3. Arquitectura TCP/IP

3.1 – Arquitectura

3.2 – Camada de Rede

3.3 – Camada de Transporte

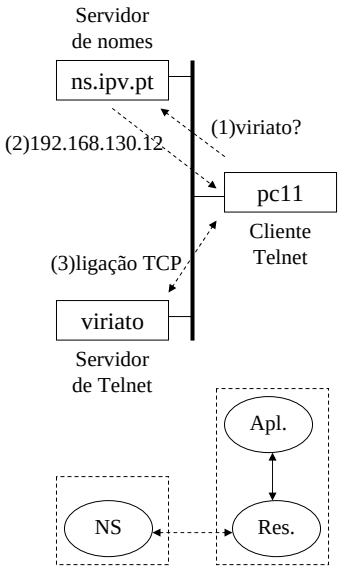
3.4 – Camada de Aplicação

- Domain Name System (DNS)
- Trivial File Transfer Protocol (TFTP)
- Bootstrap Protocol (BOOTP) → DHCP
- Telnet
- File Transfer Protocol (FTP)
- Simple Mail Transfer Protocol (SMTP)

DNS

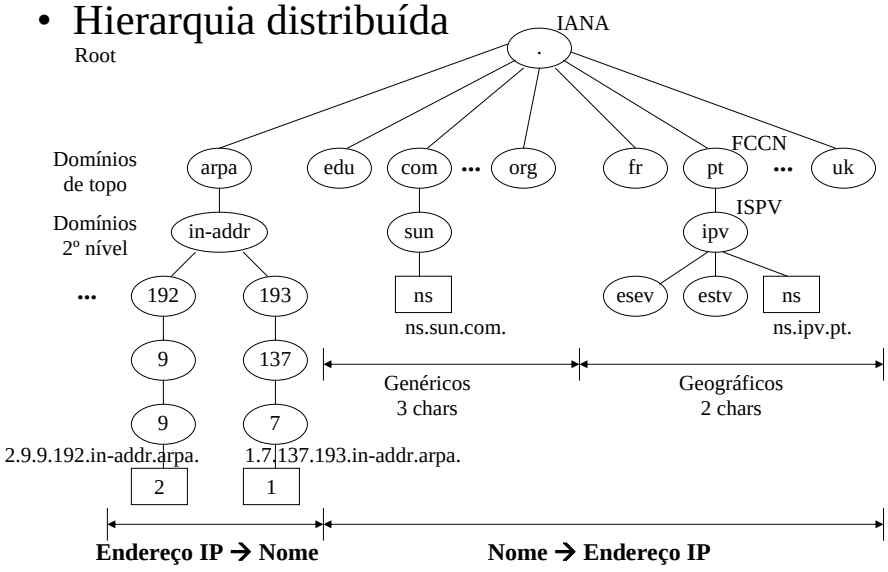
Serviço disponibilizado

- Base de dados distribuída para:
  - mapeamento entre nomes e endereços IP; e
  - encaminhamento de e-mail
- Aplicações acedem ao DNS através do ***resolver*** para traduzir nomes em endereços e vice-versa
- *Resolver* consulta um ou mais **servidores de nomes** para efectuar o mapeamento
- A consulta utiliza normalmente o protocolo UDP:53
- Nome completo: Fully Qualified Domain Name – FQDN
- Nome incompleto: acrescentar domínio



