FEUP Universidade do Porto
Faculdade de Engenharia

Redes de Comunicação

Baseado em *Computer Networks and Internets*,
Douglas E. Comer. Prentice-Hall, 2004.

Computadores e Redes de Comunicação

Mestrado em Gestão de Informação, FEUP 2004/07

Sérgio Sobral Nunes
mail: sergio.nunes@fe.up.pt
web: www.fe.up.pt/~ssn

Sumário

- Motivação e história
- Ferramentas de gestão e diagnóstico
- Transmissão de dados
- Comutação de pacotes
- Topologias de rede
- Protocolos
- Interligação de Redes
- Protocolos TCP/IP
- Aplicações e Serviços de Rede

Motivação

- As primeiras **redes locais** foram implementadas para aumentar instalações existentes. Por exemplo, através da **partilha de dispositivos**, impressoras ou discos externos.

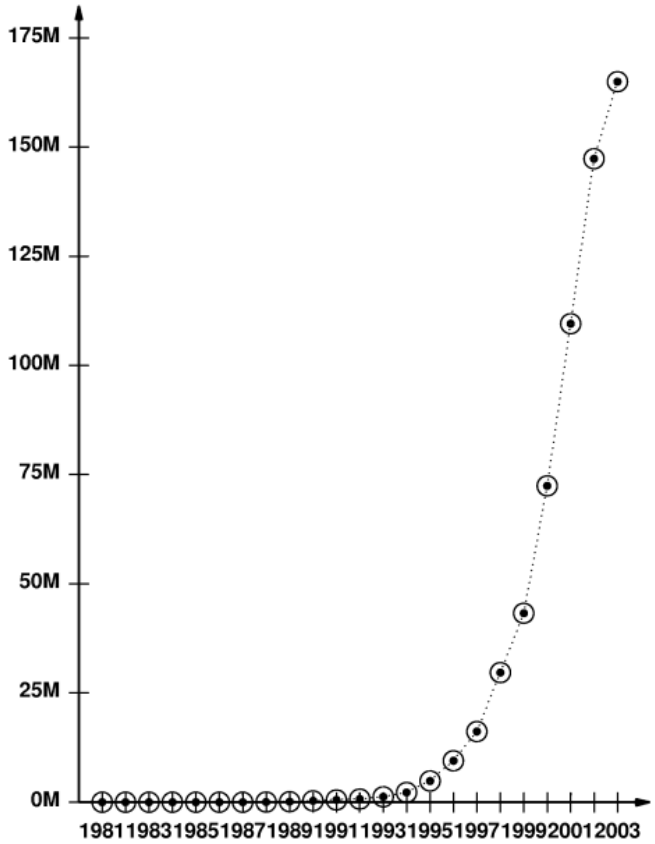
- As **redes de larga escala** surgiram como resposta à necessidade de **partilha de poder computacional**, associado ao elevado custo dos primeiros computadores digitais.

- A investigação desenvolvida pela ARPA foi determinante para o futuro das redes de comunicação. Desenvolvimento da ARPANET nos anos 70.

Breve História

- 60-70
  - Partilha de dispositivos.
  - Redes locais.
- 70
  - Partilha de poder computacional.
  - Departamento de Defesa dos EUA – ARPANET.
- 70-80
  - Investigação – governo e academia.
  - Protocolos TCP/IP.
- 90
  - World Wide Web.
  - Exploração comercial.
  - Migração para redes não governamentais.

Crescimento da Internet



Crescimento da Internet, medido pelo número de computadores ligados à rede (1981 a 2003).

Comando ping

- **`ping`** – envia uma mensagem e espera por uma resposta. Apresenta sumários relativos aos tempos de transferência (ida e volta). Ferramenta de diagnóstico simples mas muito utilizada.

```
gnomo> ping www.google.com
PING www.google.akadns.net (66.102.11.104) 56(84) bytes of data.
64 bytes from 66.102.11.104: icmp_seq=1 ttl=236 time=104 ms
64 bytes from 66.102.11.104: icmp_seq=2 ttl=236 time=87.2 ms
64 bytes from 66.102.11.104: icmp_seq=3 ttl=236 time=86.2 ms
64 bytes from 66.102.11.104: icmp_seq=4 ttl=236 time=86.6 ms
64 bytes from 66.102.11.104: icmp_seq=5 ttl=236 time=86.4 ms

--- www.google.akadns.net ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4044ms
rtt min/avg/max/mdev = 86.246/90.200/104.407/7.120 ms
```

```
gnomo> ping www.up.pt
PING www.up.pt (193.137.55.13) 56(84) bytes of data.
64 bytes from 193.137.55.13: icmp_seq=1 ttl=252 time=1.85 ms
64 bytes from 193.137.55.13: icmp_seq=2 ttl=252 time=2.06 ms
64 bytes from 193.137.55.13: icmp_seq=3 ttl=252 time=2.01 ms
64 bytes from 193.137.55.13: icmp_seq=4 ttl=252 time=4.25 ms
64 bytes from 193.137.55.13: icmp_seq=5 ttl=252 time=2.63 ms

--- www.up.pt ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4040ms
rtt min/avg/max/mdev = 1.853/2.563/4.250/0.884 ms
```

Comando traceroute

- **`traceroute`** – permite determinar as máquinas intermédias no caminho para um destino remoto. No Windows – **`tracert`**.
- Cada linha representa um computador intermédio no caminho entre a origem e o destino especificado (*hop*).

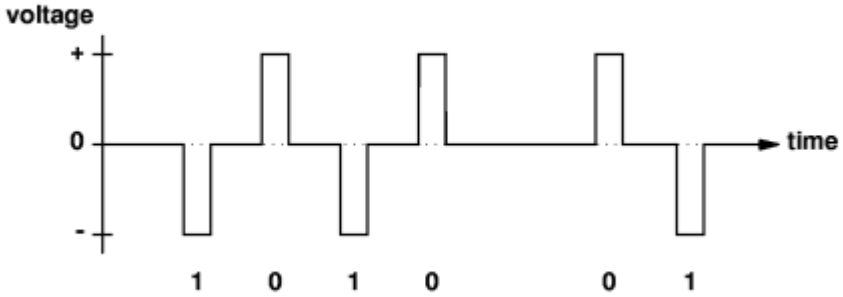
```
gnomo> traceroute www.netbook.cs.purdue.edu
traceroute to lucan.cs.purdue.edu (128.10.19.20), 30 hops max, 38 byte packets
 1  193.136.28.254 (193.136.28.254)  0.638 ms  0.372 ms  0.363 ms
 2  193.136.28.252 (193.136.28.252)  1.154 ms  0.769 ms  0.837 ms
 3  193.136.25.81 (193.136.25.81)  3.990 ms  1.622 ms  8.557 ms
 4  ROUTER15.GE.Porto.fccn.pt (193.136.4.37)  2.533 ms  3.272 ms  2.641 ms
 5  ROUTER11.GE.Porto.fccn.pt (193.137.4.2)  4.811 ms  4.778 ms  3.193 ms
 6  ROUTER8.GE.Lambda.Lisboa.fccn.pt (193.137.1.241)  7.858 ms  9.867 ms  8.369 ms
 7  ROUTER1.GE.Lisboa.fccn.pt (193.137.0.11)  10.322 ms  14.628 ms  8.169 ms
 8  fccn.pt1.pt.geant.net (62.40.103.177)  8.221 ms  8.484 ms  9.101 ms
 9  pt.uk1.uk.geant.net (62.40.96.69)  34.965 ms  38.954 ms  58.354 ms
10  uk.ny1.ny.geant.net (62.40.96.169)  106.332 ms  109.594 ms  105.548 ms
11  198.32.11.61 (198.32.11.61)  104.110 ms  105.105 ms  104.741 ms
12  chinng-nycmng.abilene.ucaid.edu (198.32.8.82)  134.299 ms  133.923 ms  137.245 ms
13  iplsng-chinng.abilene.ucaid.edu (198.32.8.77)  161.063 ms  138.466 ms  143.481 ms
14  192.12.206.250 (192.12.206.250)  138.362 ms  145.344 ms  138.276 ms
15  tel-210-m10-01-gp.tcom.purdue.edu (192.5.40.129)  139.315 ms  139.177 ms  139.618 ms
16  tel-210-c6509-01-campus.tcom.purdue.edu (192.5.40.53)  140.527 ms  140.039 ms  141.898 ms
17  * * *
18  lucan.cs.purdue.edu (128.10.19.20)  140.650 ms  140.423 ms  140.937 ms
```

Transmissão de Dados

Transmissão de Dados

- Ao nível mais baixo, todas as comunicações entre computadores, envolvem a codificação dos dados numa forma de energia e o envio dessa energia através de um **meio de transmissão**.

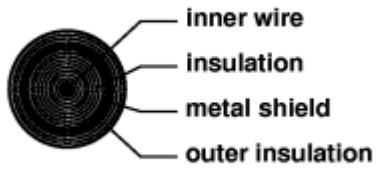
- Meios de transmissão
  - Cabos de cobre
  - Fibra óptica
  - Rádio
  - Satélite
  - Micro-ondas
  - Infravermelhos
  - Laser



Uso de voltagens para a transmissão de bits.

Cabos de Cobre

- Meio mais usado para ligar computadores. Vários tipos de cabos tendo em vista a minimização das interferências:
  - Unshielded Twisted Pair (UTP)
  - Cabo Coaxial
  - Shielded Twisted Pair (STP)

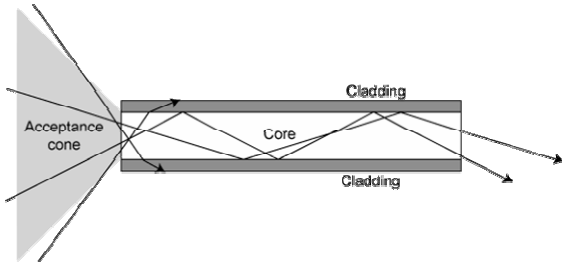


- Vantagens
  - Boa condutividade.
  - Baixo custo.
  - Fácil instalação.

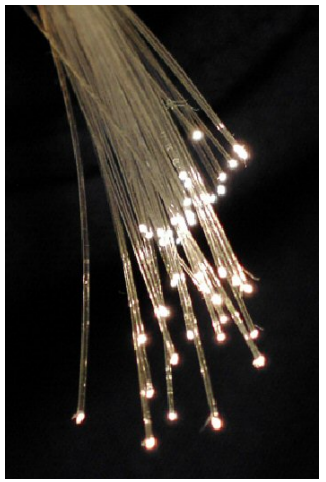
- Desvantagens
  - Vulnerável ao ruído electromagnético.

Fibra Óptica

- Emissão de um impulsos de luz através de uma fibra de vidro flexível.



- Vantagens
  - Imunes a interferências electromagnéticas.
  - Menores perdas.
  - Maior débito.



- Desvantagens
  - Interfaces dispendiosas.
  - Resolução de problemas difícil.

Rádio

- Utilização da radiação electromagnética para transmissão de dados entre computadores. Uma rede deste tipo funciona numa determinada **rádio frequência**.

- A dimensão da antena emissora/receptora determina o alcance da rede.

- Não é necessária uma ligação física directa.

- As redes *wireless* são um exemplo de aplicação.

Satélite

- Utilizados para transmissão ao longo de grandes distâncias. Dois tipos em função da altura da órbita:
  - Geoestacionários – mantêm-se sincronizados com a rotação da Terra. Instalados a 36.000Km de altura.
  - Baixa Órbita Terrestre – Próxima dos 700Km.

- Uma configuração em malha pode ser utilizada com os satélites de baixa órbita, permitindo uma cobertura permanente. Nestes casos, uma comunicação em particular por recorrer a vários satélites.

- Devido ao custo elevado de instalação inicial, é comum várias ligações serem partilhadas pelo mesmo satélite.

Satélite

Micro-Ondas

- Recurso à radiação electromagnética em gamas de frequência para além daquelas utilizadas pela rádio ou televisão.

- Uma transmissão micro-ondas pode ser direccionada, ao contrário do que acontece com as outras ondas. Permitem também o transporte de mais informação.

- Mais susceptíveis a interferências. A instalação é feita com linha de vista.

Infravermelhos

- Tecnologia de radiação electromagnética usada nos telecomandos.

- Vantagens:
  - Boa segurança.
  - Ausência dos problemas de interferência.
  - Espectro não licenciado.

- Desvantagens:
  - Limitada a distâncias curtas.
  - Transmissão em linha de vista ou por reflexão.

Laser

- Um **feixe de luz direccionado** através do ar pode ser usado para transmitir dados.
- A transmissão é feita em linha recta e não pode ser bloqueada.
- Muito vulnerável a interferências por isso de uso limitado.

Sinal Contínuo Oscilatório

- Uma corrente eléctrica não pode ser propagada uma distância arbitrária. Há uma **perda de sinal** em função da distância devido à resistência.

