SIPP)
  - Ainda não usado comercialmente
  - É possível endereçar 340.282.366.920.938.463.463.374.607.431.770.000.000 dispositivos diferentes
  - Daria para ter 1.564 endereços IP por metro quadrado da superfície do planeta Terra

# Endereçamento IP

- Cada dispositivo de uma rede TCP/IP precisa ter um endereço IP único, para que o pacote de dados consiga ser entregue corretamente
  - Você terá que obrigatoriamente usar endereços que não estejam sendo usados por nenhum outro computador da rede

# Classes de Endereços IP

a | b | c | d

Classe A	0	Identificação da rede (7 bits)	Identificação da máquina (24 bits)
Classe B	10	Identificação da rede (14 bits)	Identificação da máquina (16 bits)
Classe C	110	Identificação da rede (21 bits)	Identificação da máquina (8 bits)
Classe D	1110	Endereçamento multicast	
Classe E	1111	Reservado para uso futuro	



# Classes de Endereços IP

<b>Classe</b>	<b>Endereço mais baixo</b>	<b>Endereço mais alto</b>
A	1.0.0.0	126.0.0.0
B	128.1.0.0	191.255.0.0
C	192.0.1.0	223.255.255.0
D	224.0.0.0	239.255.255.255
E	240.0.0.0	255.255.255.254

\* alguns endereços não constam na tabela por serem de uso reservado

# Endereçamento IP

- Em rede usamos somente as classes A, B e C

<b>Classe</b>	<b>Números para Identificação da Rede</b>	<b>Números para Identificação da máquina</b>	<b>Quantidade de máquinas na rede</b>
<b>A</b>	1	3	16.777.216
<b>B</b>	2	2	65.536
<b>C</b>	3	1	256

# Endereçamento IP

- Os endereços 0 e 255 são reservados, então na prática o número de máquinas por rede é menor
  - Exemplo: Classe C: 254 máquinas
- A escolha da classe da rede depende de seu tamanho
  - Grande maioria usa classe C
- O sistema de redes que forma a estrutura básica da Internet é chamado *backbone*, e para estar na internet você deve estar ligado a ele de alguma forma (diretamente ou indiretamente)