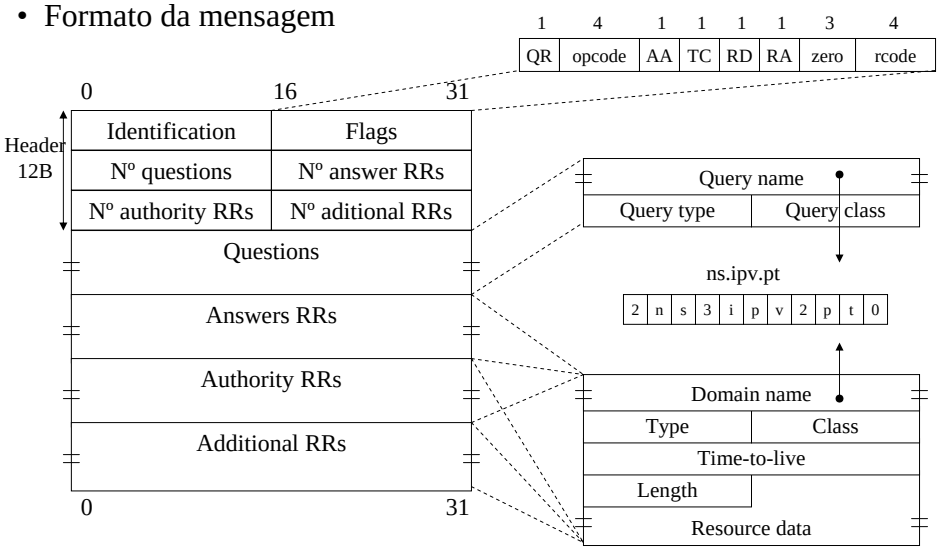
DNS

- Hierarquia distribuída



DNS

- Formato da mensagem



DNS

- Formato da mensagem (cont.)
  - Identification(16b): colocado por cliente, devolvido por servidor
  - Flags(16b):
    - QR(1b): 0→Query; 1→Response
    - Opcode(4b): 0→standard query; 1→inverse; 2→server status
    - AA(1b): Authority answer
    - TC(1b): Truncated→mais que 1 datagrama UDP (512B)
    - RD(1b): Recursion desired → servidor a resolver se não estiver na sua BD
    - RA(1b): Recursion available
    - Rcode(4b): 0→sem erros; 3→erro no formato do nome
  - Numbers(16b):
    - Pedidos: NºQ=1 (ou mais); 3 NºA=0
    - Respostas: NºQ=1 (ou mais); 3 NºA=1 ou mais

DNS

- Formato da mensagem (cont.)
  - Query/Domain name: nome a pesquisar. Sequência de etiquetas. Cada etiqueta tem comprimento e caracteres. Termina com zero
  - Type(16b): tipo de pedido(Q) ou resposta(R). Mais comuns:
    - A(1)→IP Address – Nome→Endereço (Q/R)
    - NS(2)→Name Server (Q/R)
    - CNAME(5)→Canonical Name (Q/R)
    - PTR(12)→Pointer record – Endereço→Nome (Q/R)
    - MX(15)→Mail eXchange record (Q/R) ← Exemplo: palmeida@ipv.pt
    - AXFR(252)→zone transfer request (Q)
    - ANY(255)→all records request (Q)
  - Class(16b): 1→Internet Address (inet)
  - Time-to-live (32b): nº de segundos que pode guardar em *cache*
  - Length(16b): comprimento do resource data
  - Resource data: conteúdo depende do tipo

DNS

# ping www.fccn.pt 	
Pinging nectar.fccn.pt [193.136.2.216]
	DNS (response):
	- Transaction ID=26 (0x0026)
	- Flags=Std query response, no error (0x8580)
	- Question=1 (0x0001)
	- Answer RRs=2 (0x0002)
	- Authority RRs=2 (0x0002)
	- Additional RRs=2 (0x0002)
	- Query:
	  - www.fccn.pt; A; inet
	- Answer:
	  - www.fccn.pt; CNAME; inet; 5m; 9B; nectar
	  - nectar.fccn.pt; A; inet; 5m; 4B; 193.136.2.216
	- Authority:
	  - fccn.pt; NS; inet; 5m; 7B; ns02.fccn.pt
	  - fccn.pt; NS; inet; 5m; 7B; ns01.fccn.pt
	- Additional:
	  - ns01.fccn.pt; A; inet; 5m; 4B; 193.136.192.40
	  - ns02.fccn.pt; A; inet; 5m; 4B; 193.136.2.228

DNS (query):
- Transaction ID=26 (0x0026)
- Flags=Standard query RD (0x0100)
- Question=1 (0x0001)
- Answer RRs=0 (0x0000)
- Authority RRs=0 (0x0000)
- Additional RRs=0 (0x0000)
- Query:
  - Name=www.fccn.pt
  (0x03777777 046663636E 027074 00)
  - Type=A (0x0001)
  - Class=inet (0x0001)	