- Os protocolos utilizados para comunicação local (p.e. RS-232) não podem ser utilizados em grandes distâncias.

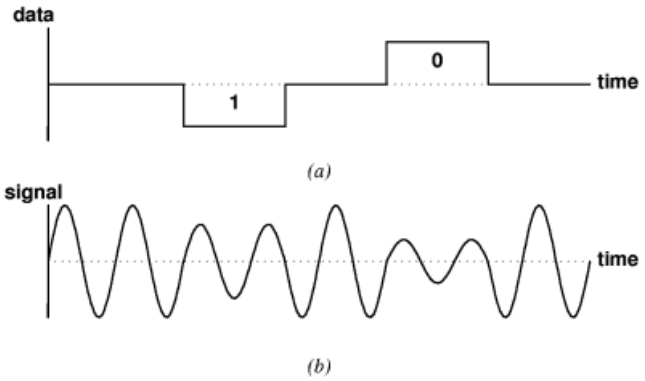
- Em transmissões de longa distância um **sinal contínuo oscilatório** propaga-se melhor do que outro tipo de sinais.

- Em vez de enviar um sinal que muda apenas com o valor, nas comunicações de longa distância, é utilizado um sinal contínuo oscilatório (*portadora*).

Modulação

- Para enviar dados, o sinal é alterado. De uma forma geral, estas alterações são designadas por **modulação**.

- Tecnologia desenvolvida no contexto dos telefones, rádio e televisão.



(a) Sinal digital. (b) Onda que resulta com a modulação. Valor 1 é codificado reduzindo a 2/3 a onda, o valor 0 reduzindo a 1/3.

Modulação e Desmodulação

- Um aparelho que recebe uma sequência de bits e aplica modulação a uma portadora de acordo com os bits recebidos, é chamado **modulador**.

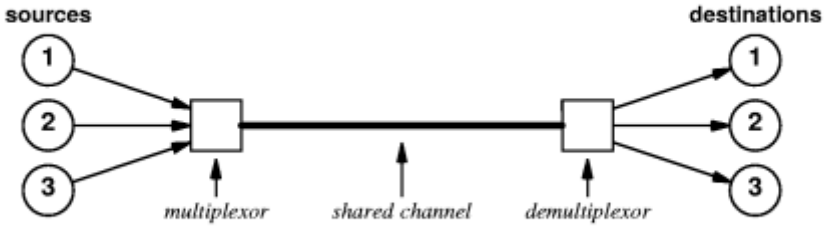
- Um aparelho que recebe uma portadora modulada e recria a sequência de bits original, é chamado **desmodulador**.

- Na prática, as redes de comunicação funcionam nos dois sentidos por isso é mais económico juntar num único aparelho as duas funções – **modem**.

Multiplexagem

- Dois ou mais sinais que usem portadoras com frequências diferentes, podem ser transmitidos em simultâneo no mesmo meio sem interferência.

- **Multiplexagem** permite que múltiplos pares de emissores/receptores, comuniquem sobre o mesmo meio em simultâneo. Por divisão de frequência, por divisão de tempo.



Transmissão de Pacotes

Comutação de Pacotes

- A maioria das redes de computador não transfere os dados como uma cadeia de bits contínuos. Como, por exemplo, a rede telefónica tradicional ou as primeiras redes de computadores.

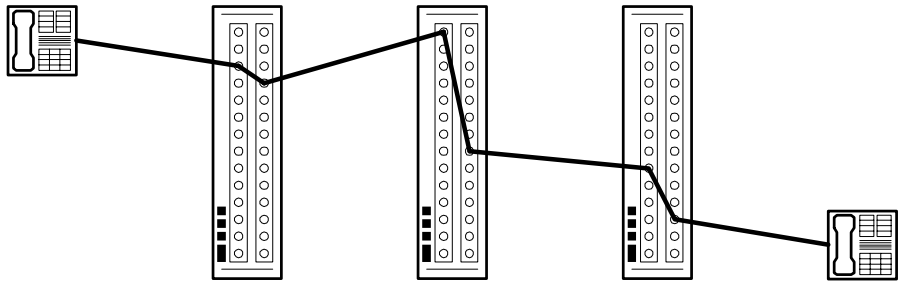
- Os dados são divididos em pequenos blocos, designados por **pacotes**, e enviados individualmente. Daí as designações de *redes de pacotes* e *redes de comutação de pacotes*.

- (1) A divisão em pequenos blocos, permite uma **melhor detecção dos blocos que chegaram sem erros**, e aqueles que não.

- (2) O recurso a pequenos blocos, permite a **partilha equitativa dos recursos disponíveis**. Os recursos não são bloqueados por longos períodos.

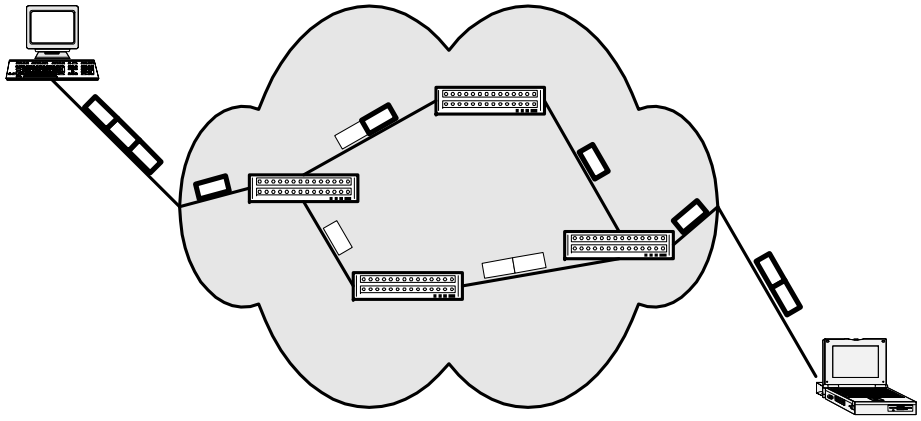
Comutação de Circuitos

- Os recursos são reservados antecipadamente para a duração da conversação.
- A **reserva estática** de recursos não é adequada para suportar comunicação de dados entre computadores.
- Rede telefónica, RDIS.



Comutação de Pacotes

- A informação é enviada em unidades de dados que **competem pelos recursos de rede**.
- Cada pacote contém um cabeçalho com informação que permite o seu encaminhamento pela rede. Os pacotes são enviados individualmente segundo uma lógica de *store and forward*.
- X.25, IP.



Erros de Transmissão

- Como o equipamento electrónico é susceptível a interferências electromagnéticas, os dados transferidos podem ser distorcidos ou perdidos.
- As interferências podem ser interpretadas pelo receptor como informação válida.

- Para a detecção dos erros de transmissão, o emissor calcula e envia informação adicional que permite a verificação dos dados por parte do receptor.
- Nenhum mecanismo é perfeito pois os próprios dados de controlo podem sofrer interferências.

Erros de Transmissão

- Bit de paridade
  - Duas formas de paridade, par ou ímpar.
  - Par: 0100101 → **1**; 0101101 → **0**.
  - Não consegue detectar erros que alterem um número par de bits.

- Checksum
  - Os dados são tratados como uma sequência de inteiros e é calculada a soma.
  - Não detecta todos os erros.

- Cyclic Redundancy Check (CRC)
  - Detecta mais erros do que os dois métodos anteriores.
  - Cálculos complexos mas simples de implementar em *hardware*.

Ligações Directas

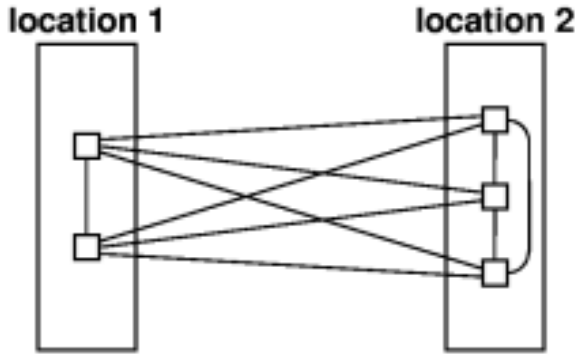
- Os primeiros sistemas de computadores utilizavam ligações directas (ponto-a-ponto).
- Cada canal ligava exactamente dois computadores.

- (1) O hardware e as especificações a utilizar podem ser as mais adequadas para a comunicação particular.
- (2) Para alterar os detalhes da implementação basta o acordo dos dois intervenientes.
- (3) É mais fácil implementar mecanismos de segurança e privacidade.

- Os problemas surgem quando se procura ligar mais do que dois computadores.

Ligações Directas

- Numa rede com ligações ponto-a-ponto, o número total de ligações necessárias pode exceder o número total de computadores a ligar.



$$\frac{N^2 - N}{2}$$

Partilha do Meio Físico

- Houve uma alteração radical nos anos 60 e 70 com o desenvolvimento das redes locais – *Local Area Networks* (LAN).
- O conceito base reside na **partilha da rede de comunicação**.
- Como há uma eliminação da duplicação, a partilha resulta na **redução de custos**.

- A necessidade de coordenação impede que estas tecnologias sejam utilizadas em redes de longa distância. Devido aos atrasos, o tempo gasto na coordenação seria superior aquele gasto na comunicação real.

- As tecnologias de redes locais (LAN) **são a forma mais popular de rede de computadores**. As LAN ligam mais computadores do que qualquer outro tipo de rede.

Topologias de Rede

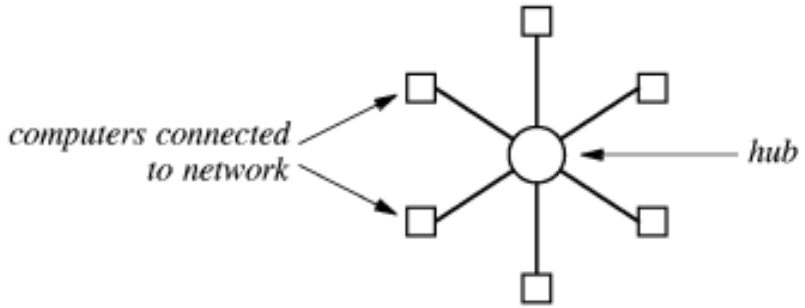
- As redes locais são agrupadas em categorias de acordo com a **forma genérica, ou topologia**.
- Representam **conceitos lógicos**, a implementação real (física) pode variar.

- As principais topologias utilizadas são:
  - Estrela
  - Anel
  - Barramento

- Cada topologia apresenta vantagens e desvantagens.
- Futuro: redes sem fios.

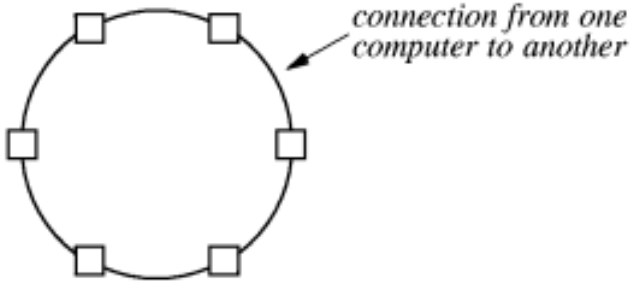
Topologia em Estrela

- Cada computador é ligado a um **ponto central**.
- O elemento central pode ser um repetidor multiporta (*hub*) ou um comutador.
- A falha parcial de uma ligação não tem impacto sobre a rede.
- Exemplo: Redes ATM.



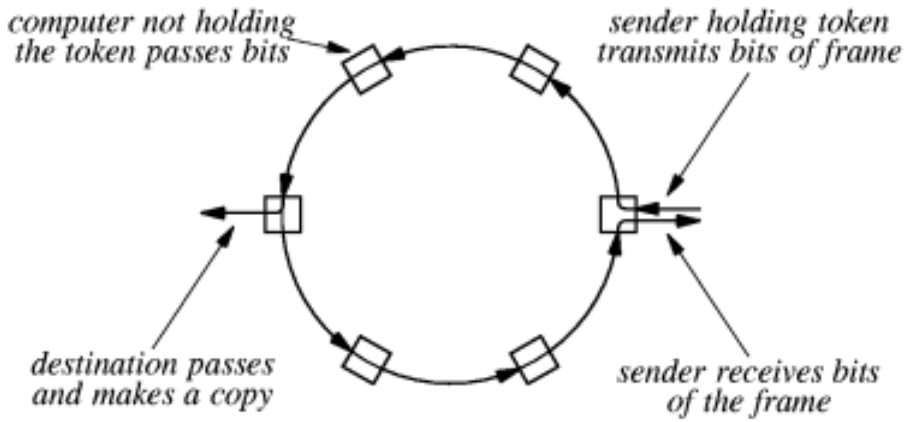
Topologia em Anel

- Os computadores são ligados num **circuito fechado**. Existência de repetidores em cada ponto.
- Coordenação de acessos é simplificada.
- Baixa tolerância a falhas nas ligações.