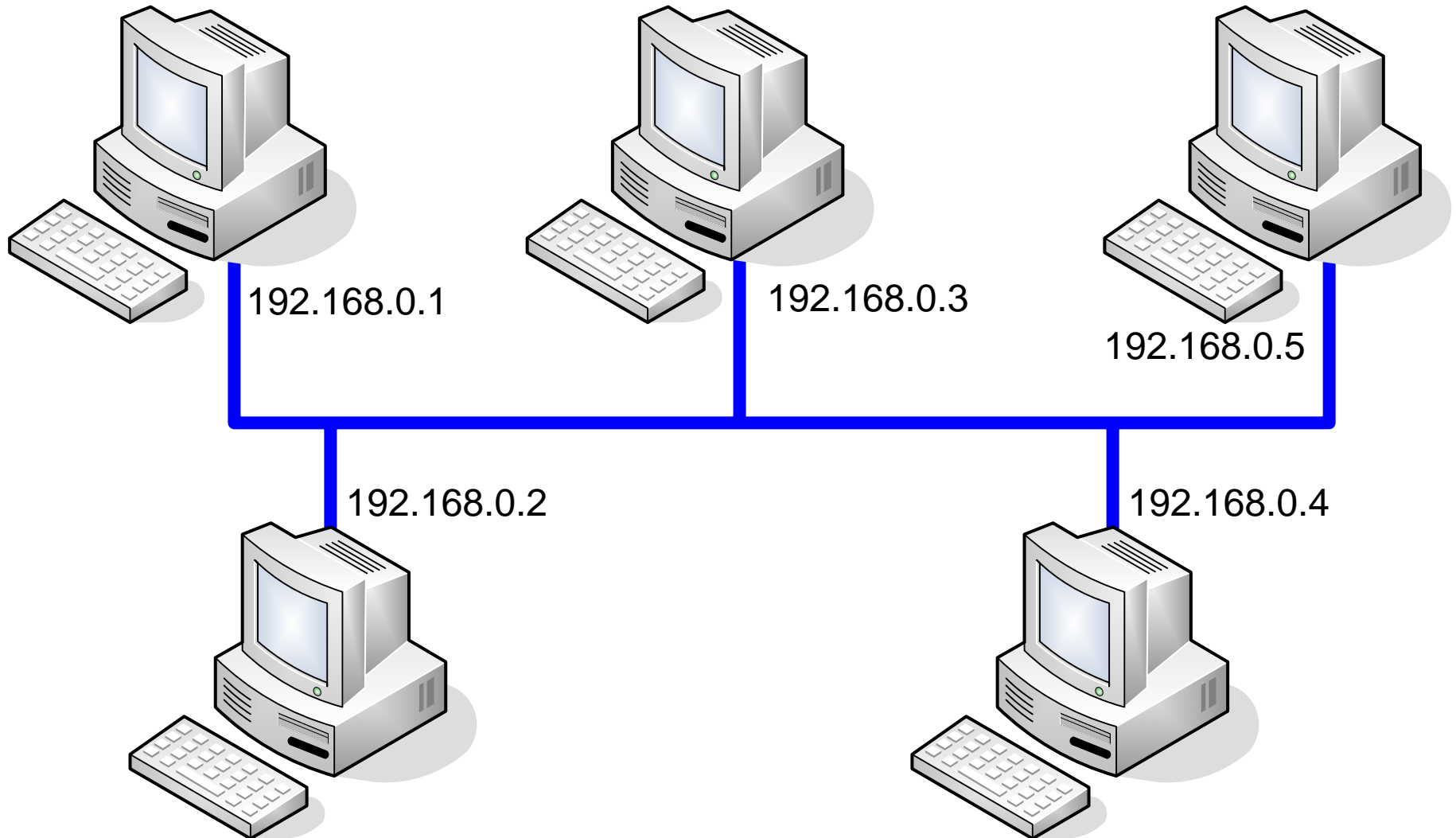
# Endereçamento IP

- A Internet possui uma estrutura hierárquica
  - Responsável pelo backbone é responsável pelo controle e fornecimento de endereços IPs a seus subordinados
  - Por sua vez, os IPs de um backbone foram atribuídos pelo backbone hierarquicamente superior a ele
- Teoricamente, se sua rede não está na Internet você pode usar quaisquer endereços IPs, mas se mais tarde ela for conectada, o conflito será inevitável.

# Endereçamento IP

- Alguns endereços IPs são reservados para redes privadas
  - Roteadores reconhecem esses endereços como sendo de redes particulares e não os repassam para o resto da Internet
    - Mesmo que um roteador esteja configurado errado e passe o pacote adiante, outro roteador configurado corretamente irá barrá-lo
  - Endereços especiais reservados para redes privadas:
    - Classe A: 10.0.0.0 a 10.255.255.255
    - Classe B: 172.16.0.0 a 172.31.255.255
    - Classe C: 192.168.0.0 a 192.168.255.255