DNS

- Servidores de nomes
  - Pelo menos dois, um na rede local outro no ISP
  - Cada servidor mantém duas BD por domínio, uma para resolver nomes outra para resolver endereços
  - Pode manter *cache* para resolver mais rápido (normal em servidores recursivos)
  - Contém uma BD com os *root-servers*
  - Pode delegar sub-domínios a outros servidores
  - Tipos de servidor:
    - Primário: mantém as BD
    - Secundários: copiam as BD do primário (através de ligações TCP:53)
  - Recursividade, se pedido não está nas BD:
    - Servidor não recursivo: devolve endereço IP do NS respectivo
    - Servidor recursivo: consulta o NS respectivo e devolve o mapeamento
  - Problemas de segurança: envenenamento do DNS

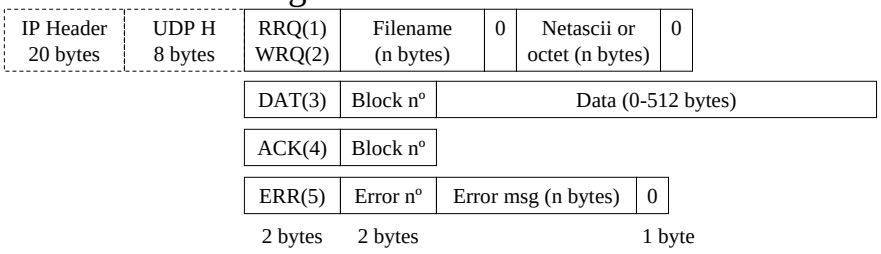
NOTA: o *resolver* (cliente) não faz cache, no entanto as aplicações que o utilizam podem fazer

TFTP

Serviço disponibilizado:

- Transferência de ficheiros
- Implementação pequena e simples para caber em ROM
- Usado em sistemas sem disco (router, switch, ...)
- Utiliza o protocolo UDP:69 (pequeno e simples)
- Não existe segurança (*username* e *password*)

Formato das mensagens:



TFTP

- Modo de operação típico:
  - 1º - cliente envia pedido de leitura (RRQ) com a indicação do nome do ficheiro e o modo de transferência
  - 2º - servidor envia bloco de dados de 512 bytes
  - 3º - cliente envia confirmação de recepção
  - 4º - repete-se 2º e 3º passo ← *stop-and-wait*
  - 5º - bloco menor que 512B indica fim do ficheiro (0B se o comprimento dos dados for múltiplo de 512)
- Notas:
  - É normal o servidor usar outro porto no 2º passo para deixar o porto 69 livre para outros clientes
  - O modo de transferência (*netascii* ou *octet*) serve para formatar os dados do mesmo modo em ambos os lados (camada de Apresentação do modelo OSI)

BOOTP, DHCP

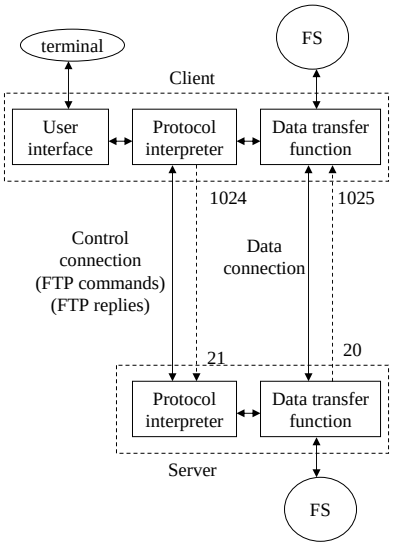
- Serviço disponibilizado:
  - Obter configurações de rede:
    - Endereço IP e máscara de rede
    - Endereço IP de saída da LAN (*gateway*)
  - Obter ficheiro de arranque
    - Nome do servidor
    - Nome do ficheiro
  - Utiliza o protocolo UDP:67(servidor):68(cliente)
- Modo de operação típico:
  - Cliente envia pedido para toda a rede (255.255.255.255)
  - Servidor responde com as configurações (consulta BD através do endereço físico do cliente)
  - Cliente utiliza TFTP para obter ficheiro de arranque
- Dynamic Host Configuration Protocol (DHCP):
  - Semelhante ao BOOTP. As configurações de rede podem ser mais completas (domínio, proxy, ...) e válidas num dado período (*lease*)