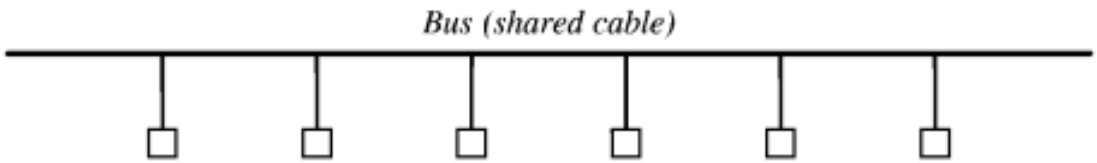
Topologia em Anel

- Mecanismo de acesso mais utilizado – passagem do testemunho (*token*).
- Redes **token ring**. Utilização de **um testemunho** para controlar a utilização da rede.



Topologia em Barramento

- Ligação através de um **único cabo**, ao qual os computadores são ligados.
- Requer menos cabo na instalação.
- Baixa tolerância a falhas nas ligações.



Ethernet

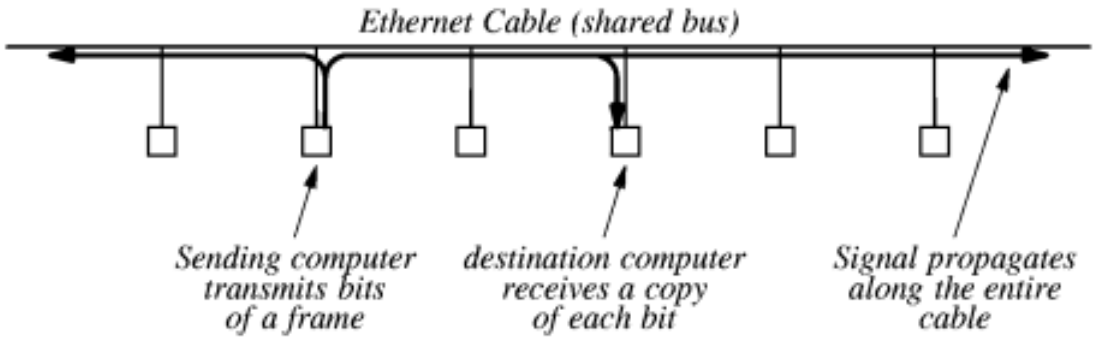
- Inventada nos anos 70 na Xerox Parc.
- Actualmente a norma é controlada pelo IEEE.
- Utiliza uma topologia em barramento.

- Implementação original → 10 Mbps
- Fast Ethernet → 100 Mbps
- Gigabit Ethernet → 1000 Mbps / 1 Gbps

- Tecnologia de rede local mais utilizada.

Ethernet

- Enquanto um computador utiliza o meio, todos os outros esperam.
- São necessários mecanismos para controlar a transmissão. Ex: CSMA/CD.

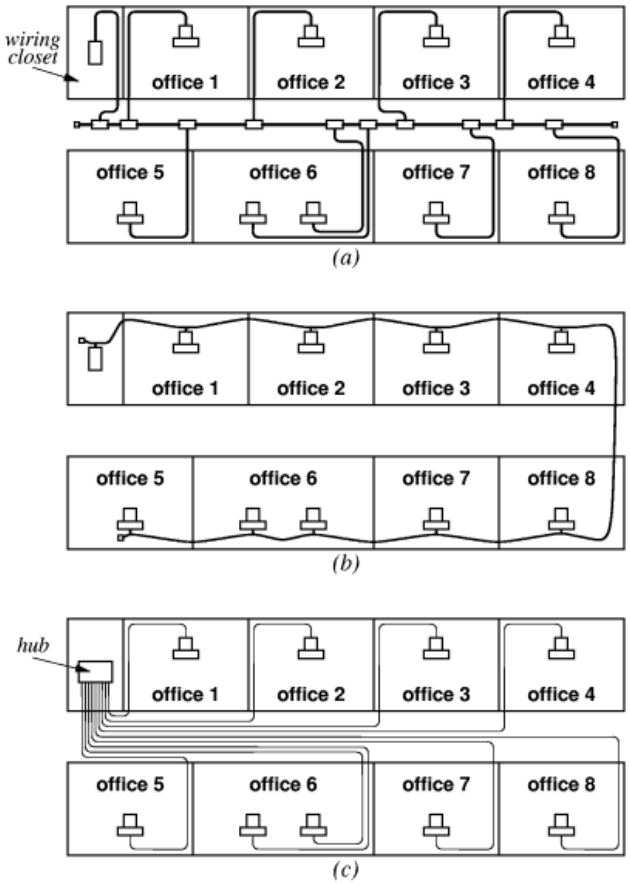


Topologia Física

- A diferença de velocidade entre o CPU e a rede de comunicação é um problema importante.
  - (1) Não faz sentido limitar a rede à velocidade do CPU mais lento.
  - (2) Não faz sentido impor uma velocidade fixa para todos os computadores numa rede.
- A existência de um equipamento específico – **placa/carta de rede**, permite que o computador lide com redes mais rápidas do que o CPU seria capaz de suportar.
- Acomoda a diferença de velocidades entre a rede e o computador.

Topologia Física

- A tecnologia Ethernet utiliza uma topologia em barramento.
- A implementação física pode seguir diferentes opções de ligação.
- A tecnologia determina a topologia lógica.
- O esquema de ligações determina a topologia física.



Extensão de Redes Locais

- Um aspecto fundamental das LAN é a limitação em termos de distância.

- Existem tecnologias que permitem estender estas distâncias

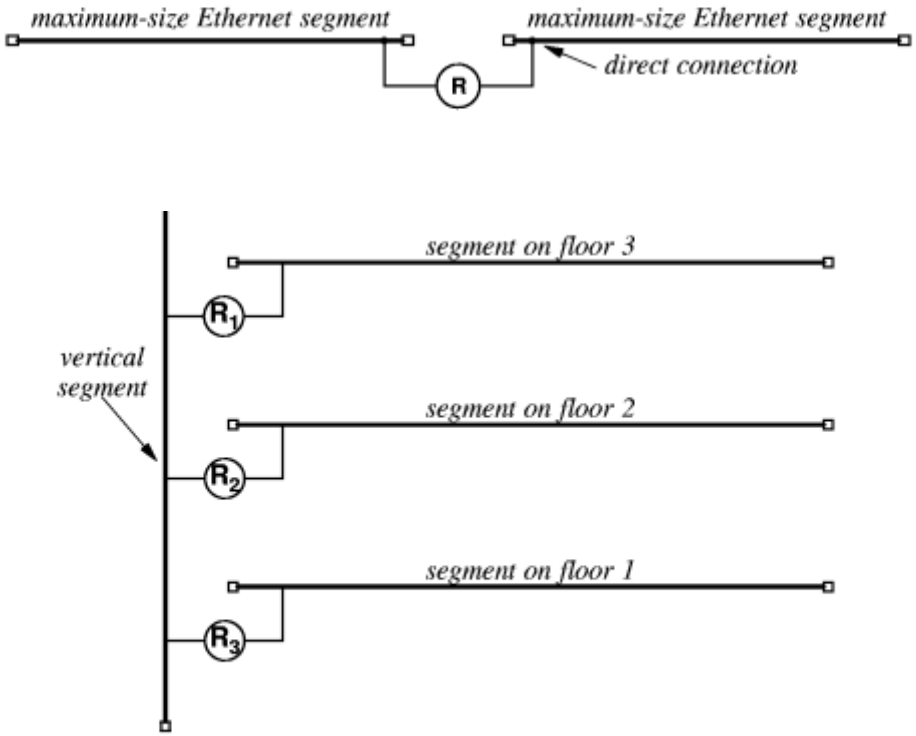
  – **Fibra Óptica**: permite estabelecer uma ligação entre um computador e uma LAN remota.

  – **Repetidores**: liga dois segmentos de rede independentes. Reenvia o sinal amplificado sem qualquer filtragem.

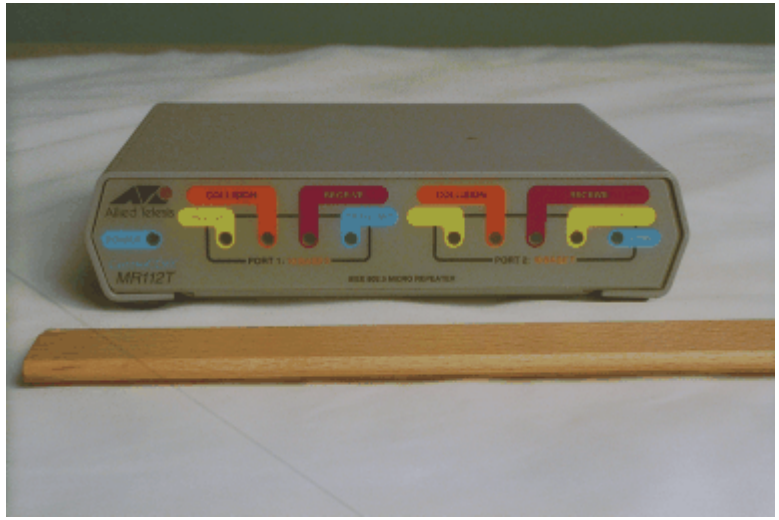
  – ***Bridges***: reenvia pacotes válidos de um segmento para outro. Não reenvia interferências ou outros problemas.

Repetidores

- Amplifica e envia todos os sinais eléctricos que ocorrem num segmento para o outro segmento.
- Se uma colisão ocorre num segmento, os repetidores provocam o mesmo problema no(s) outro(s).



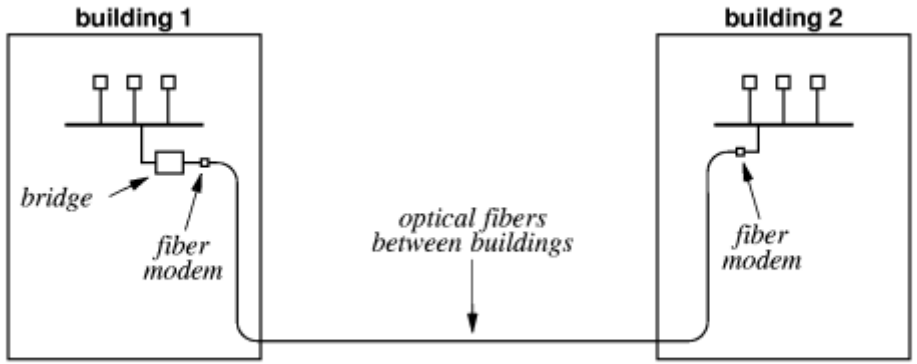
Repetidores



Frente e verso de um repetidor Ethernet. Na frente são visíveis os vários indicadores de estado. No verso é possível identificar uma ligação RJ-45 e uma ligação coaxial Ethernet.

Bridges

- As *bridges* examinam os endereços físicos dos pacotes e decidem se reenviar ou não para outros segmentos.
- A utilização de *bridges* pode melhorar o desempenho da rede.



Tipos de Redes

- As tecnologias de rede podem ser classificadas segundo três categorias genéricas, de acordo com o tamanho da rede que pode ser criada.

  – *Local Area Networks* (**LAN**) – podem abranger um edifício único ou *campus*.

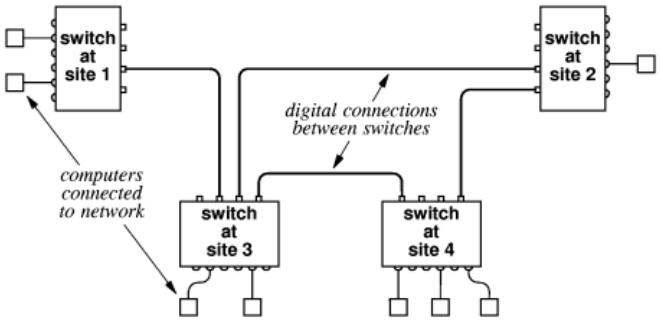
  – *Metropolitan Area Networks* (**MAN**) – podem abranger uma cidade. Poucas tecnologias se inserem nesta categoria.

  – *Wide Area Networs* (**WAN**) – podem abranger múltiplas cidades, países ou continentes.

Wide Area Networks

- As tecnologias de rede WAN podem ser utilizadas para formar redes que abrangem uma **área arbitrariamente longa** e um **número arbitrário de computadores**.

- O equipamento base de uma WAN é o *packet switch*. Um conjunto de *packet switches* são interligados para formar uma WAN.



Switches

Ethernet switch Cisco Catalyst 3000. Este equipamento tem 16 ligações Ethernet de 10Mbps. Junto ao topo é possível identificar 2 ligações de 100Mbps.

Store and Forward

- Os *packet switches* funcionam numa lógica de *store and forward* – os pacotes são colocados em memória até ser possível reenviá-lo para o destino.

- Permite lidar com tráfego abrupto; Criar filas de espera para determinados recursos; Reduzir a necessidade de coordenação.