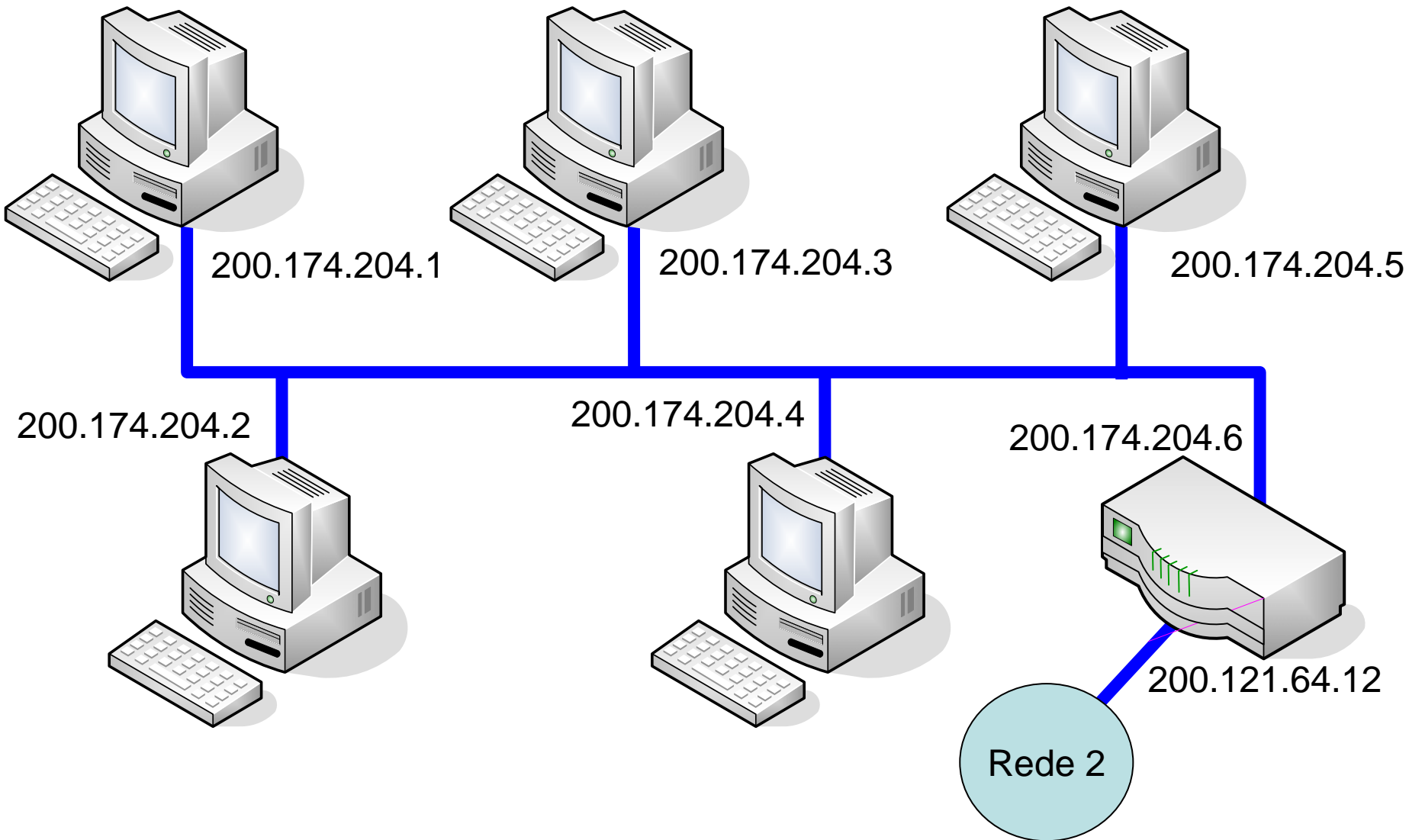
# Exemplo de uma rede TCP/IP



# Endereçamento IP

- O endereço 255 é reservado para *broadcast* (enviar um pacote de dados para todas as máquinas da rede ao mesmo tempo)
- Para conectar essa rede a Internet existem duas soluções
  - A primeira seria obter um endereço classe C público e atribuir um IP único na Internet e válido dentro da rede

# Exemplo de uma rede TCP/IP conectada a Internet





# Endereçamento IP

- Outra solução para conectar a rede à Internet é criar uma tabela de tradução no roteador, que pega os pacotes vindos com endereços IPs válidos na Internet e converte esses endereços em endereços privados, aceitos somente na rede local. Essa tradução pode ser estática ou dinâmica.
  - **Estática:** um determinado endereço privado sempre é convertido em um mesmo endereço público
  - **Dinâmica:** é usada por clientes que não precisam prestar serviço para a rede. Assim mais de um endereço privado pode estar usando um mesmo IP público.

# Endereçamento IP

- DHCP (Dynamic Host Configuration Protocol)
  - Permite atribuição automática ou manual de endereços IPs para computadores da rede
  - Quanto um cliente solicita um endereço IP o servidor DHCP atribui um IP a ele por um certo período (que deverá ser renovado quando o prazo estiver espirando)

# Máscara de Rede

- É formada por 32 bits no mesmo formato que o endereço IP e cada bit 1 da máscara informa a parte do endereço IP que é usada para o endereçamento da rede e cada bit 0 informa a parte do endereço IP que é usada para o endereçamento das máquinas. Dessa forma as máscaras padrões são:
  - Classe A: 255.0.0.0
  - Classe B: 255.255.0.0
  - Classe C: 255.255.255.0
- Valores fora do padrão podem ser usados quando houver necessidade de segmentar a rede

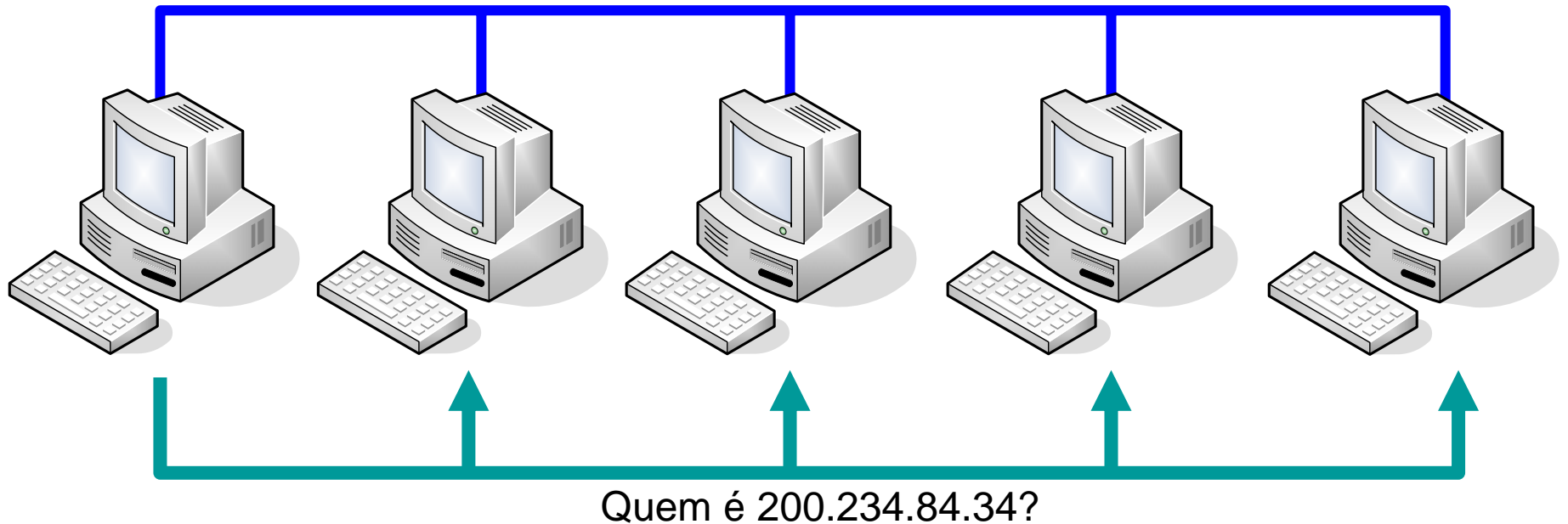
# ARP (Address Resolution Protocol)

