Arquitetura de Rede de Computadores

TCP/IP – Protocolos e Serviços

Prof. Pedro Neto

Aracaju – Sergipe - 2011

Ementa da Disciplina

5. TCP/IP - Protocolos e Serviços
    i. Protocolos da Camada de Internet/Rede
        a. ARP
        b. RARP
        c. IP
        d. ICMP
        e. Protocolos de Roteamento
            - RIP
            - OSPF
    ii. Protocolos da Camada de Transporte
        a. UDP
        b. TCP

Ementa da Disciplina

iii. Protocolos da Camada de Aplicação
   a. DNS
   b. DHCP
   c. TELNET
   d. FTP
      - TFPT
   e. SMTP
   f. POP3 e IMAP
   g. HTTP

TCP/IP –Protocolos e Serviços

Protocolos da Camada de Internet - Rede

- A camada de rede trata da comunicação entre máquinas.
- Fornece funções necessárias para interconectar redes e gateways formando um sistema coerente .
- É responsável pela entrega de dados desde a origem até o destino final.
- Responsável pelo Roteamento.

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

Protocolos da Camada de Internet - Rede

Esta camada aceita uma requisição de envio de pacote, vinda da camada de **Transporte**, com a identificação da máquina para onde o pacote deve ser transmitido. Encapsula o pacote em um **Datagrama IP**, preenche o cabeçalho do **Datagrama**, usa um algoritmo de roteamento para determinar se o **Datagrama** deve ser entregue diretamente, ou enviado para um **Gateway**. Finalmente, o **Datagrama** é passado para a interface de rede apropriada, para que este possa ser transmitido.

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

ARP – Address Resolution Protocol

As redes TCP/IP baseiam-se inteiramente em um endereço virtual: o IP, porém as máquinas são identificadas pelos protocolos das camadas abaixo através do endereço físico: o MAC.

O protocolo ARP é responsável por fazer a conversão entre os endereços IP e MAC da rede. Tomemos como exemplo uma grande rede onde os pacotes TCP/IP são encaminhados até a rede de destino através de roteadores. Na rede de destino o protocolo ARP entra em ação para detectar o endereço MAC para onde o pacote deve ser entregue, uma vez que há somente o endereço IP.

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

ARP – Address Resolution Protocol

Primeiramente o **ARP** manda uma mensagem de Broadcast para rede perguntando se todas as máquinas qual delas responde pelo endereço IP de destino. A máquina correspondente responde enviando seu endereço MAC para que transmissão possa ser estabelecida.

Para evitar mensagens de broadcast sucessivas, o dispositivo transmissor armazena em memória os últimos endereços MAC acessados e seus respectivos IPs.

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

RARP – Reverse Address Resolution Protocol

Este protocolo faz o inverso do protocolo **ARP**: Ele descobre o endereço IP através do MAC.

Utilizados em redes onde as estações de trabalho não possuem armazenamento local (HD), conhecidas também como clientes magros (Thin Clients). Neste caso as máquinas não tem como acessar as informações de seus IP configurados. Há a figura de um servidor RARP que armazena uma tabela com os endereços MACs e seus respectivos IPs.

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP/IP –Protocolos e Serviços

IP – Internet Protocol

O protocolo **IP** obtém os pacotes oriundos dos protocolos da camada de transporte (**UDP e TCP**) e envia para a camada Física (Enlace+Física). Na camada de rede, os pacotes são encapsulados em **datagramas**, e na camada abaixo, os datagramas são encapsulados em quadros (frames).

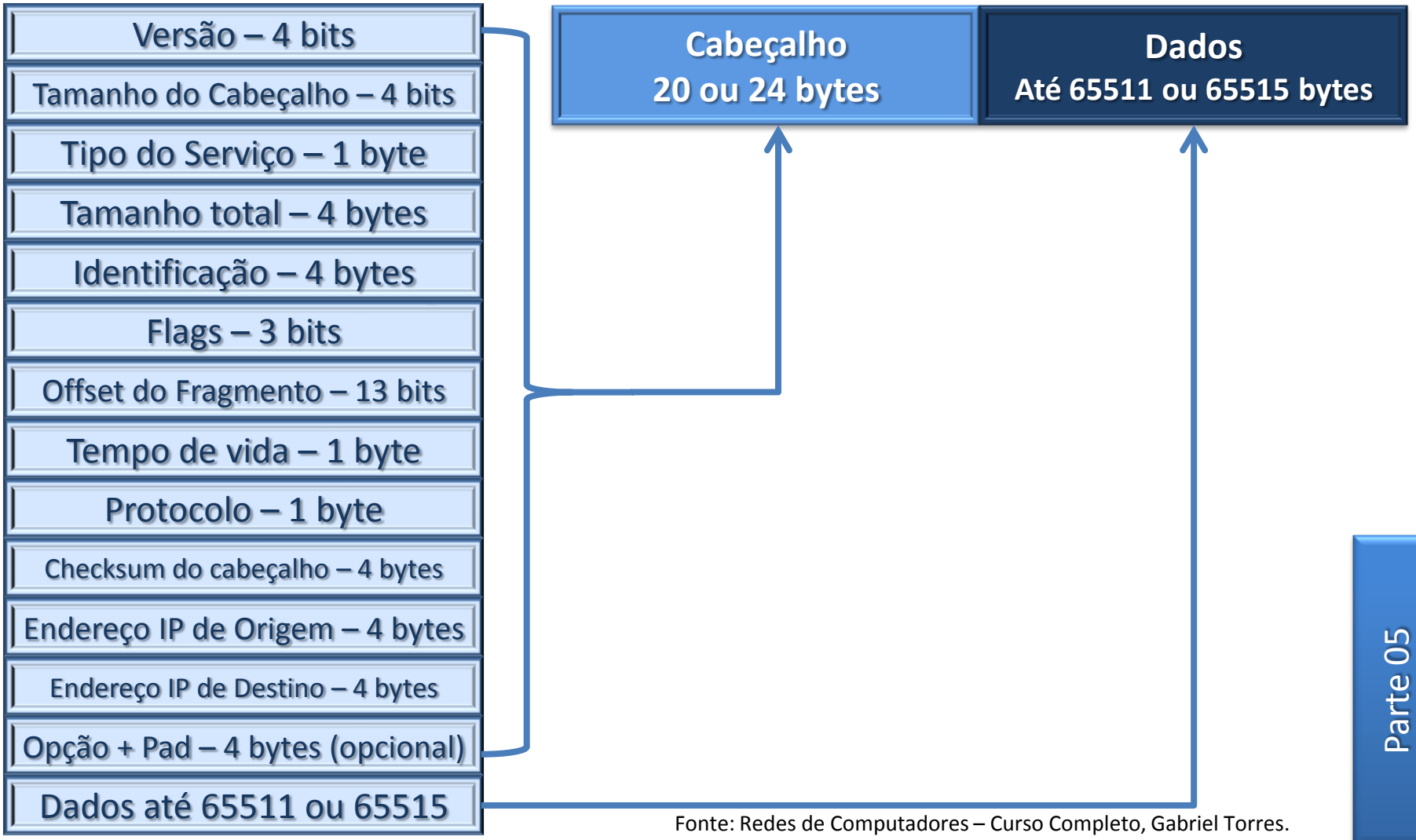
O protoclo **IP** não é orientado a conexão. Em outras palavras, ele não verifica se o **datagrama** chegou ou não ao destino, trabalho este feito pelo protocolo **TCP** (camada de transporte).