- É um **paradigma fundamental nas redes WAN**, uma vez que é possível que múltiplos computadores comuniquem em simultâneo.

Medidas de Desempenho

- **Atraso** (*delay*) – tempo que um bit demora a atravessar a rede de um computador para outro, normalmente em milisegundos.

- **Débito** (*throughput*) – medida da taxa a que os dados podem ser enviados através da rede, normalmente em *bits per second* (bps).

- O **atraso**, medido em segundos, representa o tempo que um *bit* individual permanece em transito.
- O **débito**, medido em *bits* por segundo, representa o número de bits que podem entrar na rede por unidade de tempo. O débito representa a capacidade da rede.

Medidas de Desempenho

- Na prática, o atraso e o débito não são completamente independentes.
- O aumento do tráfego numa rede provoca um aumento no atraso verificado. Uma rede que funcione próxima dos 100% da capacidade de débito total, apresenta um atraso elevado.
- O produto **atraso x débito** representa o volume de dados máximo que pode estar presente na rede.
- **Jitter** – representa a variância do atraso. Dado importante na transmissão de dados em tempo-real.

Protocolos

- Um acordo que especifica o *formato* e o *significado* das mensagens a trocar numa rede é conhecido como um **protocolo de comunicação**.

- Aplicações informáticas que utilizam a rede não interagem directamente com o *hardware*. Recorrem a programas que implementam complexos protocolos de comunicação.

- Não basta a existência de *hardware* para a implementação de redes de comunicação, são *necessários programas* que implementam os protocolos de comunicação.

Protocolos e Camadas

- Em vez de definir um protocolo único que lide com todos os detalhes de todas as formas de comunicação possíveis, os problemas foram decompostos e organizados em módulos independentes.

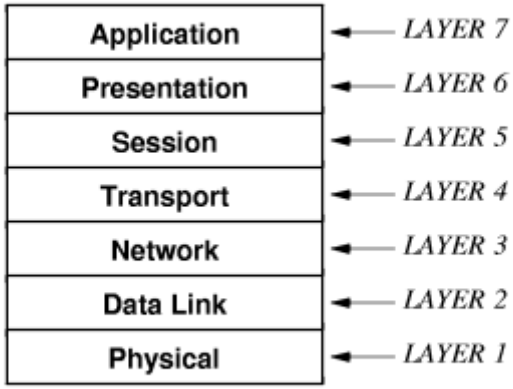
- Em vez de desenvolver estes vários módulos (protocolos) isoladamente, o desenvolvimento é integrado originando **famílias de protocolos**.

- A **estruturação em camadas** é uma forma de dividir o problema em partes. Permite dominar a complexidade.

Camadas

- Uma família de protocolos pode ser desenhada de forma a que **cada protocolo corresponda a uma camada**.

- A *International Organization for Standardization* (ISO) definiu, nos anos 80, um modelo de referência com 7 camadas.



Modelo de Referência OSI

- O *Open Systems Interconnection Reference Model* (OSI) permitiu estabelecer uma referência para o desenvolvimento de equipamentos por parte dos diversos fabricantes.

- O modelo OSI é uma construção genérica e abstracta. Não implementa nenhum protocolo concreto.

- Este modelo estabelece conceitos base importante e, apesar de antigo, ainda é utilizado para descrever protocolos recentes.

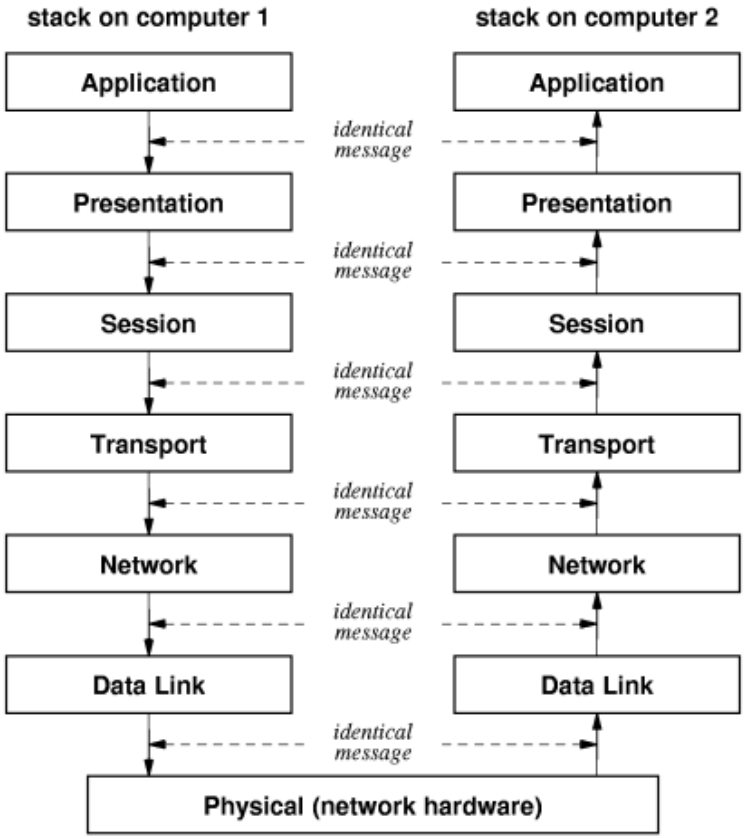
Modelo de Referência OSI

- A comunicação entre uma aplicação A e uma aplicação B pode ser descrita seguinte sequência:
  - Para comunicar com a aplicação B, a aplicação A usa os serviços da camada 7, ...
  - ... as entidades da camada 7 de A comunicam com as entidades da camada 7 de B usando um protocolo da camada 7, ...
  - ... o protocolo da camada 7 usa os serviços da camada 6, ...
  - ...
  - ... até, na camada 1, haver uma troca de dados ao nível do suporte físico (*hardware*).

Modelo de Referência OSI

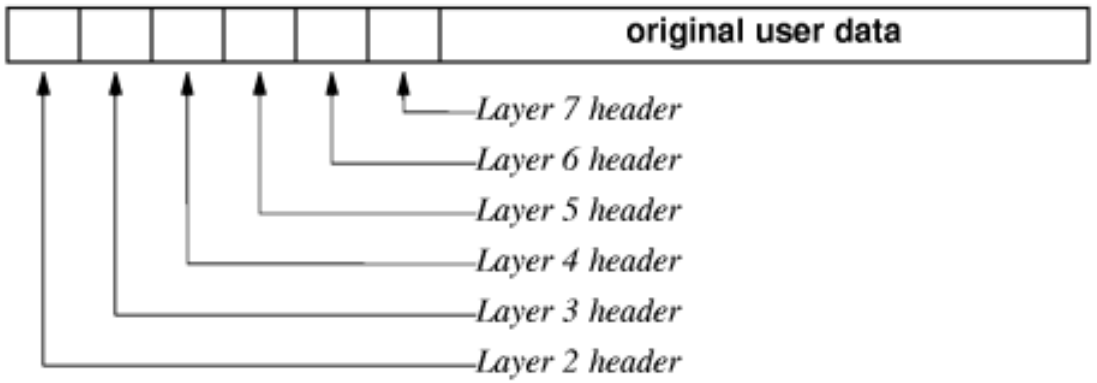
Os programas na camada N no destino, devem receber uma **mensagem idêntica** à enviada pelos programas na camada N na origem.

A camada N no destino aplica as **transformações inversas** às aplicadas na camada N na origem.

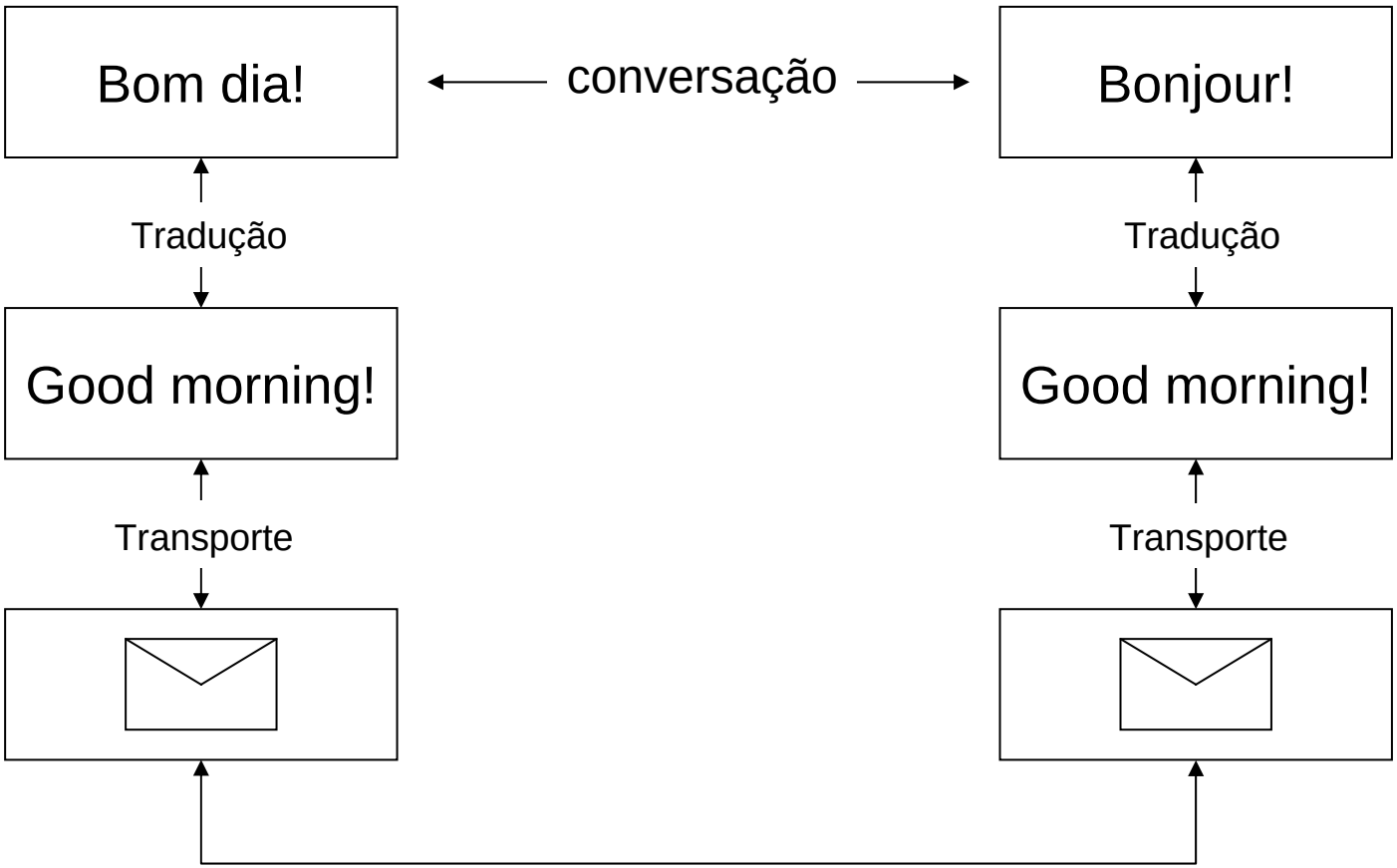


Modelo de Referência OSI

- Normalmente, cada camada adiciona informação, sob a forma de um cabeçalho, antes de enviar os dados para a camada inferior.



Analogia


Bom dia!
conversação
Bonjour!
Tradução
Tradução
Good morning!
Good morning!
Transporte
Transporte

Camadas OSI (1-4)

- **Física** – equipamento básico de rede. Características mecânicas, eléctricas e funcionais da interface física entre sistemas.
- **Ligação de Dados** – organização dos dados em pacotes e transmissão dos pacotes pela rede.
- **Rede** – atribuição de endereços e encaminhamento de pacotes através da rede.
- **Transporte** – transferência fiável de dados.

Camadas OSI (5-7)

- **Sessão** – estabelecimento de sessões de comunicação entre duas partes. Especificações para segurança e autenticação.

- **Apresentação** – representação dos dados. Estes protocolos são necessários porque diferentes fabricantes de computadores utilizam representações internas diferentes.

- **Aplicação** – especifica como uma aplicação em particular utiliza a rede. Por exemplo a especificação do FTP, SMTP.

Interligação de Redes

Interligação de Redes

- O conceito de **interligação de redes (internetworking)** é fundamental na comunicação entre computadores.

- Redes de **diferentes organizações** e implementadas usando **tecnologias distintas** devem poder comunicar.

- As tecnologias de interligação permitem, a partir da ligação de múltiplas redes físicas, criar um **sistema de comunicação homogéneo**.

Interligação de Redes

- Cada tecnologia é desenhada para resolver um conjunto específico de restrições.
  - Por exemplo, tecnologias LAN para distâncias curtas e tecnologias WAN para grandes distâncias.