- As redes TCP/IP baseiam-se em um endereçamento virtual (IP), mas as placas de rede utilizam endereçamento MAC
- O protocolo ARP é responsável por fazer a conversão entre endereços IPs e os endereços MAC da rede.
  - Em uma grande rede, os pacotes TCP/IP são enviados até a rede de destino através dos roteadores
  - Atingindo a rede de destino o protocolo ARP entra em ação para detectar o endereço da placa de rede para qual o pacote deve ser entregue, já que no pacote há somente o endereço IP

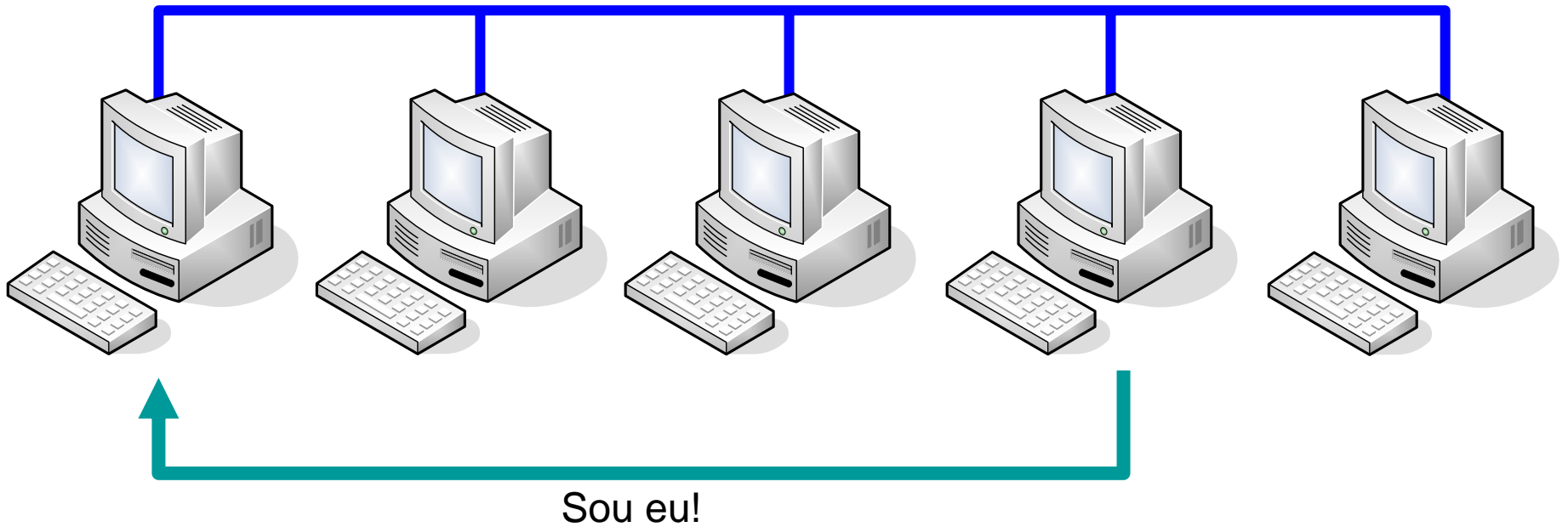
# ARP (Address Resolution Protocol)

- Funciona primeiramente enviando uma mensagem de broadcast para a rede perguntando a todas as máquinas qual responde pelo IP destinatário do pacote que chegou
- A máquina responsável por tal IP responde, identificando-se e informando seu endereço MAC para que a transmissão possa ser feita
- O dispositivo armazena os endereços IPs recentemente usados e seus endereços MACs correspondentes em uma tabela na memória