A principal função do **IP** é o roteamento, adicionando mecanismos para que o programa chegue mais rapidamente ao destino.

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP/IP –Protocolos e Serviços

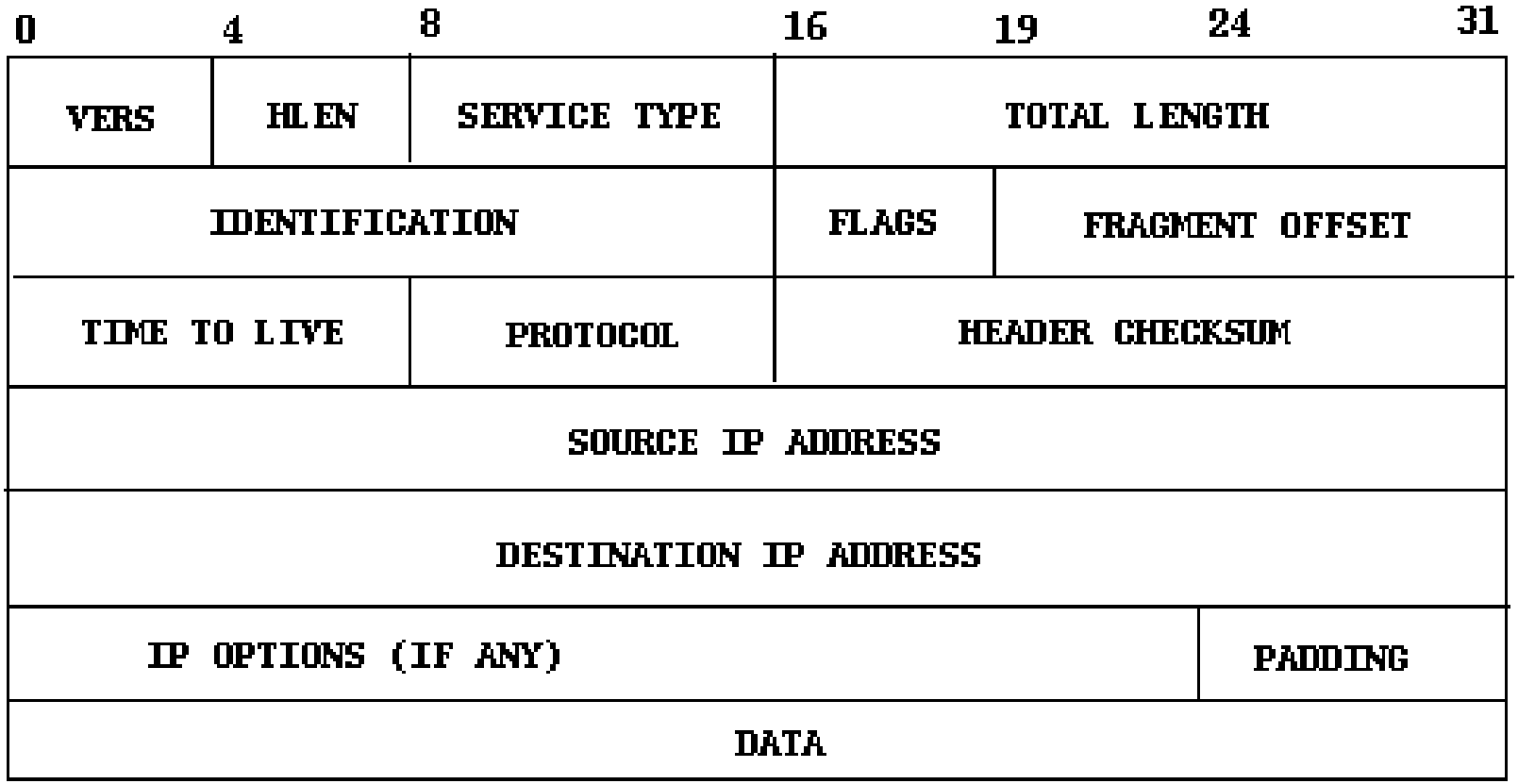
IP – Datagrama



Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP/IP –Protocolos e Serviços

IP – Datagrama



Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP/IP –Protocolos e Serviços

IP – Datagrama

Versão - o primeiro campo do cabeçalho de um **datagrama IPv4** é o campo de versão, com quatro bits.

Tamanho do Cabeçalho - o segundo campo, de quatro bits, é o **IHL** (acrónimo para *Internet Header Length*) com o número de palavras de 32 bits no cabeçalho IPv4 (20 bytes). Um cabeçalho mínimo tem vinte bytes de comprimento, logo o valor mínimo em decimal no campo IHL seria 5.

Tipo do serviço - Informa a qualidade desejada na entrega do **Datagrama.** Campo não utilizado por não apresentar resultados práticos.