- **Nenhuma tecnologia em particular é ideal para todas as situações.**

- Nos anos 70, tornou-se evidente que cada rede implementada se estava a tornar uma **ilha**. Os computadores apenas podiam comunicar com outros dispositivos **ligados à mesma rede**.

Interligação de Redes

- Obrigar o utilizador a recorrer a diferentes terminais para aceder a diferentes serviços resulta num **decréscimo da produtividade individual**.

- Um sistema de comunicação que oferece **serviço universal** permite que qualquer par arbitrário de computadores comunique.

- Incompatibilidades ao nível do suporte físico impedem que redes implementadas em diferentes tecnologias sejam ligadas por *bridges*,

Interligação de Redes

- Para ultrapassar as incompatibilidades foram desenvolvidas tecnologias que permitem fornecer um **serviço universal através de redes heterogéneas**.

- Esta solução tem a designação de **internetworking** e recorre ao **suporte físico** e ao **suporte lógico**.

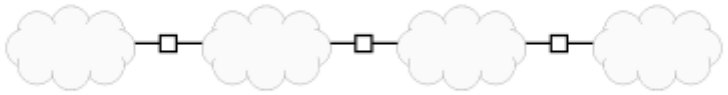
- O sistema resultante da ligação de redes físicas é conhecido como **internetwork** ou **internet**.

- Existem internets com poucas redes e internets compostas por centenas de redes físicas.

Routers

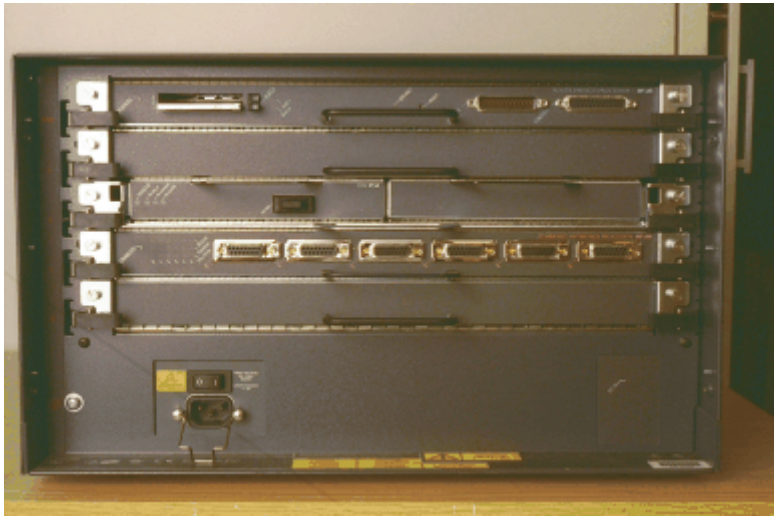
- O equipamento básico usado para interligar redes heterogéneas é o **router**.

- **Um router é um equipamento especialmente desenhado para interligar redes.** Um router pode interligar redes que usem diferentes tecnologias.



Uma internet formada por **quatro redes físicas** interligadas usando **três routers**. Cada uma das redes pode ser uma LAN ou WAN.

Routers



Um router Cisco 7500. O topo é ocupado pela placa de processamento (memória, processador). Inclui interfaces de fibra óptica para redes ATM e conectores AUI para redes Ethernet.

Um router Cisco 12000 GSR (gigabit speed router). Capacidade até 160 Gbps. Inclui interfaces para gigabit Ethernet.

Internets

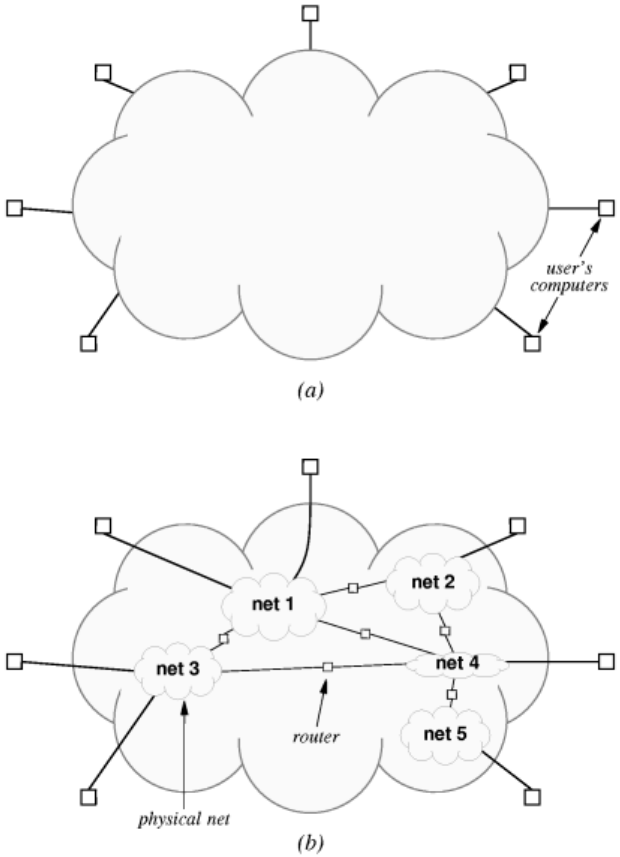
- **Uma internet consiste num conjunto de redes interligadas por routers.**

- Para atingir o **serviço universal** são necessários protocolos.

- Programas informáticos, que **implementem os protocolos**, são necessários nos computadores e nos routers para tornar o serviço universal possível.

- Uma internet é designada por **rede virtual** porque representa uma abstracção. Os detalhes físicos são escondidos pelo protocolo.

Internets



(a) A ilusão de uma rede única. Um rede virtual

(b) A rede física existente. Cada computador está ligado a uma rede física independente. Routers ligam as diversas redes.

Protocolos TCP/IP

- Os protocolos mais importantes desenvolvidos para a interligação de redes são conhecidos como **Protocolos Internet TCP/IP**, ou abreviadamente TCP/IP.

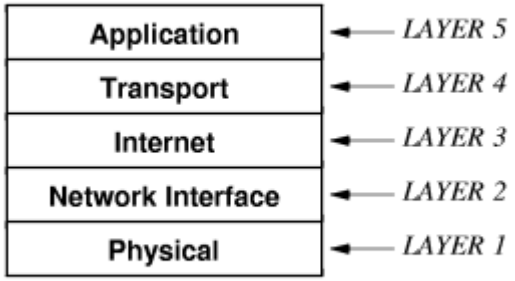
- O desenvolvimento destes protocolos foi iniciado nos anos 70 apoiado pela ARPA. Os militares dos EUA foram das primeiras organizações a ter múltiplas redes físicas.

- A tecnologia TCP/IP tornou possível uma **Internet** global.

Protocolos TCP/IP

- Os investigadores que desenvolveram o TCP/IP inventaram um modelo de camadas novo.

- Este modelo é designado por **Modelo de Camadas TCP/IP** ou **Modelo de Referência Internet** e contém 5 camadas.



Camadas TCP/IP

- Os protocolos TCP/IP estão organizados em **cinco camadas conceptuais**. Algumas camadas deste modelo correspondem a várias camadas do modelo OSI.

- **Camada 1 - Física**
  - Suporte físico de rede.

- **Camada 2 - Rede**
  - Como organizar dados em pacotes e como transmitir pacotes através de uma rede.

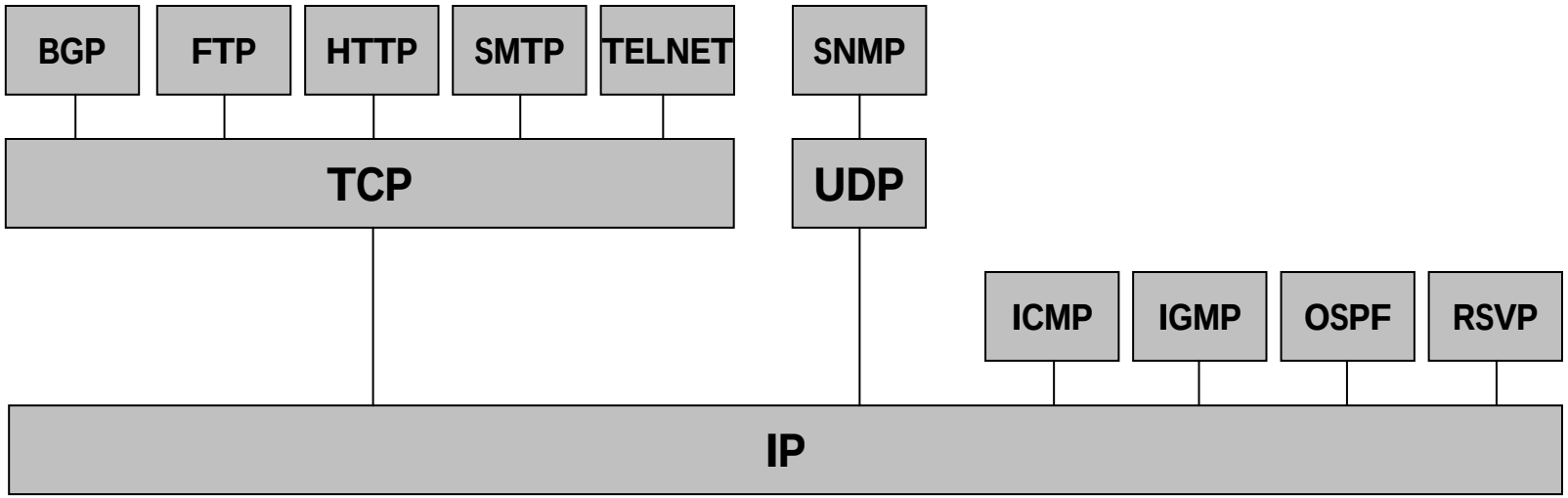
- **Camada 3 - Internet**
  - Especifica o formato dos pacotes enviados através da internet, bem como os mecanismos usados para o encaminhamento.

Camadas TCP/IP

- **Camada 4 - Transporte**
  - Especifica como obter transferência fiável.

- **Camada 5 - Aplicação**
  - Cada protocolo desta camada especifica como uma aplicação utiliza a internet. Corresponde às camadas 6 e 7 do modelo ISO.

Protocolos TCP/IP



BGP = Border Gateway Protocol
FTP = File Transfer Protocol
HTTP = HyperText Transfer Protocol
ICMP = Internet Control Message Protocol
IGMP = Internet Group Management Protocol
IP = Internet Protocol
OSPF = Open Shortest Path First
RSVP = Resource ReSerVation Protocol
SMTP = Simple Mail Transfer Protocol
SNMP = Simple Network Management Protocol
TCP = Transmission Control Protocol
UDP = User Datagram Protocol

Protocolo Internet

- O principal objectivo de um protocolo internet é **oferecer uma rede virtual**, escondendo os detalhes das redes físicas.
- Uma **rede virtual é uma abstracção** criada exclusivamente por aplicações informáticas.
- Um aspecto crítico de qualquer rede de comunicação é o endereçamento. Numa rede virtual os computadores devem usar um **esquema de endereçamento uniforme**.
- O protocolo define um endereçamento **independente da identificação física** de cada computador.

Endereçamento IP

- Na família de protocolos TCP/IP, o endereçamento é especificado pelo **Internet Protocol (IP)**, na camada 3.

- A norma IP especifica que a cada máquina é atribuído um número único de 32 bits, designado por **endereço IP**.

- Cada pacote que circula na rede contém o endereço IP do **emissor** (origem) e do **receptor** (destino).

- Um endereço IP é dividido em duas partes, prefixo e sufixo. O **prefixo identifica a rede física**. O **sufixo identifica o computador** nessa rede.

Endereçamento IP

- Numa rede internet, a cada rede física é atribuído um identificador – **identificador de rede**.

- Este esquema de endereçamento hierárquico tem **dois aspectos importantes**:

  – Cada computador tem um endereço único.
  – Apesar de ser necessário coordenar globalmente a atribuição dos prefixos, a atribuição dos sufixos pode ser coordenada localmente.

Endereçamento IP

- Para facilitar a manipulação por parte de humanos, os endereços IP são representados segundo uma **notação decimal separada por pontos** (*dotted decimal notation*).

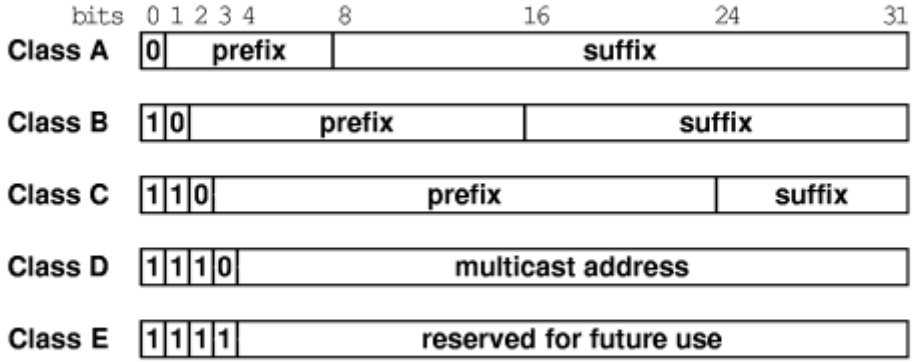
- Cada conjunto de 8 bits (octeto) é representado em decimal e pontos são usados para separar os 4 octetos.