# ARP (Address Resolution Protocol)



# ARP (Address Resolution Protocol)



# RARP (Reverse Address Resolution Protocol)

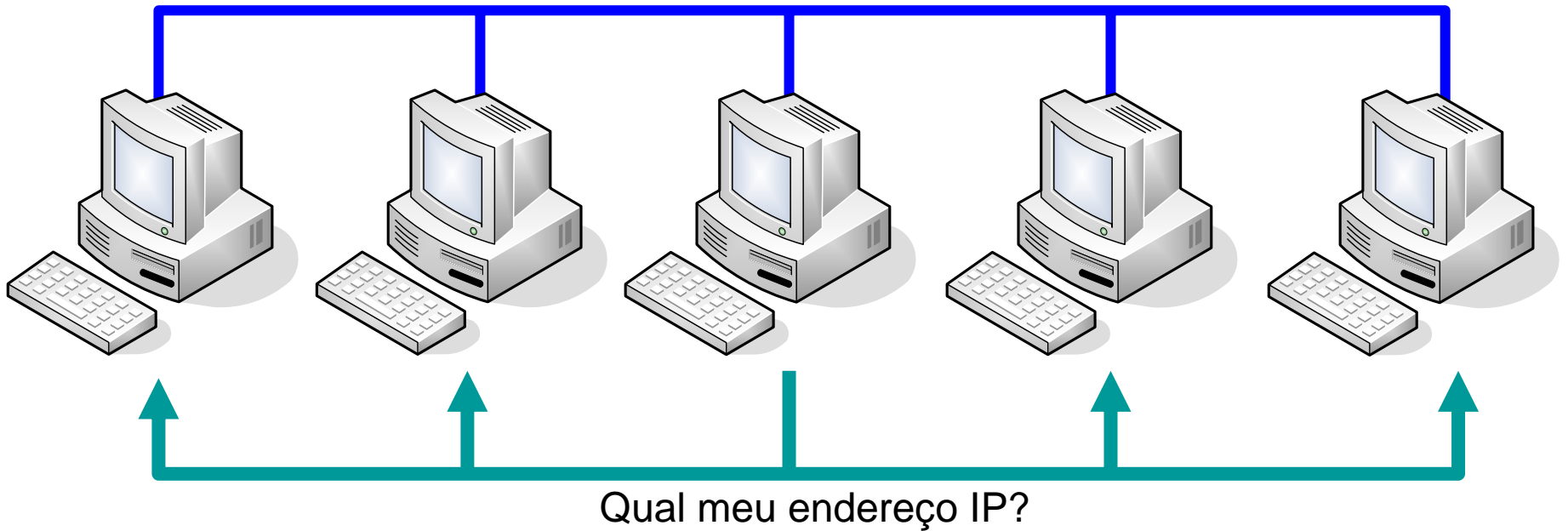
- Permite que uma máquina descubra um endereço IP através de um endereço MAC, fazendo o inverso do que o protocolo ARP faz
- Quando ligamos um computador ele não sabe seu endereço IP
  - Essa informação estará gravada no disco rígido ou alguma memória não volátil
  - Estações com boot remoto não tem como saber seu endereço IP, e portanto não tem como usar TCP/IP



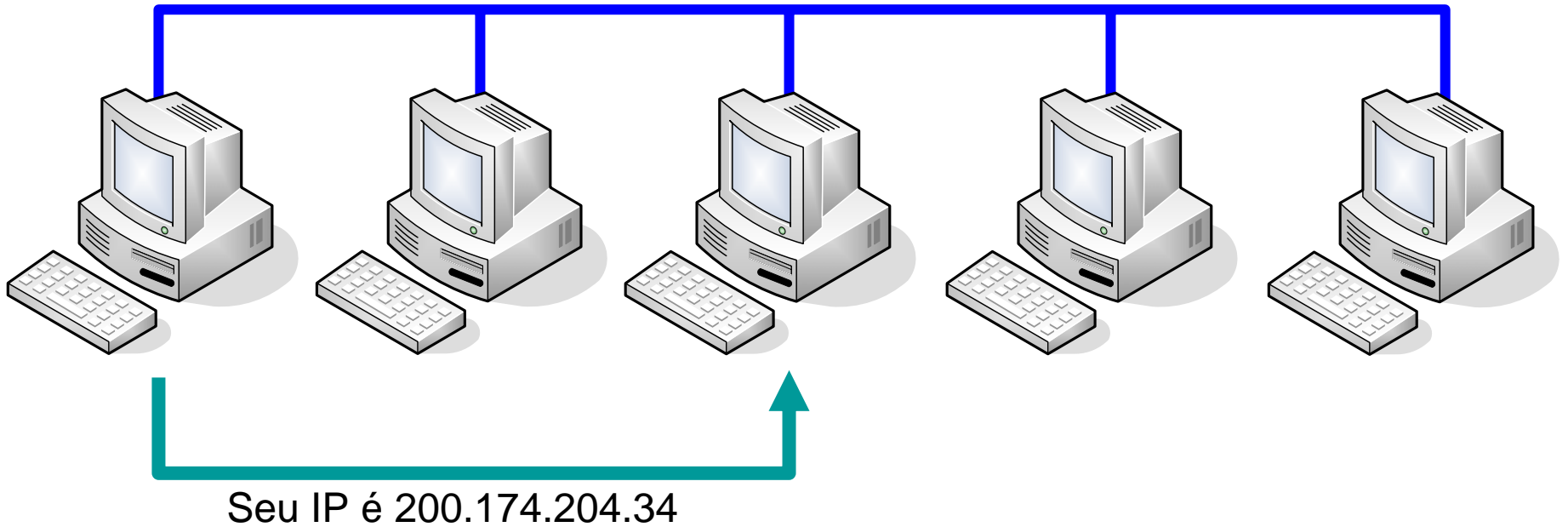
# RARP (Reverse Address Resolution Protocol)