Tamanho total – Indica o número total de bytes do **Datagrama.** Sendo de 16 bits, seu tamanho máximo é de 65.535 bytes. Quanto maior o tamanho, maior será o tempo ocupado na rede, tornando-a mais lenta. Logo veremos que o **datagrama** pode ser fragmentado, assumindo tamanhos menores.

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP/IP –Protocolos e Serviços

IP – Datagrama

Identificação. Este campo de 16 bits é usado para identificar fragmentos identificativos do datagrama IP original. Ou seja, em caso de fragmentação, se faz necessária a identificação do **datagrama**.

Flags - o campo de 3 bits que segue é usado para controlar ou identificar fragmentos.

Offset - o campo **offset** do fragmento tem 13 bits, e permite que um receptor determine o local de um fragmento em particular no datagrama IP original.

Tempo de vida - o TTL (*time to live*, ou seja, tempo para viver) ajuda a prevenir que os datagramas persistam (ex. andando aos círculos) numa rede. O valor é decrementado a cada passagem por um Gateway/Roteador, até chegar ao destino, ou se chegar a zero o **datagrama** é descartado.

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP/IP –Protocolos e Serviços

IP – Datagrama

Protocolo – Indica o protocolo que pediu o envio do **datagrama**, através de um código numérico. Ex.: **TCP** = 6, **UDP** = 7, **ICMP** = 1, etc. Dessa maneira o receptor saberá a que protocolo entregar os dados no destino.

Checksum - Realiza o cálculo em cima dos dados somente do cabeçalho, verificando se o mesmo está corrompido.

Endereço de origem/destino – Endereços IP de origem e destino

Opções – Campo opcional, geralmente não utilizado, deixando o cabeçalho com 20 bytes de tamanho. É utilizado em testes de verificação de erro na rede. Armazena a rota percorrida (traceroute).

Dados – Campo que contém os dado encapsulados.

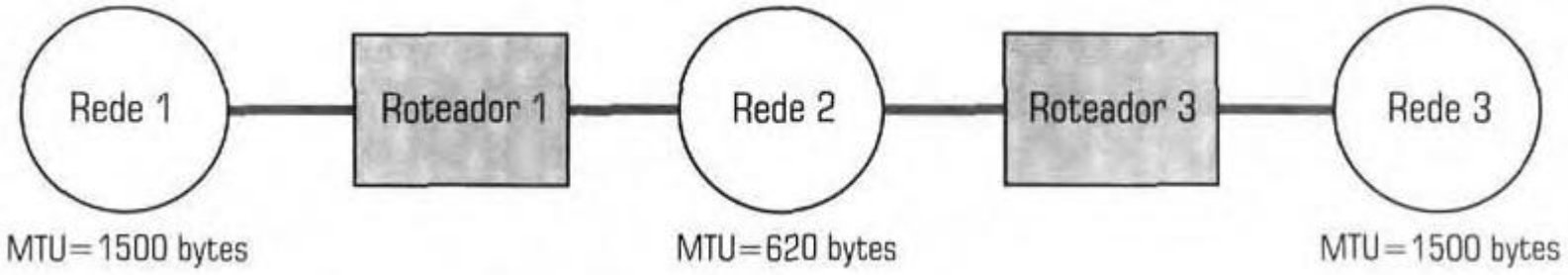
Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP/IP –Protocolos e Serviços

IP – Fragmentação de Datagramas

Os **datagramas** são enviados na camada física através de quadros. Por conta disso, seu tamanho estará limitado ao tamanho dos mesmos de acordo com o protocolo utilizado. No caso do Ethernet, o quadro tem o tamanho máximo de 1500 bytes. Logo o tamanho máximo (cabeçalho + dados) do **datagrama** será de 1500 bytes também. A essa característica nós damos o nome de **MTU** (Maximun Transfer Unit).

A arquitetura TCP/IP foi criada para ser usada em um ambiente de redes heterogêneas interligadas. Na transmissão de uma informação entre redes distintas, pode ocorrer de redes intermediárias possuirem um MTU menor que o da rede de origem. Logo o pacote não caberia no quadro desta rede. É aí que entra a fragmentação de pacotes.

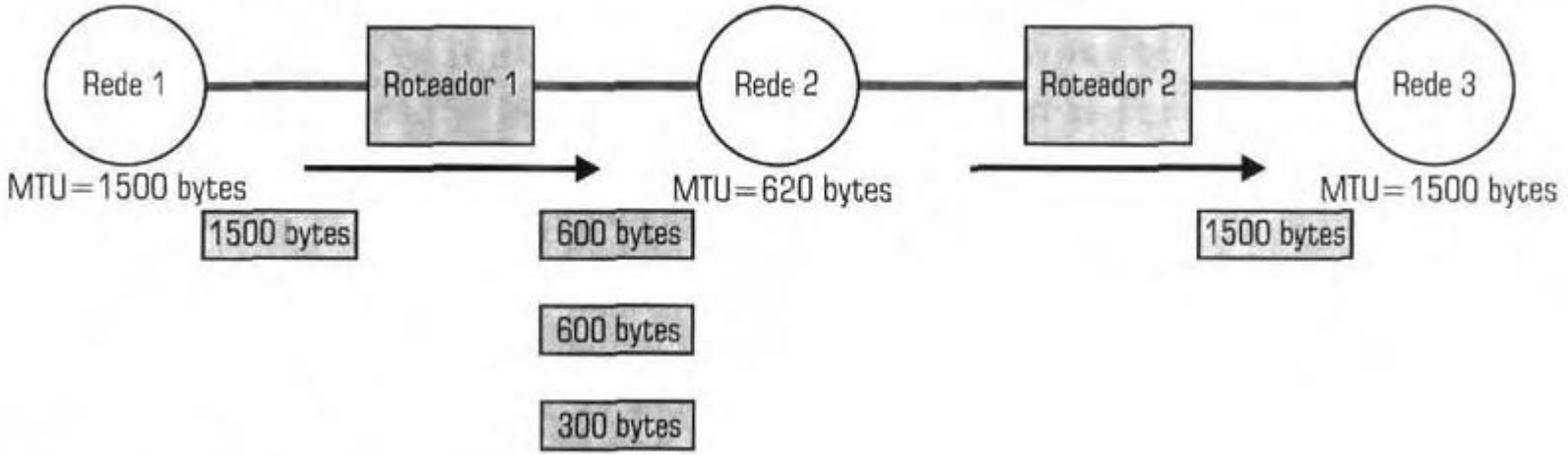


Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP/IP –Protocolos e Serviços

IP – Fragmentação de Datagramas

A fragmentação é realizada pelos roteadores que ao enviar um pacote por uma rede de MTU diferente, fragmenta-o e remonta-o se necessário.



Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

IP – Fragmentação de Datagramas

A fragmentação é possível graças a 3 campos do **datagrama:**

- **Identificação**
  Identifica o **datagrama** de origem da fragmentação.
- **Flags**
  Indica se o **datagrama** pode ou não ser fragmentado e se é ou não o último fragmento.
- **Offset do fragmento**
  Controla a ordem dos fragmentos.

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

ICMP – Internet Control Message Protocol

Parte integrante do protocolo **IP**. Tem como objetivo retornar erros à origem da transmissão. As mensagens **ICMP** geralmente são enviadas automaticamente em uma das seguintes situações:

- Um pacote IP não consegue chegar ao seu destino (p.ex.: Tempo de vida do pacote expirado)
- O Gateway não consegue retransmitir os pacotes na freqüência adequada (p.ex.: Gateway congestionado)
- O Roteador indica uma rota melhor para a máquina a enviar pacotes.

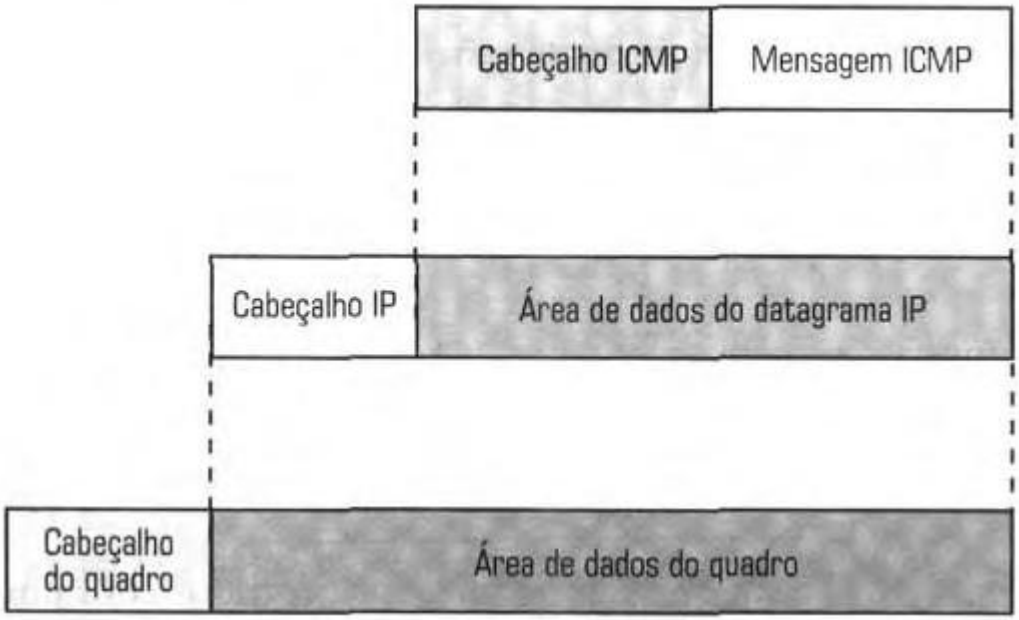
O **ICMP**, como parte do protocolo **IP**, usa um **datagrama IP** para transmitir. Logo, como o **IP** não verifica se o **datagrama** chegou corretamente ao destino , pode ocorrer da mensagem ser perdida no caminho.

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP/IP –Protocolos e Serviços

ICMP – Internet Control Message Protocol

Apesar ser encapsulado no **datagrama IP**, o **ICMP** não é considerado um protocolo de alto nível como **UDP e TCP**.



Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP/IP –Protocolos e Serviços

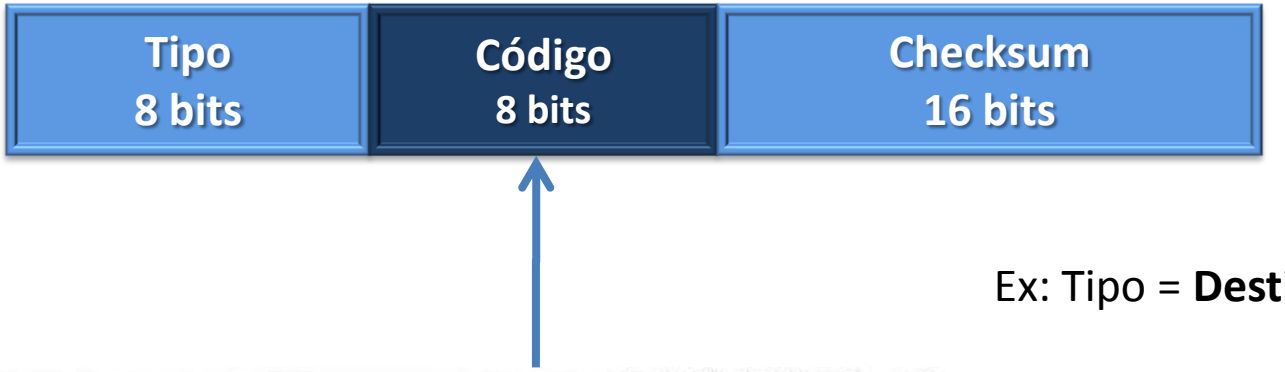
ICMP – Estrutura da Mensagem

Valor	Tipo da mensagem ICMP
0	Resposta à mensagem de eco
3	Aviso de destino inalcançável
4	Redução da velocidade de transmissão
5	Solicitação de redirecionamento
8	Mensagem de eco
11	Tempo de vida excedido
12	Problema nos parâmetros
13	Solicitação de horário
14	Resposta à solicitação de horário
17	Solicitação da máscara de endereçamento
18	Resposta à solicitação da máscara de endereçamento