- O valor máximo de cada octeto é 255. Assim, a gama de endereços IP está compreendida entre **0.0.0.0** e **255.255.255.255**.

Classes de Endereços IP

- Para determinar o espaço reservado para o prefixo e para o sufixo, dentro dos 32 bits disponíveis, foram definidas **três classes de endereços**.
  - Um **prefixo maior** permite um maior número de redes, mas menos computadores em cada rede.
  - Um **prefixo menor** permite menos redes, mas mais computadores.
- Os primeiros 4 bits de um endereço determinam a classe a que pertence.

Classes de Endereços IP



- Originalmente foram definidas **5 classes**.
  - As classes primárias (A, B e C) são utilizadas para os computadores (*hosts*).
  - A classe D é utilizada para identificar um conjunto de computadores (multicasting).

Classes de Endereços IP

Class	Range of Values
A	0 through 127
B	128 through 191
C	192 through 223
D	224 through 239
E	240 through 255

A gama de valores decimais encontradas no primeiro valor de cada classe. Exemplo: 130.23.33.1 é um endereço da classe B; 210.39.2.1 da classe C.

Address Class	Bits In Prefix	Maximum Number of Networks	Bits In Suffix	Maximum Number Of Hosts Per Network
A	7	128	24	16777216
B	14	16384	16	65536
C	21	2097152	8	256

Número de redes físicas e computadores por rede em cada uma das três classes.

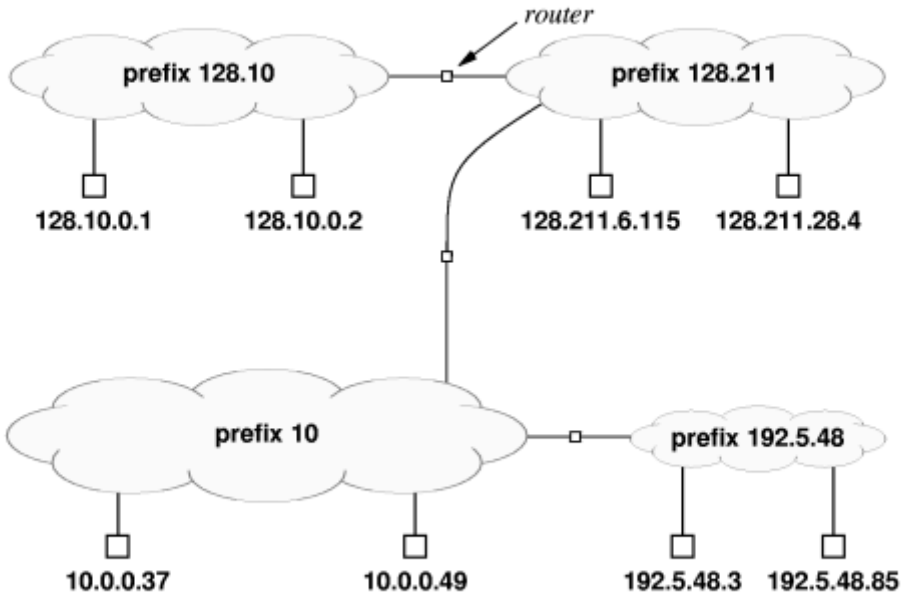
Classes de Endereços IP

- A atribuição local de endereços é coordenada ao nível dos *Internet Service Providers* (**ISP**).

- A coordenação global é feita por uma entidade central, a *Internet Assigned Number Authority* (**IANA**). Desta forma é possível garantir que cada prefixo é único em toda a Internet.

- No contexto de uma rede concreta, o **administrador de rede** gere a atribuição dos sufixos. Esta atribuição é feita de forma arbitrária.

Classes de Endereços IP



Duas redes de classe B (prefixos 128.10 e 128.211), uma rede de classe A (prefixo 10) e uma rede de classe C (prefixo 192.5.48).

Subredes IP

- A categorização utilizando apenas 3 classes resulta num **esquema demasiado inflexível**, tornando-se numa limitação.

- Por mais pequena que seja, uma rede necessita sempre de reservar um **mínimo de 256 endereços** (classe C). Muitos endereços nunca são utilizados.

- Para resolver este problema, foi desenvolvido o **mecanismo de subredes**. Com este mecanismo, em vez de existirem apenas três classes, a **divisão entre o prefixo e o sufixo pode ocorrer em qualquer ponto**.

Subredes e Máscaras IP

- As subredes são **implementadas armazenando informação adicional** com cada endereço.

- A informação adicional especifica a fronteira exacta entre o prefixo e o sufixo e tem a designação de **máscara de** (sub)**rede** (*address mask* ou *subnet mask*).

- Por ser computacionalmente mais eficiente, a máscara de rede tem, como o endereço IP, 32 bits. Para cada bit pertencente ao prefixo, a máscara tem o valor 1.

Máscaras IP

	Representação Binária	Representação Decimal
Endereço IP	11000000.11100100.00010001.00111001	192.228.17.57
Máscara de rede	11111111.11111111.11111111.11100000	255.255.255.224
Endereço AND Máscara	11000000.11100100.00010001.00100000	192.228.17.32
Endereço da (sub)rede	11000000.11100100.00010001.001xxxxx	1
Endereço da máquina	xxxxxxxx.xxxxxxxx.xxxxxxxx.xxx11001	25

	Representação Binária	Representação Decimal
Máscara para a classe A	11111111.00000000.00000000.00000000	255.0.0.0
Máscara para a classe B	11111111.11111111.00000000.00000000	255.255.0.0
Máscara para a classe C	11111111.11111111.11111111.00000000	255.255.255.0

Endereços Reservados

- O protocolo IP reserva um conjunto de endereços para **usos específicos**. Estes endereços não devem ser atribuídos a nenhum computador da rede.

- O **sufixo 0** é reservado para representar o **endereço da rede**. Por exemplo, o endereço 128.211.0.0/16 representa a rede a que foi atribuída o prefixo 128.211.

- O **sufixo 1** é reservado para representar o **endereço de broadcast**. Este endereço permite enviar um pacote a todos os computadores de uma rede. Para o exemplo anterior, o endereço de broadcast seria 128.211.255.255.

Endereços Reservados

- O endereço **255.255.255.255** é reservado para representar o **endereço de broadcast limitado a uma rede física**.

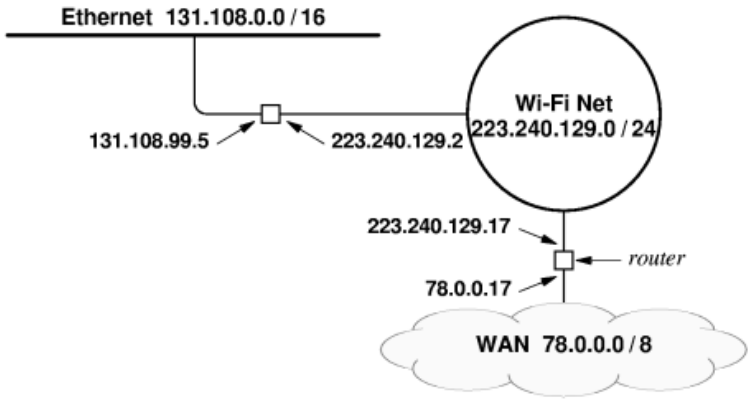
- Durante o arranque (apenas), o endereço **0.0.0.0** é usado para representar **este computador**.

- Para a realização de testes, o protocolo define **endereços de loopback**. Pacotes enviados para estes endereços nunca chegam a sair do computador. O **prefixo 127** está reservado com este objectivo. Exemplos: 127.0.0.1, 127.32.22.4.

Routers e Endereços IP

- Cada endereço IP não identifica um computador, mas sim a ligação entre um computador e uma rede.

- Um computador ligado a várias redes (um router) terá um **endereço IP por cada ligação**.



Resolução de Endereços

- Os **endereços IP são virtuais**, uma abstracção mantida por programas informáticos. Assim, é necessário um **mapeamento entre o endereço IP e o endereço físico** do equipamento.

- Existem vários mecanismos para a **resolução de endereços**:
  - **Pesquisa em tabelas**. Os mapeamentos são mantidos em tabelas.
  - **Calculado**. Usando operações aritméticas, o endereço físico é calculado a partir do endereço IP.
  - **Troca de mensagens**. Combinadas com os métodos anteriores.

- A família TCP/IP inclui o Address Resolution Protocol (**ARP**) usado para apoiar a resolução de endereços. Complementado com o protocolo **RARP**.

Datagramas IP

- O serviço base oferecido pelo protocolo IP **não oferece ligação permanente** entre as partes (*connectionless*).

- Num serviço com estas características, cada pacote é **enviado de forma independente**.

- De forma simplificada, o emissor cria um pacote que inclui o endereço IP do destino e envia-o para o router mais próximo. Os routers, de acordo com informação interna, reenviam o pacote ao longo da rede. Quando o pacote chega ao último router é entregue ao receptor.

Datagramas IP

- Diferentes tecnologias usam **diferentes formatos** para a representação dos pacotes.

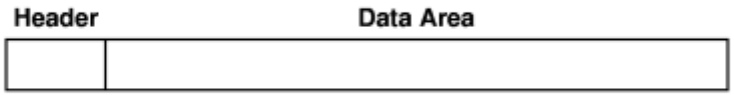
- Para ultrapassar a heterogeneidade, os protocolos internet definem um **formato universal para os pacotes**, independente do suporte físico.

- Os protocolos TCP/IP usam o nome **datagrama IP** para designar um pacote internet.

Datagramas IP

- Um datagrama IP pode transportar um **número arbitrário de dados**. Não existe um limite fixo.

- O cabeçalho inclui os **endereços IP** da origem e do destino.

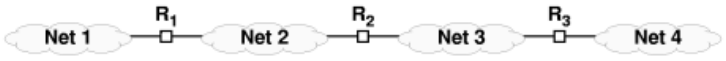


Estrutura genérica de um datagrama IP com o cabeçalho seguido dos dados a enviar. O cabeçalho inclui informação sobre o destino.

Envio de Datagramas

- Ao longo do caminho, cada router examina o datagrama e, de acordo com o endereço do destino, envia-o para uma das redes a que está ligado.

- Para saber que rede escolher para cada endereço de destino, cada router mantém uma **tabela de encaminhamento**.



(a)

Destination	Next Hop
net 1	R_1
net 2	deliver direct
net 3	deliver direct
net 4	R_3

(b)

(a) Um exemplo onde três routers ligam quatro redes físicas.

(b) A tabela de encaminhamento conceptual presente no router R2.

Tabelas de Encaminhamento

- A **informação nas tabelas de encaminhamento** pode ser mantida de forma estática ou dinâmica.
- A designação **encaminhamento estático** é usada quando a informação nas tabelas não muda após o carregamento.
- A designação **encaminhamento dinâmico** é usada quando a informação é alterada automaticamente ao longo do tempo.
- No encaminhamento dinâmico, os routers actualizam a informação com base em informação obtida a partir de outros routers. O principal objectivo é **conhecer as rotas óptimas** para cada destino.

Envio de Datagramas

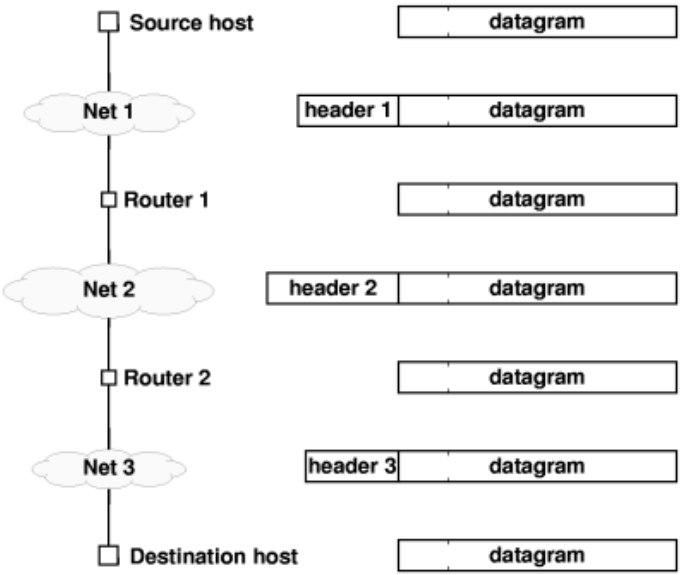
- Como o protocolo IP foi desenhado para funcionar sobre qualquer tipo de rede física, o **suporte físico pode falhar**.

- Como resultado, os datagramas IP podem:
  - Ser **duplicados**.
  - Sofrer **atrasos** significativos.
  - Ser **corrompidos**.
  - Ser **perdidos**.