TELNET

- Serviço disponibilizado:
  - Execução remota através de um terminal virtual de rede (NVT)
  - Servidor/cliente mapeamento dos seus terminais para o NVT
  - Utiliza o protocolo TCP:23
- Modo de operação típico:
  - Cliente envia caracter (tecla pressionada)
  - Servidor ecoa caracter para o cliente
  - Cliente mostra o caracter (ecrã)
- Comandos do Telnet:
  - Sinalização em banda; byte 0xFF seguido de comando
  - Exemplos: EOF(236); ABORT(238); NOP(241); BRK(243)
- Opções do Telnet:
  - Negociadas no início
  - Exemplos: echo(1); terminal type(24); window size(31); line mode(34)

FTP

- Serviço disponibilizado:
  - Transferência de ficheiros
  - Ligação de controlo (LC) para transferir comandos e respostas
  - Ligação de dados (LD) para transferir a informação (uma por ficheiro)
  - Utiliza o protocolo TCP:21(LC):20(LD)
- Modo de operação típico:
  - 1. Ligação de controlo – servidor cria ligação passiva e espera por ligações activas de clientes. Esta ligação fica activa durante todo o tempo de comunicação entre o cliente e o servidor
  - 2. Ligação de dados – criada cada vez que é necessário transferir um ficheiro



FTP

- Representação dos dados:
  - 1. Tipo de ficheiro
    - **ASCII file type** (texto)
    - EBCDIC file type (texto – entre sistemas EBCDIC)
    - Image file type (binário)
    - Local file type (binário – sistemas com tamanhos de bytes diferentes)
  - 2. Controlo do formato (ficheiros de texto)
    - **Nonprint**
    - Telnet format control
    - Fortran carriage control
  - 3. Estrutura
    - **File structure** (sem estrutura interna)
    - Record structure (com estrutura interna, só para ficheiros de texto)
    - Page structure (sistema operativo TOPS-20)
  - 4. Modo de transmissão
    - **Stream mode** (fluxo de bytes)
    - Block mode (fluxo de blocos – cabeçalho mais dados)
    - Compressed mode (compressão dos dados)

FTP

- Comandos da aplicação (depende da implementação):
  - ! delete literal prompt send
  - ? debug ls put status
  - append dir mdelete pwd trace
  - ascii disconnect mdir quit type
  - bell get mget quote user
  - binary glob mkdir recv verbose
  - bye hash mls remotehelp
  - cd help mput rename
  - close lcd open rmdir

FTP

- Comandos FTP:
  - Caracteres enviados numa linha (CR + LF) no formato:
    - COMD [parâmetro] CRLF
  - Alguns comandos:
    - USER *username* – nome do utilizador
    - PASS *password* – enviar password
    - ABOR – abortar comando anterior ou transferência de dados
    - LIST *filelist* – listar ficheiros ou directorias
    - PORT *n1,n2,n3,n4,n5,n6* – endereço IP (n1.n2.n3.n4) e porto (n5*256 + n6) do cliente
    - QUIT – terminar comunicação
    - RETR *filename* – obter ficheiro (download)
    - STOR *filename* – colocar ficheiro (upload)
    - SYST – tipo de servidor
    - TYPE *type* – estabelece tipo de ficheiro (A: ASCII, I: Image)

FTP

- Respostas FTP:
  - Caracteres enviados numa linha (CR + LF) no formato
    - XYZ descrição CRLF
  - Significado dos dígitos
    - 1yz – resposta positiva preliminar
    - 2yz - resposta positiva completa
    - 3yz - resposta positiva intermédia
    - 4yz – resposta negativa transiente
    - 5yz – resposta negativa permanente
    - x0z – erro de sintaxe
    - x1z – informação
    - x2z – ligação
    - x3z – autenticação e contabilidade
    - x4z – não especificada
    - x5z – estado do sistema de ficheiros
    - xyz – z especifico para cada resposta