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP/IP –Protocolos e Serviços

ICMP – Estrutura da Mensagem



Ex: Tipo = **Destino Inalcançável**

Código	Significado
0	Rede inalcançável
1	Máquina inalcançável
2	Protocolo inalcançável
3	Porta inalcançável
4	Fragmentação necessária e flag DF ativado

Código	Significado
5	Falha na rota de origem
6	Rede de destino desconhecida
7	Máquina de destino desconhecida
8	Máquina de origem isolada
9	Comunicação com a rede de destino está proibida pela administração da rede
10	Comunicação com a máquina de destino está proibida pela administração da rede
11	Rede inalcançável para o tipo de serviço solicitado
12	Máquina inalcançável para o tipo de serviço solicitado

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

ICMP – Exemplo de Mensagens

Eco

Verifica se o caminho entre o Transmissor e Receptor está bom. A mensagem de Eco é reenviada de volta pelo Receptor incluindo os dados do **datagrama** original. Ex: utilizado no utilitário Ping.

Destino Inalcançável

Acontece quando um roteador não consegue entregar a informação ao destino. Pode ocorrer quando é necessário fragmentar um **datagrama** e o **Flag** está setado para não fragmentável.

Congestionamento

O Roteador recebe um número de maior de **datagramas** do que ele pode suportar.

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

ICMP – Exemplo de Mensagens

Redirecionamento

Caso haja alguma rota de destino melhor do que a definida no **datagrama**, o roteador informa ao transmissor esta rota para que o mesmo atualiza sua tabela de rotas.

Problemas de Parâmetros

Acontece quando o roteador não consegue decodificar o cabeçalho do **datagrama**.

Solicitação de Horário

Uma máquina solicita o horário de outra na rede. Usado para sincronização de relógios (atraso da rede) e para medição de tempo de reposta na rede.

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

Protocolos de Roteamento

Servem para comunicação entre roteadores em grandes redes, atualizando de forma dinâmica as tabelas de roteamento dos mesmos. Os protocolos de roteamento podem operar de 2 maneiras:

- Informando o menor caminho (baseado em distância)
- Informando o melhor caminho (menos congestionado, baseado no estado do link)

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

Protocolos de Roteamento - RIP

RIP – Routing Information Protocol

Os roteadores enviam suas tabelas de roteamento para os demais roteadores para que eles atualizaem suas tabelas, mantendo as rotas atualizadas.

Busca definir as melhores rotas baseadas na distância, o que nem sempre representa o melhor. Caminhos congestionados ou fora do ar não são levados em conta

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

Protocolos de Roteamento - OSPF

OSPF – Open Shortest Path First

Apesar do nome, este protocolo, diferentemente do **RIP**, é baseado na melhor rota (mais rápida), ou seja, no estado do link.

Resolve as questões do **RIP.**

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

Protocolos da Camada de Transporte

Os protocolos na camada de transporte podem resolver problemas como confiabilidade (o dado alcançou seu destino?) e integridade (os dados chegaram na ordem correta?). Na arquietura TCP/IP os protocolos de transporte também determinam para qual aplicação um dado qualquer é destinado.

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP/IP –Protocolos e Serviços

UDP – User Data Protocol

Se difere do TCP por:

- Protocolo de transporte não orientado à conexão.
- Não verifica se o pacote de dados chegou ao destino.
- A montagem e checagem da informação fica por conta da Aplicação.

Com isso:

- Transmissão mais rápida
- Tamanho do pacote de dado menor.
- Não mecanismos de verificação.

Utilizado em:

- Redes pequenas e confiáveis.
- Dados pequenos.
- Aplicações não preocupadas com a confiabilidade dos dados

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP/IP –Protocolos e Serviços

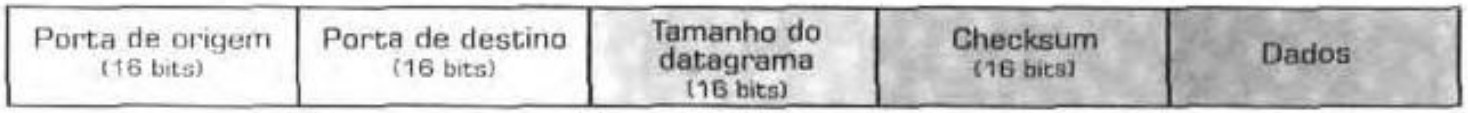
UDP – Usos mais comuns

Porta	Uso
7	Eco
9	Discard
13	Daytime
15	Netstatus
19	Chargen
37	Time
42	Host Name Server
43	Whois
53	DNS
69	TFTP

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP/IP –Protocolos e Serviços

UDP – Datagrama/Pacote



Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP/IP –Protocolos e Serviços

TCP – Transmission Control Protocol

- Protocolo mais complexo da arquitetura TCP/IP.
- Responsável pela checagem e ordenação dos datagramas
- Utilização de canais virtuais chamados portas

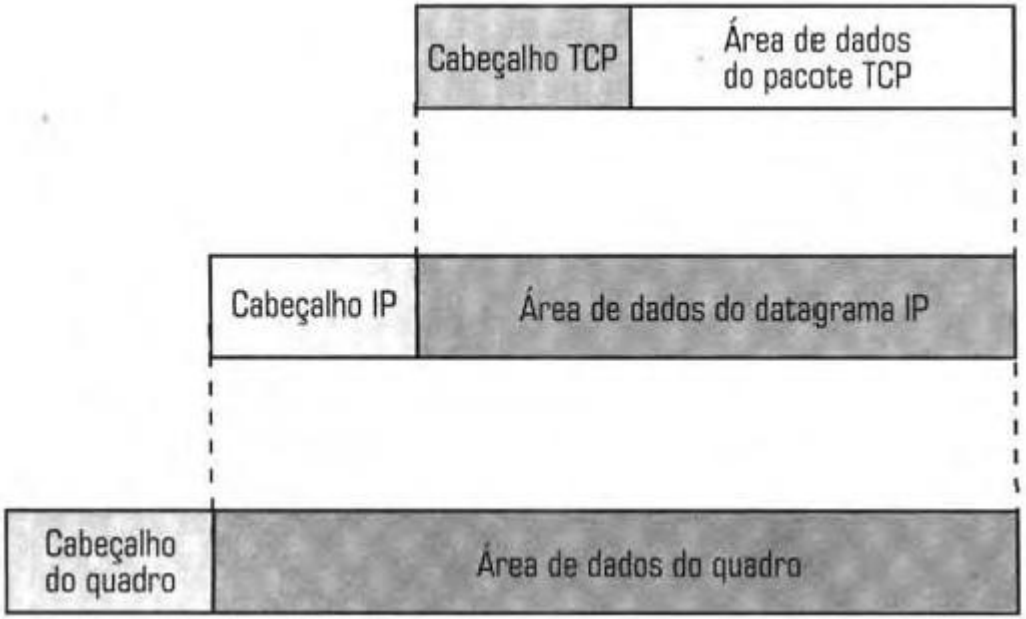
Porta	Uso
11	Systat
15	Netstat
20	FTP (Dados)
21	FTP (Controle)
23	Telnet
25	SMTP
43	Whois
79	Finger
80	HTTP