- Nesses casos utilizamos um servidor RARP, que armazena uma tabela com os endereços MACs das máquinas da rede e seus respectivos IPs
- Uma máquina que precisa saber seu próprio endereço IP envia um pedido para todas as máquinas, mas somente o servidor RARP responde, informando seu IP
- A partir daí, o endereço IP ficará na memória RAM da máquina

# RARP (Reverse Address Resolution Protocol)



# RARP (Reverse Address Resolution Protocol)



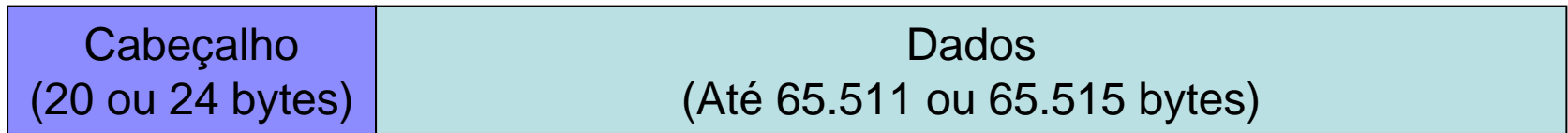
# IP (Internet Protocol)

- Pega os dados enviados pela camada de transporte (TCP ou UDP) e envia para a camada física
  - Na camada física os datagramas serão empacotados em quadros (como já vimos anteriormente)
- IP não é orientado a conexão
  - Não verifica se o datagrama chegou ao destino
    - Isso é feito pelo TCP, que pega os dados que estão chegando e os coloca em ordem, pedindo uma retransmissão caso algum dado esteja faltando

# IP (Internet Protocol)

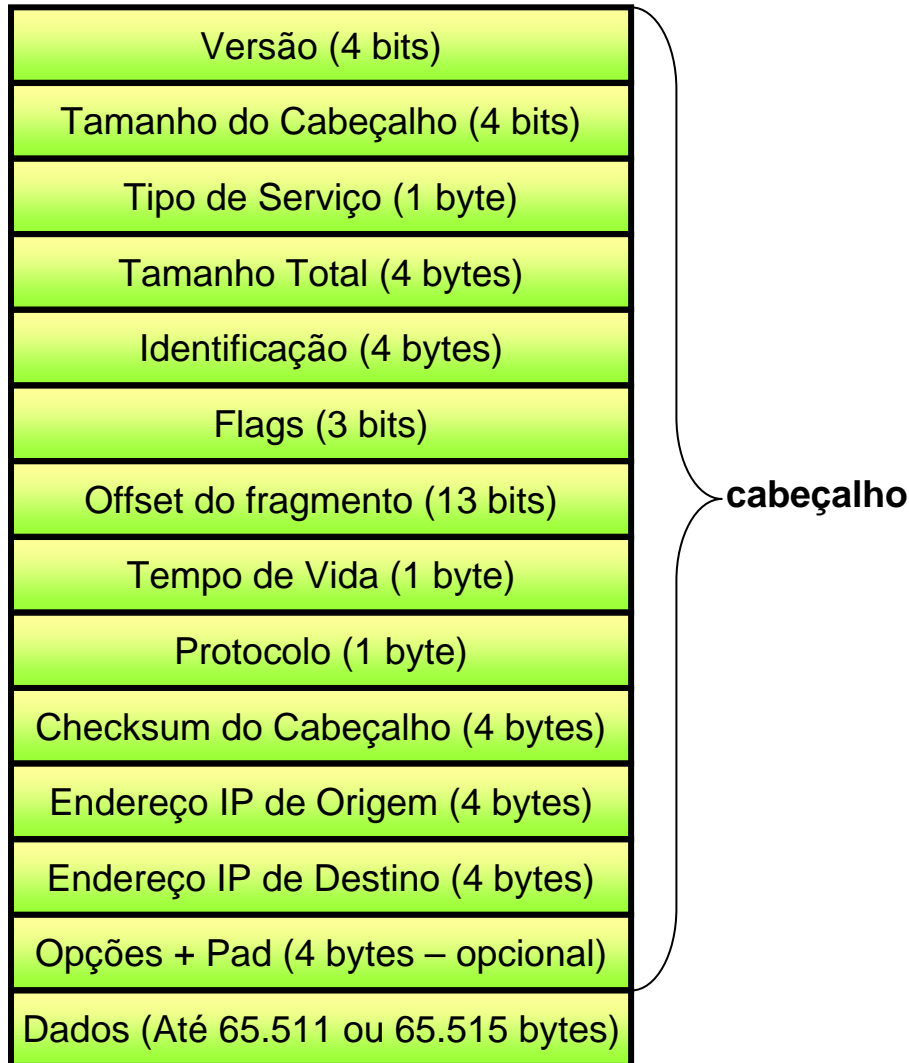
- Principal função: roteamento
  - Adicionar mecanismos para que o datagrama chegue o mais rápido possível ao destino
    - Feito com auxílio dos roteadores de rede
      - Escolhem o caminho mais rápido entre a origem e o destino