- O **protocolo IP não garante a resolução** de nenhum destes problemas. Programas em camadas superiores devem existir para ultrapassar cada um destes cenários.

Envio de Datagramas

- Para atravessar uma rede física, o datagrama IP é **encapsulado** num pacote do suporte físico.



Um datagrama IP durante uma viagem numa internet. Sempre que atravessa uma rede física, o datagrama é encapsulado num pacote específico à tecnologia da rede.

IPv6

- A **versão 4** do protocolo IP (IPv4) limita os endereços possíveis a um **espaço de 32 bits**.

- Devido ao crescimento exponencial da Internet, prevê-se que dentro de **20 anos este espaço esteja esgotado**.

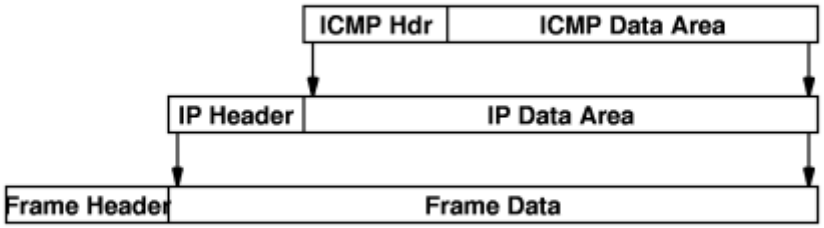
- A versão 6 do protocolo IP (**IPv6**), desenhada pelo IETF, utiliza **128 bits para representar os endereços**.

- A representação dos endereços usa uma notação hexadecimal
  - `69DC:8864:FFFF:FFFF:0:1280:8C0A:FFFF`
  - `FF0C::B1` (comprimida)

ICMP

- Para a detecção de alguns tipos de erros, os protocolos TCP/IP incluem um protocolo com este objectivo.

- O **Internet Control Message Protocol** (ICMP) define um conjunto de mensagens para controlo dos erros de transmissão.



Ocorrem dois níveis de encapsulamento para uma mensagem ICMP. Primeiro dentro de um datagrama, depois dentro de um pacote da rede física.

UDP

- O protocolo IP **não distingue múltiplas aplicações** num mesmo computador. Não é um protocolo de transporte.

- O **User Datagram Protocol** (UDP) oferece um serviço **ponto-a-ponto** ou de **transporte**.

- É um **protocolo da camada 4**, fornece um serviço de transporte de mensagens entre aplicações em diferentes computadores.

TCP

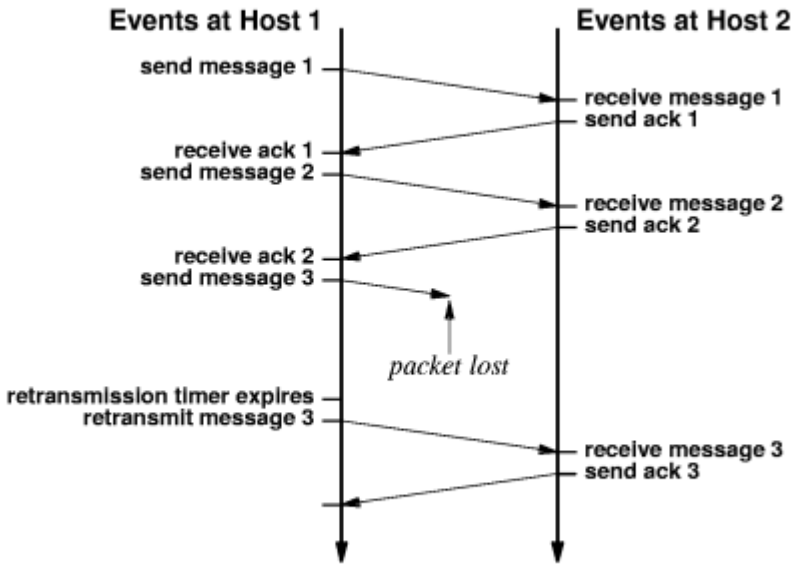
- O **Transmission Control Protocol** (TCP) é o principal protocolo na família TCP/IP.

- É um protocolo de transporte (camada 4) que **oferece entrega fiável**. Uma característica fundamental em muitas aplicações.

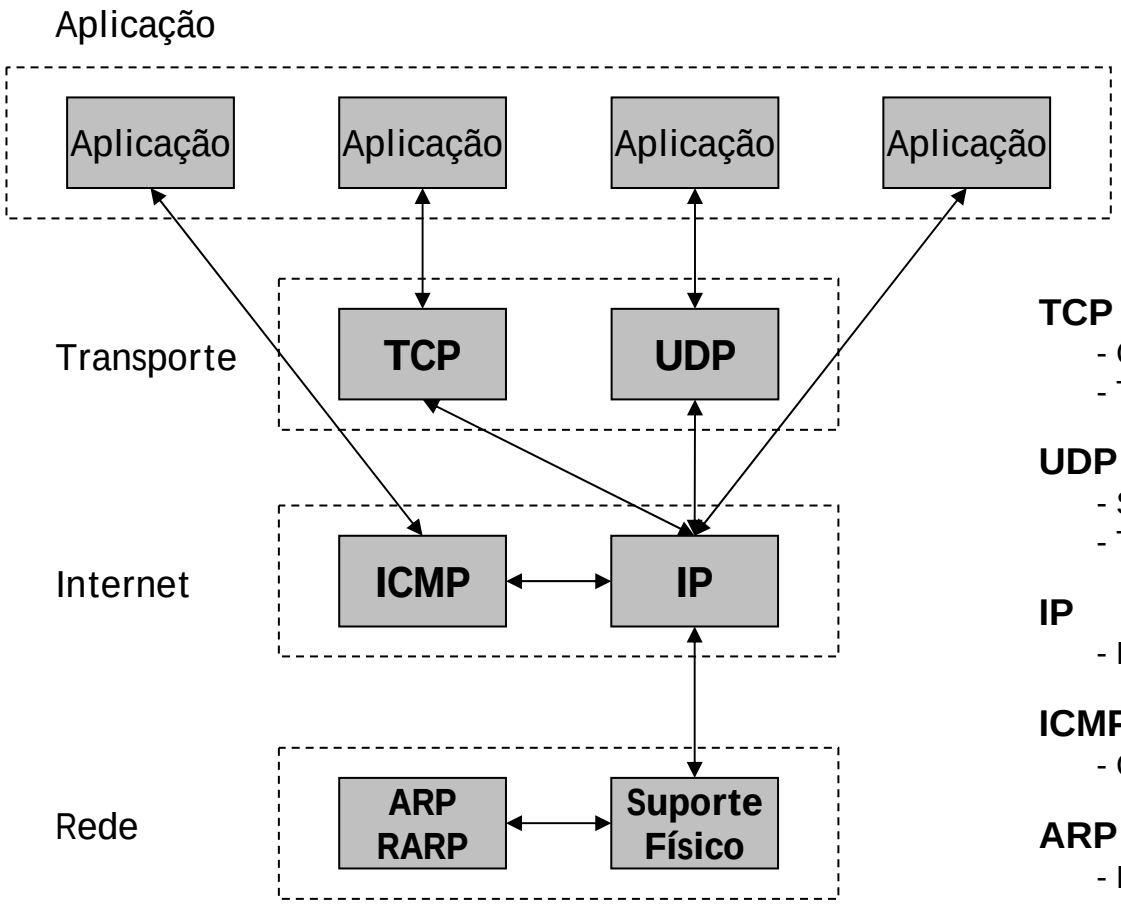
- Entre outros serviços, o TCP oferece: *ligação permanente*, *comunicação ponto-a-ponto*, *fiabilidade total* (sem duplicação nem perda) e *bidireccionalidade*.

TCP

- Para oferecer **fiabilidade** o protocolo usa um conjunto de tecnologias. Uma das mais relevantes é a **retransmissão** dos dados.



ARP, IP, ICMP, UDP e TCP



TCP
- Com manutenção de ligação.
- Transporte fiável entre aplicações.

UDP
- Sem ligação permanente.
- Transporte não fiável.

IP
- Encaminhamento de datagramas.

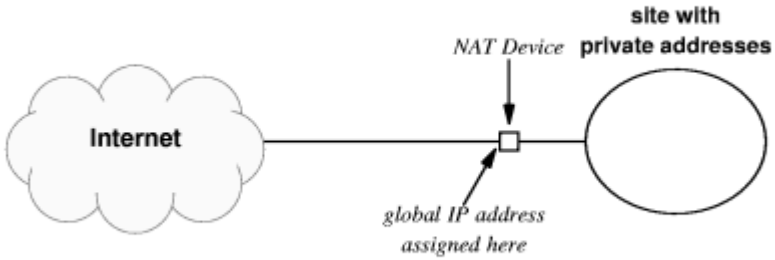
ICMP
- Controlo de erros.

ARP / RARP
- Resolução de endereços.

NAT

- Face ao crescimento acentuado da Internet tornou-se importante a definição de estratégias para **conservação dos endereços IP**. (Ver também o conceito de *subredes*)

- Uma tecnologia conhecida como **Network Address Translation** (NAT) permite que um conjunto de computadores use a Internet através de um único endereço IP.



Um dispositivo, colocado entre o sítio privado e a Internet, mantém informação que permite o mapeamento entre o endereço privado e o endereço público.

Aplicações em Rede

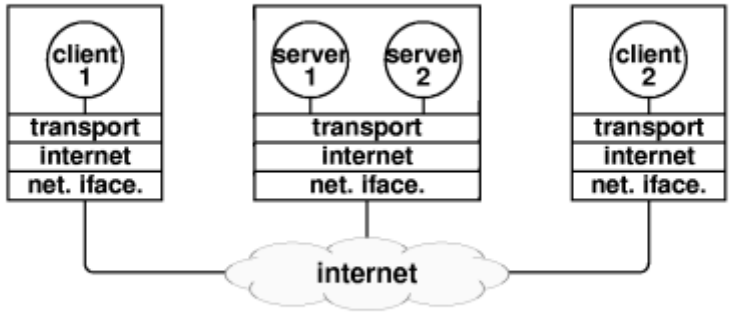
Interacção Cliente/Servidor

- Uma **internet fornece apenas a infraestrutura** de um sistema de comunicação, não inicia comunicações.
- As comunicações são mantidas por, dois ou mais, **programas informáticos**.
- As aplicações em rede usam uma forma de comunicação conhecida como **paradigma cliente/servidor**.
- Uma aplicação **servidor espera, de forma passiva**, por um contacto, enquanto que uma aplicação **cliente inicia comunicações activamente**.

Interacção Cliente/Servidor

- O fluxo de informação, numa interacção cliente/servidor, pode ser em qualquer sentido.

- A generalidade dos programas servidores permitem a **execução simultânea** de várias instâncias (concorrência).



Interacção Cliente/Servidor

- A interface entre um programa informático e os protocolos de comunicação é conhecida como a **Application Program Interface** (API).

- A **socket API** é uma norma *de facto* na indústria. Define um conjunto de procedimentos para: estabelecer ligação, enviar dados, receber dados, fechar ligação.

- Um programa vê uma socket como um **mecanismo de entrada e saída de dados**. Seguem o paradigma abrir-ler-escrever-fechar.

DNS

- Os endereços IP não são adequados para manipulação directa por parte dos utilizadores.

- As **pessoas utilizam nomes simbólicos** para identificar recursos.
  - `gnomo.fe.up.pt` → `193.136.28.132`
  - `search.yahoo.com` → `216.109.117.133`

- Para traduzir os nomes em endereços numéricos, a Internet fornece um serviço chamado **Sistema de Nomes de Domínio** (*Domain Name System, DNS*).

DNS

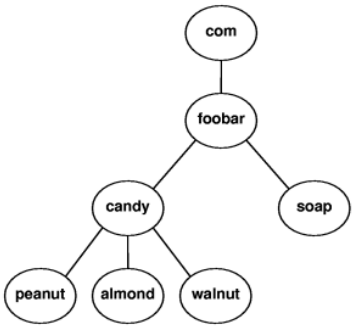
- Os nomes de domínios usam uma **estrutura hierárquica**, representada por uma sequência alfa-numérica de segmentos separados por pontos.