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP/IP –Protocolos e Serviços

TCP – Transmission Control Protocol

Encapsulamento dos dados TCP/IP.



Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP – Transmission Control Protocol

Ao receber um pacote de dados o TCP envia uma mensagem de confirmação (ack) ao transmissor. Caso o transmissor não receba esta mensagem de confirmação em determinado tempo, o pacote é retransmitido.

Este tempo é conhecido como RTT- Round Trip Time, ou Tempo Aproximado de Viagem, que é calculado dinamicamente pelo TCP.

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP/IP –Protocolos e Serviços

TCP – Conexão

Conexão é a comunicação estabelecida entre 2 máquinas, sendo o TCP responsável por abrí-la, mantê-la e fechá-la.

A abertura é feita através de um processo chamado handshake (aperto de mão). Este processo é feito em 3 tempos.

Transmissor –> Receptor
Receptor –> Transmissor
Transmissor –> Receptor

A conexão é mantida através do envio de dados entre transmissor e receptor.

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP – Conexão

Ocorrendo tudo bem, e não havendo mais dados para serem transmitidos, a conexão é fechada pelo transmissor. O fechamento é feito da mesma forma que a abertura: handshake em 3 tempos.

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP/IP –Protocolos e Serviços

TCP – Socket

O **TCP** remonta os pacotes em dados e os repassa para os protocolos da camada de aplicação através do uso de **portas**. Porém existe um problema: Pode haver mais de uma aplicação utilizando o mesmo protocolo de aplicação. Por exemplo, 2 browsers abertos acessando a Internet.

Cada porta permite o uso de um conceito chamado **socket**, que define uma conexão dentro de uma porta.
Os **sockets** podem ser classificados em **ativos** e **passivos.** O primeiro envia dados e o segundo recebe.

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP – Janela

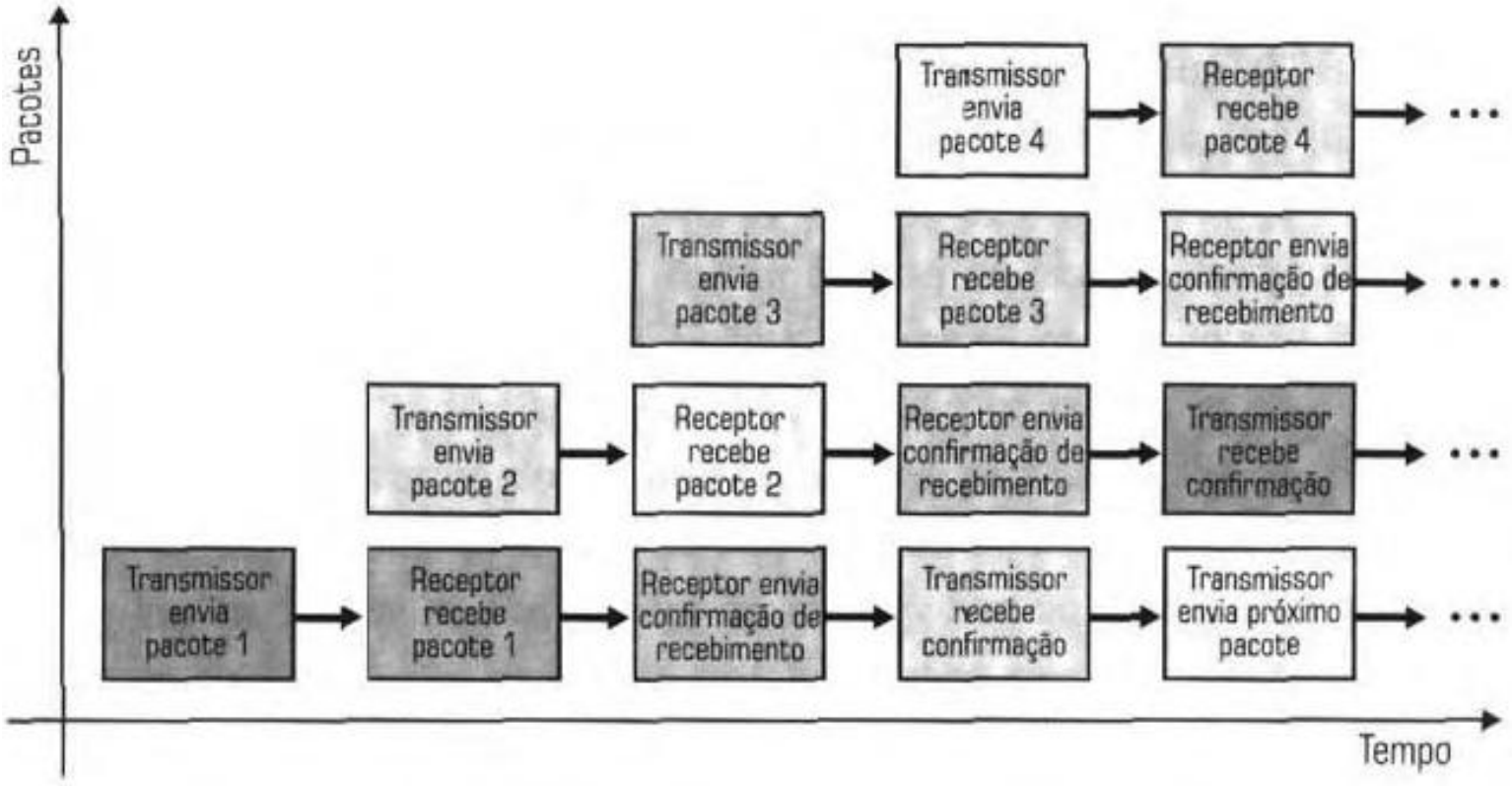
O **TCP** usa o conceito de **Janela** para aumentar o desempenho do envio de pacotes. O transmissor pode enviar outros pacotes antes de ter recebido a confirmação de recebimento dos primeiros pacotes enviados.