FTP

C:\>ftp -d 193.137.7.10	Cliente estabelece ligação activa
Connected to 193.137.7.10.	
220 FTP server ready.	Servidor 1º enviar (completa, ligação)
User (193.137.7.51:(none)): anonymous	
---> USER anonymous	Cliente envia USER
331 Guest login ok, send your e-mail address as password.	Servidor responde (intermédia, autenticação)
Password:	
---> PASS palmeida@ipv.pt	Cliente PASS
230 Guest login ok, access restrictions apply.	Servidor (completa, autenticação)
ftp> cd net	
---> CWD net	Cliente CWD
250 CWD command successful.	Servidor (completa, FS)
ftp> ls	-- ls -> PORT + NLST --
---> PORT 172,16,0,1,5,66	Cliente PORT 172.16.0.1 1346
200 PORT command successful.	Servidor (completa, sintaxe)
---> NLST	Cliente NLST
150 Opening ASCII mode data connection for file list.	Servidor (preliminar, FS)
floppy.tgz malloc.tar.gz squid-2.4.STABLE4-src.tar.gz	-- transferência do ficheiro --
226 Transfer complete.	Servidor (completa, ligação) ←dados
ftp: 57 bytes received in 0,03Seconds 1,90Kbytes/sec.	
ftp> quit	
---> QUIT	Cliente QUIT
221 Goodbye.	Servidor (completa, ligação)

FTP

- Utilizador *anonymous*:
  - Permite que qualquer pessoa entre no servidor (normalmente, só com direitos de leitura)
  - Deve-se enviar o endereço de e-mail como *password*
  - Alguns servidores requerem que o endereço IP do cliente tenha um nome associado (pesquisa DNS do tipo PTR)
- Modo de transferência passivo
  - Por questões de segurança, o estabelecimento de ligações TCP de sistemas externos (servidor) para sistemas internos (cliente) não é permitida em muitas redes
  - Cliente indica ao servidor para abrir ligação de dados passiva:
    - PASV ← cliente
    - 227 Entering passive mode (193,137,7,10,99,16) ← servidor
  - Cliente estabelece ligação de dados activa para o porto devolvido na resposta ao comando PASV
  - Cliente/Servidor transfere ficheiro

SMTP

- O SMTP (Simple Mail Transport Protocol) é o protocolo utilizado na Internet para transferência de mensagens entre utilizadores
- Pode funcionar sobre TCP, sobre outro qualquer protocolo ou ainda transferir directamente as mensagens entre processos, quando os utilizadores estão na mesma máquina
- Aplicações de gestão de mensagens: mail, mailx, eudora, Outlook Express ...
- Os utilizadores são endereçados pelo seu “user name” ou por uma outra designação que eles escolham. À identificação dos utilizadores são adicionados os vários domínios hierárquicos a que eles pertencem

SMTP

- Um endereço de correio electrónico tem a forma:
  - utilizador@computador.domínio; ou
  - utilizador@domínio
- Exemplo:
  - palmeida@infante.ipv.pt
    - Aplicação cliente utiliza o DNS para obter o endereço IP (A infante.ipv.pt → 193.137.7.3)
    - Cliente estabelece ligação activa para o servidor na porta 25
  - palmeida@ipv.pt
    - Aplicação cliente utiliza o DNS para obter servidores do domínio (MX ipv.pt → 10 infante; 20 teotonio)
    - Aplicação cliente utiliza o DNS para obter o endereço IP (A infante.ipv.pt → 193.137.7.3)
    - Cliente estabelece ligação activa para o servidor na porta 25
    - Cliente tenta outros servidores se o utilizador não existir no actual

SMTP

- Envio:
  - Aplicação cliente envia e-mail por SMTP para o agente de transferência de mensagens (MTA – *Message Transfer Agent*) existente na rede local (*relay* MTA)
  - O *relay* MTA guarda-o na *mailbox* se o destinatário for local ou envia-o para o *relay* MTA da rede destino
  - Políticas de *anti-relay* para evitar o envio de mensagens cujo remetente não seja local (o envio por SMTP não requer autenticação)
- Recepção:
  - Aplicação cliente consulta *mailbox* do *relay* MTA através de um dos seguintes protocolos:
    - POP3 (Post Office Protocol version 3)
      - » Só permite uma pasta para guardar todos os e-mails
      - » Permite deixar os e-mails no servidor (pouco comum)
    - IMAP4 (Interactive Mail Access Protocol version 4)
      - » Permite uma estrutura de pastas para guardar os e-mails
      - » Permite marcar as mensagens como lidas
      - » Permite deixar os e-mails no servidor (mais comum, webmail)