# Estrutura do Datagrama IP



Estrutura simplificada

# Estrutura do Datagrama IP



- O campo Opções+Pad pode não existir, reduzindo o tamanho do cabeçalho para 20 bytes
- A área de dados não tem tamanho fixo, portanto o tamanho do datagrama IP é variável
- O tamanho máximo é 65.535 (incluindo o cabeçalho)

# Estrutura do Datagrama IP

- **Versão:** indica a versão do protocolo IP que está sendo usado. O protocolo IP que estamos descrevendo é o IPv4
  - Portanto encontraremos o valor 4 nesse campo
- **Tamanho do cabeçalho** (IHL, Internet Header Length): indica o comprimento do cabeçalho do datagrama, dado em número de palavras de 32 bits
- **Tipo de Serviço:** informa a qualidade desejada para entrega do datagrama, falaremos dele mais adiante
- **Tamanho Total:** número total de bytes que compõem o datagrama. Esse campo possui 16 bits, portanto o tamanho máximo do datagrama é 65.535 bytes ( $2^{16}$ )
  - Quanto maior o datagrama, mais a estação ocupa a rede (deixando-a mais lenta), portanto normalmente utiliza-se valores bem menores que 65.535 bytes, um valor comum é 576 bytes.
- **Identificação:** quando um datagrama é criado recebe um número de identificação que será usado para identificá-lo caso ele seja fragmentado no caminho até o destino



# Estrutura do Datagrama IP

- **Flags:** usado para controlar a fragmentação de datagramas, será estudo mais adiante
- **Offset do Fragmento:** usado para controle da fragmentação de datagramas, também explicado mais adiante
- **Tempo de Vida (TTL):** tempo máximo de vida do datagrama, cada vez que o datagrama passa por um gateway (um roteador, por exemplo) esse número é decrementado.
  - Quando chega a zero o datagrama é descartado, não atingindo o destino
  - No receptor o protocolo IP percebe que está faltando um datagrama e pede retransmissão
  - Objetivo: eliminar datagramas que demorem muito para chegar ao destino (rota muito longa ou mesmo errada devido a roteador mal configurado no caminho)
- **Protocolo:** indica o protocolo que pediu o envio do datagrama, através de um código numérico
  - Exemplo: número 6 indica TCP, 17 indica UDP

# Estrutura do Datagrama IP

- **Checksum do Cabeçalho:** cálculo do checksum somente do cabeçalho (não usa os dados no cálculo)
  - Conta menor e mais rápida de ser feita
  - Os roteadores analisam esse campo e refazem o checksum para saber se o cabeçalho está ou não corrompido
- **Endereço IP de origem:** endereço IP de onde está partindo o datagrama
- **Endereço IP de destino:** endereço IP de destino do datagrama
- **Opções + Pad:** campo opcional. Se não for usado, o cabeçalho passa a ter 20 bytes. Como seu tamanho é variável ele é preenchido com zeros até completar 32 bits (que são conhecidos como *pad* ou *padding*)
  - Usado em testes e verificações de erro na rede
- **Dados:** são os dados que o datagrama está carregando
  - Tamanho máximo de 65.515 bytes ou 65.511 bytes
  - Normalmente utiliza-se valores em torno de 556 bytes