A figura a seguir mostra uma **Janela** de 4 pacotes. Este processo aumenta o desempenho do protocolo, pois neste exemplo ao receber a confirmação do primeiro pacote, o transmissor estará enviando o quinto pacote.

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP/IP –Protocolos e Serviços

TCP – Janela



Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP – Janela

O **TCP** utiliza na verdade um processo mais complexo do que o descrito nos slide anterior, onde ao invés de número de pacotes, as **Janelas** são medidas em **bytes** enviados. E o tamanho das **Janelas** é variável e pode ser mudado a qualquer instante pelo protocolo para melhoria do desempenho.

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP – Organização dos Segmentos/Pacotes recebidos

Como falamos, os pacotes podem chegar fora de ordem. Cabe ao **TCP** organizar os pacotes e pedir retransmissão se necessário.

A confirmação de recebimento de um pacote é feita enviando ao transmissor não o número do pacote recebido e sim número de seqüência do próximo pacote. Porém isto gera um problema:

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP – Organização dos Segmentos/Pacotes recebidos

Por exemplo, se o **TCP** estiver trabalhando com uma área de dados de 536 bytes. Os 3 primeiros pacotes irão chegar com os números de seqüência de 1, 537 e 1073.
Caso o primeiro pacote seja perdido no caminho, o transmissor irá enviar a confirmação com o nº da próxima seqüência igual a 1, pois o primeiro pacote é aguardado.

Neste caso os 3 pacotes serão retransmitidos. Esta é uma falha do **TCP:** fazer com que os pacotes de uma **Janela** sejam retransmitidos caso um dos segmentos seja perdido, mesmo que tenham sido recebidos corretamente.

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP/IP –Protocolos e Serviços

TCP – Estrutura do segmento

Porta de Origem – 16 bits
Porta de Destino – 16 bits
Nº de seqüência – 32 bits
Nº de confirmação (Ack) – 32 bits
Offset – 4 bits
Reservado – 6 bits
Bits de Controle – 6 bits
Janela – 16 bits
Checksum – 16 bits
Ponteiro de Urgência – 16 bits
Opções +Pad – 32 bits
Dados

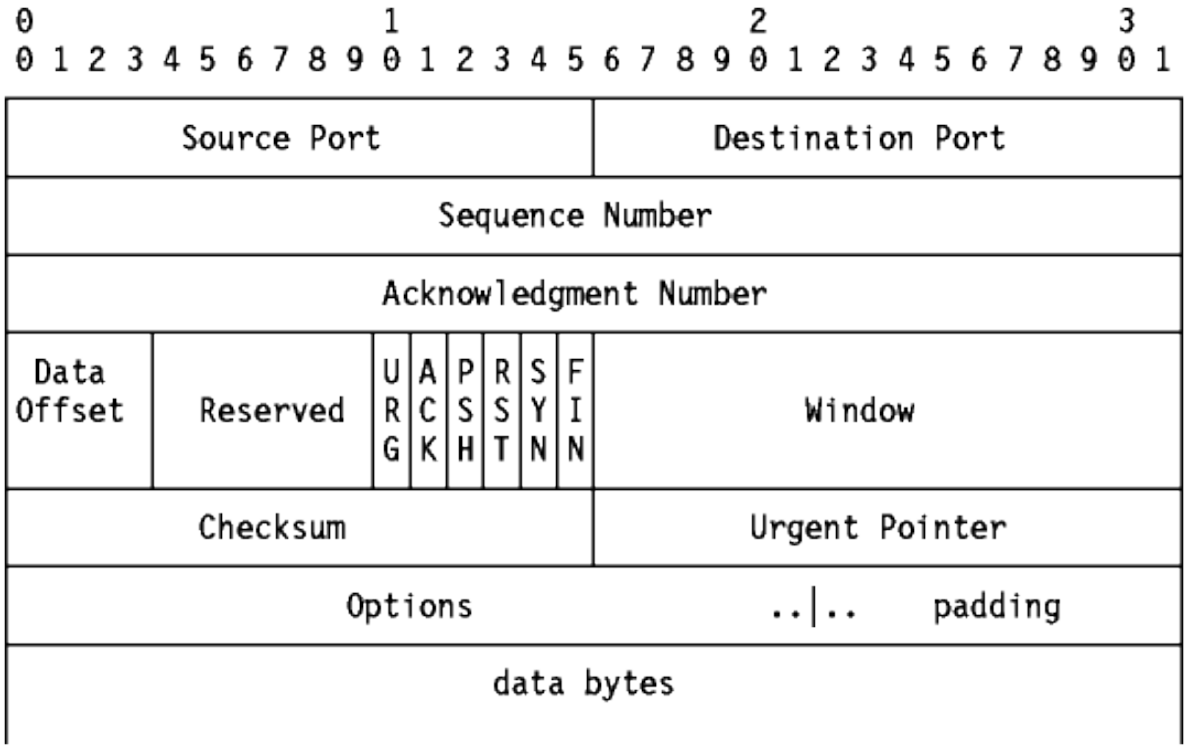
Ao conhecermos a estrutura do protocolo **TCP,** tornar-se-á mais fácil o entendimento de seu funcionamento.

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP/IP –Protocolos e Serviços

TCP – Estrutura do segmento

Representação Clássica



Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP – Estrutura do segmento

Porta de origem
Indica a aplicação que originou os dados.