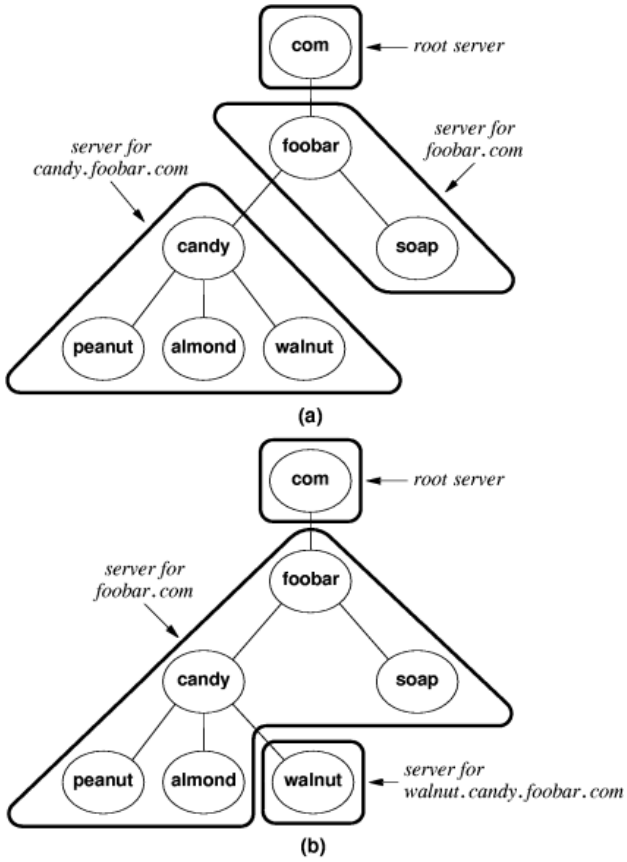
- O **segmento mais significativo** (extremo direito) é designado por domínio de nível de topo (*top-level domain , TLD*).

- Os domínios de topo são controlados a nível internacional pela *Internet Corporation for Assigned Names and Numbers* (**ICANN**). Em Portugal (.pt), a gestão é feita pela **FCCN**.

- Geralmente utiliza-se o primeiro termo de um endereço para designar o serviço oferecido (apenas uma convenção).

DNS





Dois exemplos de como distribuir os servidores para gerir uma mesma hierarquia de nomes.

Cada organização decide como dividir os nomes entre os servidores.

DNS

- Uma aplicação que pretende **resolver um endereço**, torna-se um cliente do sistema de nomes de domínios.
- Um **cliente envia um pedido ao servidor mais próximo** que, responde directamente ou, se não souber a resposta, contacta outros servidores.
- Os servidores têm informação sobre os domínios (zonas) para os quais são **autoridades** (primário).
- Os servidores também podem ter informação sobre outros domínios para os quais são **servidores secundários**. Esta informação é obtida a partir dos primários.

Comando dig e whois

- O **comando dig** (*domain information groper*) permite interrogar o serviço de DNS.

- Sintaxe do comando:
  - `dig [@servidor] [opções] [nome]`

- O **comando whois** permite obter informação administrativa sobre os detentores de domínios.

- Sintaxe do comando:
  - `whois [opções] nome`

Comando dig

```
gnomo> dig www.fe.up.pt

; <<>> DiG 9.2.3 <<>> www.fe.up.pt
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22178
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 5

;; QUESTION SECTION:
;www.fe.up.pt.                  IN      A

;; ANSWER SECTION:
www.fe.up.pt.           86400   IN      CNAME   sifeup.fe.up.pt.
sifeup.fe.up.pt.        86400   IN      A       193.136.28.205

;; AUTHORITY SECTION:
fe.up.pt.               86400   IN      NS      magoo.fe.up.pt.
fe.up.pt.               86400   IN      NS      ns1.fe.up.pt.
fe.up.pt.               86400   IN      NS      ns2.fe.up.pt.

;; ADDITIONAL SECTION:
ns1.fe.up.pt.           86400   IN      A       193.136.28.10
ns1.fe.up.pt.           86400   IN      AAAA    2001:690:2200:9a01::10
ns2.fe.up.pt.           86400   IN      A       193.136.28.9
ns2.fe.up.pt.           86400   IN      AAAA    2001:690:2200:9a01::9
magoo.fe.up.pt.         86400   IN      A       193.136.28.37

;; Query time: 2 msec
;; SERVER: 193.136.28.10#53(193.136.28.10)
;; WHEN: Fri Jan  7 17:51:56 2005
;; MSG SIZE  rcvd: 227
```

Correio Electrónico

- Cada caixa de correio electrónico tem um **endereço único**, dividido em duas partes separadas por @ (*at*):
  - Identificação da caixa.
  - Identificação do computador onde reside a caixa.

  - *caixa*`@`*computador*
  - `joao.silva@empresaweb.pt`

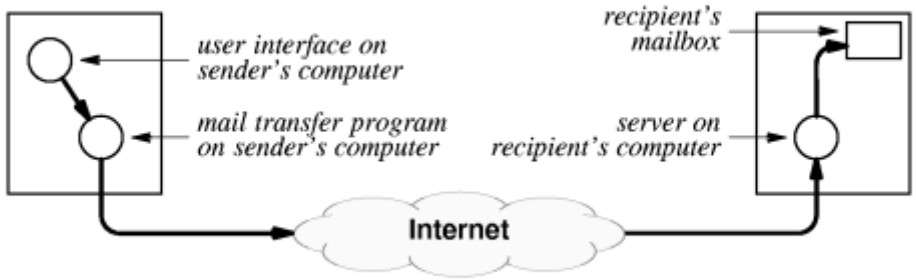
- Os programas no **emissor** usam a segunda parte para seleccionar o destino.

- Os programas no **receptor** usam a primeira parte para seleccionar uma caixa em particular.

Correio Electrónico

- Depois de estabelecida a ligação entre duas máquinas (via TCP), os programas utilizam o *Simple Mail Transfer Protocol* (**SMTP**) para transferir a mensagem.

- O SMTP trata dos detalhes envolvidos na transferência.

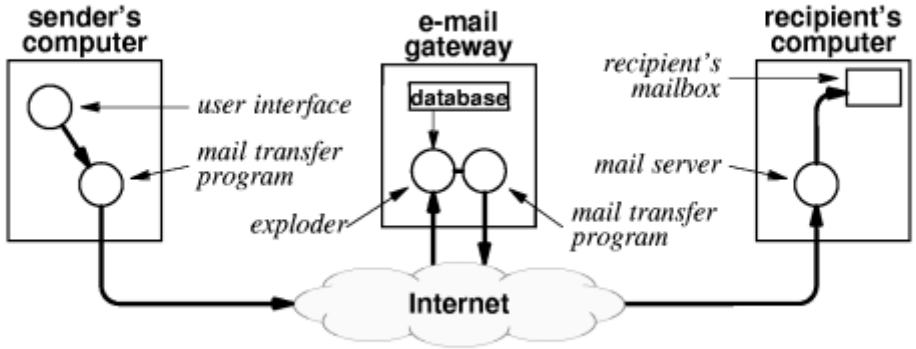


O percurso de uma mensagem de correio electrónico. O programa no computador do emissor torna-se cliente do servidor de correio remoto.

Correio Electrónico

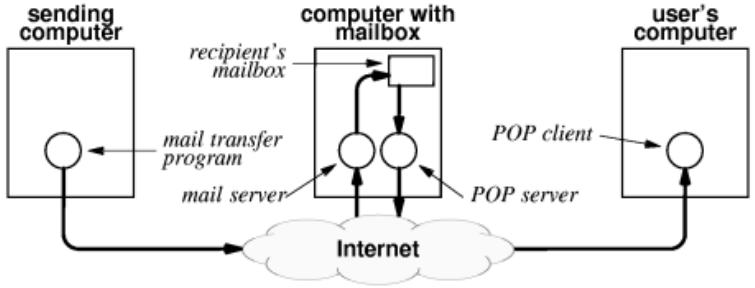
- O serviço de correio electrónico segue uma arquitectura do tipo **armazenamento-e-reenvio** (*store-and-forward*).

- Computadores dedicados a esta tarefa (*mail relaying*), armazenam temporariamente as mensagens e fazem o reenvio.



Correio Electrónico

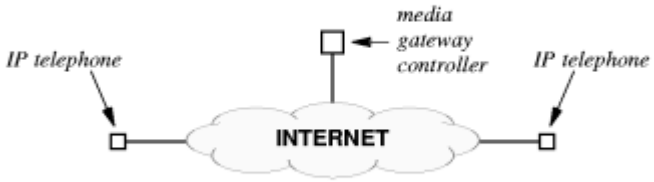
- Uma caixa de correio só pode ser colocada num computador se existir nesse computador um **servidor de correio electrónico**.
- Por outro lado, deve existir uma **ligação permanente** à Internet.
- O *Post Office Protocol* (**POP**) permite aceder a caixas de correio remotas.



Telefonia IP (VoIP)

- **Telefonia IP**, ou **Voz sobre IP** (VoIP), é uma aplicação recente desenvolvida com tecnologias Internet.

- A principal **motivação é económica**. A infraestrutura baseada na comutação de pacotes tem um custo significativamente menor do que a comutação de circuitos tradicionais.



Um telefone IP utiliza um controlador para encontrar outro telefone IP e estabelecer uma chamada.

Transferência de Ficheiros

- Um **serviço de transferência de ficheiros** pode mover uma cópia de um ficheiro de um computador para outro.
- A **transferência de ficheiros é complexa** devido às diferenças na forma como os diferentes sistemas operativos representam os dados.
- O *File Transfer Protocol* (**FTP**) é o protocolo mais popular.
- Problemas de **segurança** têm reduzido o uso deste protocolo. O protocolo SFTP é uma alternativa segura.

World Wide Web

- A *World Wide Web* (**WWW**) é um repositório de larga escala de informação.

- A informação é armazenada em **documentos hiperligados**, que compõem o que se designa por *hipermédia distribuído*.

- A WWW é construída com base em **3 conceitos base**:
  - **Identificação**. Os URL são usados para identificar os recursos.
  - **Recursos**. Os recursos representam informação disponível, podem ser documentos HTML, documentos CSS, imagens, áudio, vídeo, etc.
  - **Transferência**. O protocolo HTTP é usado para a transferência de documentos entre o servidor e os clientes (navegadores).

World Wide Web

- A identificação de cada recurso é feita usando um *Uniform Resource Locator* (**URL**), que tem a seguinte sintaxe genérica:
  - `protocolo://computador:porta/caminho/documento`
  - `http://paginas.fe.up.pt/~ssn/crc/index.html`
  - `http://www.google.com/`
- O *HyperText Transfer Protocol* (**HTTP**) rege a interacção entre o cliente e o servidor.

World Wide Web

- Genericamente, os **documentos Web** podem ser agrupados em três categorias de acordo com a altura em que os conteúdos são determinados:
  - **Estáticos**. Um documento estático reside num ficheiro no servidor Web. Cada pedido resulta sempre no mesmo conteúdo.
  - **Dinâmicos**. Um documento dinâmico é criado pelo servidor Web de cada vez que é pedido. Exemplos: PHP, ASP, Perl.
  - **Activos**. Um documento activo corresponde a um programa que é executado localmente pelo cliente. Exemplos: Flash, Java, JavaScript.

Segurança em Redes

- Uma rede não pode ser categorizada de forma absoluta como segura ou não segura. **Não existe uma definição única** que satisfaça todas as necessidades.

- A definição de uma política de segurança é complexa porque é necessário considerar, para além dos **aspectos técnicos**, os **aspectos humanos**.

- Para definir uma política de segurança é necessário quantificar o **valor da informação**. Uma tarefa complexa porque a informação é, muitas vezes, armazenada ou comunicada de forma arbitrária.

Segurança em Redes

- **Aspectos de segurança** que devem ser considerandos aquando da definição de políticas:
  - **Integridade dos Dados**. Refere-se à protecção face à mudança. A mensagem enviada é exactamente igual à recebida?
  - **Disponibilidade dos Dados**. Refere-se à protecção face a interrupções do serviço. Os dados mantêm-se acessíveis a utilizadores legítimos?
  - **Confidencialidade dos Dados**. Refere-se à protecção contra acessos não autorizados.
  - **Privacidade**. Refere-se à protecção face à intromissão e descoberta.

Segurança em Redes

- Várias **tecnologias** foram desenvolvidas para lidar com os vários aspectos da segurança. Alguns exemplos:
  - *Cyclic Redundancy Check* (CRC)
  - *Pretty Good Privacy* (PGP)
  - *Public Key Infrastruture* (PKI)
  - *Secure Shell* (SSH)
  - *Secure Socket Layer* (SSL)
  - *Wired Equivalent Privacy* (WEP)
  - *Virtual Private Network* (VPN)
  - *Firewall*

Bibliografia

- **Principal**
  - Douglas E. Comer – *Computer Networks and Internets*. 4ª Edição. Prentice-Hall, 2004.

- **Secundária**
  - Douglas E. Comer – *The Internet Book*. 3ª Edição. Prentice-Hall, 2003.
  - Andrew S. Tanenbaum – *Computer Networks*. 4ª Edição. Pearson, 2003.
  - William Stallings – *Data and Computer Communications*. 6ª Edição. Prentice-Hall, 2000.
  - Douglas E. Comer – *Computer Networks and Internets (book website)*. http://www.netbook.cs.purdue.edu/
  - CISCO – *Internetworking Technology Handbook*. http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/
  - Wikipedia – *Computer Network*. http://en.wikipedia.org/wiki/Computer_network