# Tipo de Serviço

- Destinado a distinguir entre diferentes tipos de serviços
- São possíveis várias combinações de confiabilidade e velocidade
  - Exemplos de prioridade:
    - Voz digitalizada: velocidade
    - Arquivos de dados: segurança
- Teoricamente serviria para um servidor optar por um enlace dependendo do serviço
  - Exemplo:
    - Conexão de satélite para arquivos (latência alta, velocidade alta)
    - Conexão ISDN para voz (latência baixa, velocidade baixa)
- Na prática os roteadores atuais ignoram completamente esse campo

# Fragmentação de datagramas

- Quando os datagramas são enviados à rede através da camada Física, seu tamanho fica limitado ao da área de dados do protocolo usado nessa camada.
  - Por exemplo: em uma rede Etherneto tamanho máximo é 1500 bytes
  - Essa característica é chamada MTU (Maximum Transfer Unit)
  - O pacote passa por vários roteadores antes de chegar a seu destino, e pode encontrar roteadores com diferentes MTU
  - A solução é a fragmentação de datagramas
    - Dividi-los em 2 ou mais quadros menores e depois juntá-los novamente

# ICMP (Internet Control Message Protocol)

- Mecanismo utilizado pelos roteadores para informar que um problema ocorreu
  - Congestionamento
  - TTL de datagrama zerado
- Ele apenas informa a máquina transmissora que um erro ocorreu
  - Não se importa em corrigi-lo
- Parte integrante do IP

# ICMP (Internet Control Message Protocol)

- Eco: utilizado para saber se o caminho entre o transmissor e o receptor está bom
  - Ping
- Destino Inalcançável: enviada quando o roteador não consegue entregar o datagrama
- Congestionamento: se o roteador está recebendo mais datagramas do que consegue processar, ele começa a descartá-los, e informa a máquina transmissora para diminuir a velocidade
- Redirecionamento: o roteador pode verificar que há uma rota melhor para ser usada, e avisa o transmissor
- Tempo de Vida excedido: se o TTL do datagrama é zerado, o roteador informa o transmissor
- Problema nos Parâmetros: quando o roteador não consegue processar o datagrama e não há outra mensagem ICMP que cubra o problema encontrado, essa mensagem é enviada
- Solicitação de Horário: uma máquina pode pedir o horário do relógio de outra. Pode ser usado para sincronizar o relógio de duas máquinas, mas o atraso da rede impede que a sincronia fique perfeita

# UDP (User Data Protocol)

- Não orientado a conexão
  - Não verifica se os dados chegaram ao destino
  - O protocolo de aplicação deve implementar essa verificação se for necessário
- Vantagem: transmissão de dados mais rápida
  - Cabeçalho menor que o TCP
  - Não precisa esperar mensagens de confirmação
- Viável em redes locais confiáveis
- Na Internet usado apenas quando a taxa de perda de pacotes não seja um problema
  - Streaming de audio e vídeo

# TCP (Transmission Control Protocol)

- Recebe datagramas IP, os coloca em ordem e verifica se todos chegaram corretamente
- Aplicativos enviam e recebem dados pela rede TCP através de canais virtuais de comunicação (http – 80, telnet – 23, etc..)
- TCP empacota os dados adicionando informações de porta de origem e destino, entre outras, passando o pacote de dados ao protocolo IP
- Se o transmissor não recebe uma confirmação de recebimento dentro de um determinado tempo o pacote é enviado novamente



# Conexão

- Comunicação entre duas aplicações em duas máquinas diferentes
- O protocolo TCP é responsável por abri-las, mantê-las e fechá-las
- A abertura é feita através de um processo chamado *handshake*
- A conexão é mantida através do envio de pacotes do transmissor ao receptor
- Se tudo correr bem a transmissão será encerrada quando não houverem mais dados a ser transmitidos

# Protocolos de Aplicação

- DNS (Domain Name System): usado para identificar máquinas através de nomes em vez de endereços IP
- Telnet: usado para comunicar-se remotamente com uma máquina
- FTP (File Transfer Protocol): usado na transferência de arquivos
- SMTP (Simple Mail Transfer Protocol): usado no envio e recebimento de e-mails
- HTTP (Hyper Text Transfer Protocol): usado na transferência de documentos hipermídia (WWW, World Wide Web)

# Questões

1. Qual a diferença entre TCP e UDP? Cite exemplo de utilização de cada um deles
2. Cite 3 protocolos da camada de aplicação do TCP/IP e suas respectivas funções
3. Para que servem as portas (ou portos) no protocolo TCP/IP?
4. Para que serve o protocolo ARP? E o RARP?
5. Para que serve o protocolo ICMP?

# Referências Bibliográficas

- TORRES, Gabriel. *Redes de Computadores: Curso Completo*. Axcel Books, 2001.
- TANENBAUM, Andrew S. *Redes de Computadores*. Campus, 2003.