Porta de destino
Indica a aplicação para os dados serão entregues no receptor.

Nº de Seqüência
Indica o número do primeiro byte presente no segmento.

Nº de confirmação
É o acknowledge (ack). É colocado o número de seqüência do próximo segmento.

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP – Estrutura do segmento

Reservado
Campo não utilizado.

Bits de Controle (Flags)
Usados para controle, conforme a tabela:

Bit	Significado
URG	O campo Ponteiro Urgente é válido
ACK	O campo Número de Confirmação é válido
PSH	Força a entrega dos dados (push)
RST	Reiniciar a conexão
SYN	Sincronismo, determina o Número de Seqüência inicial
FIN	O transmissor chegou ao fim de seus dados

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP – Estrutura do segmento

Tamanho da Janela
Define o tamanho da **Janela** em bytes, usada na conexão.

Checksum
Cálculo para checagem de dados.

Ponteiro de Urgência
Caso existam dados que precisem ser processados antes da conexão chegar ao fim, este campo informa a posição onde os dados urgentes terminam. O bit de controle **URG** deve estar ativado.

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP – Estrutura do segmento

Opções + **Pad**

Campo opcional, geralmente não utilizado, deixando o cabeçalho com 20 bytes de tamanho. É utilizado para troca de informações entre o transmissor e receptor sobre o tamanho máximo do próximo segmento **(MSS – Maximum Segment Size).**

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

Protocolos de Aplicação

Opções + **Pad**

Campo opcional, geralmente não utilizado, deixando o cabeçalho com 20 bytes de tamanho. É utilizado para troca de informações entre o transmissor e receptor sobre o tamanho máximo do próximo segmento **(MSS – Maximum Segment Size).**

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP/IP –Protocolos e Serviços

Protocolos de Aplicação

Aqui descreveremos os protocolos de alto nível, ou seja, os protocolos usados na comunicação das aplicações com a camada de transporte.

Apesar de existirem diversos protocolos , aqui iremos abordar alguns dos protocolos mais comuns.

Vamos a eles.

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

DNS – Domain Name System

O protocolo **DNS** atua como um serviço na rede que permite nomear endereços IP no sentido de localizar as máquinas nas redes, usando nomes no lugar de números.

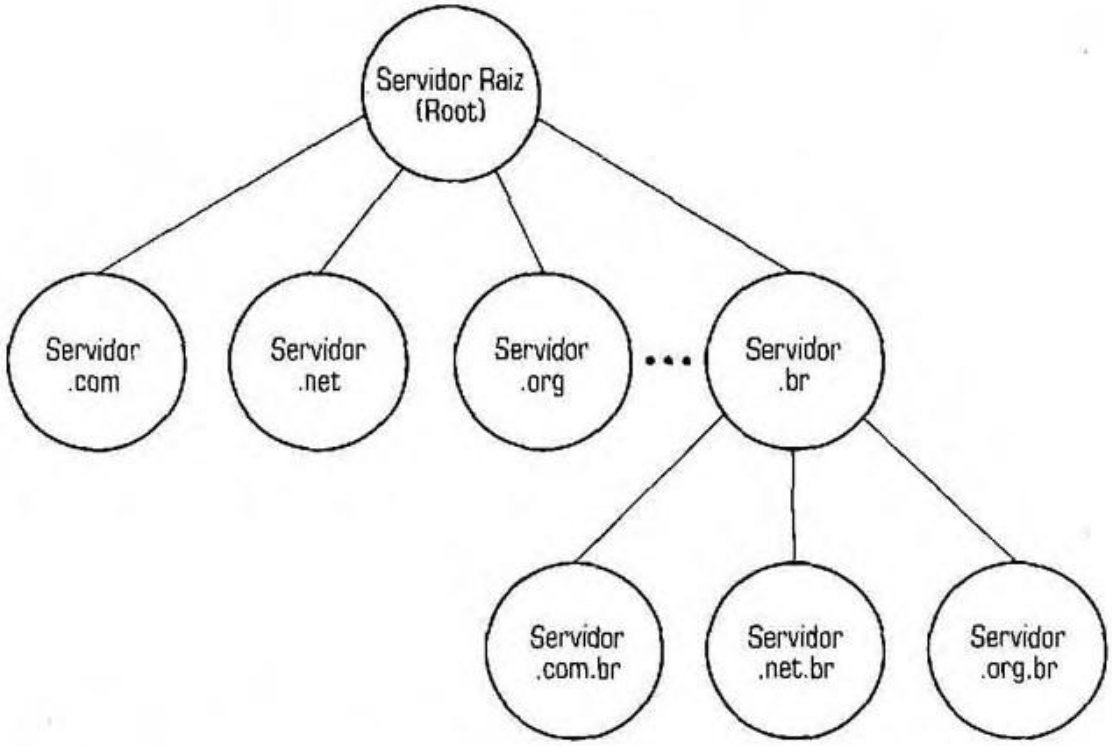
Como exemplo de uso desse serviço, temos os sites de internet, onde, para acessá-los, digitamos um endereço URL no lugar de um número IP. Ao digitar um endereço no browser e pedir para conectar, o browser se conecta com um servidor DNS que fará a conversão do nome do site para um endereço IP, permitindo a conexão. Os servidores **DNS** realizam 2 funções: converter endereços nominais em **IP** e vice-versa.

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP/IP –Protocolos e Serviços

DNS – Domain Name System

O sistema utilizado na Internet possui uma organização hierárquica:



Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

DNS – Domain Name System

O processo de pesquisa do endereço se inicialmente no servidor **DNS** local (Uma rede TCP deve ter ao menos 1 servidor **DNS**), caso este servidor não realize a **resolução** do nome, esse pedido é passado para o servidor **DNS** logo acima na hierarquia, e assim sucessivamente até localizar ou não o endereço IP.

Afim de diminuir o tráfego na rede, é que ao encontrar um endereço, os servidores mais abaixo na hierarquia armazenam esta informação em ***cache***, que tem um tempo de vida determinado, no sentido de não ficarem desatualizados.

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

DNS – Domain Name System

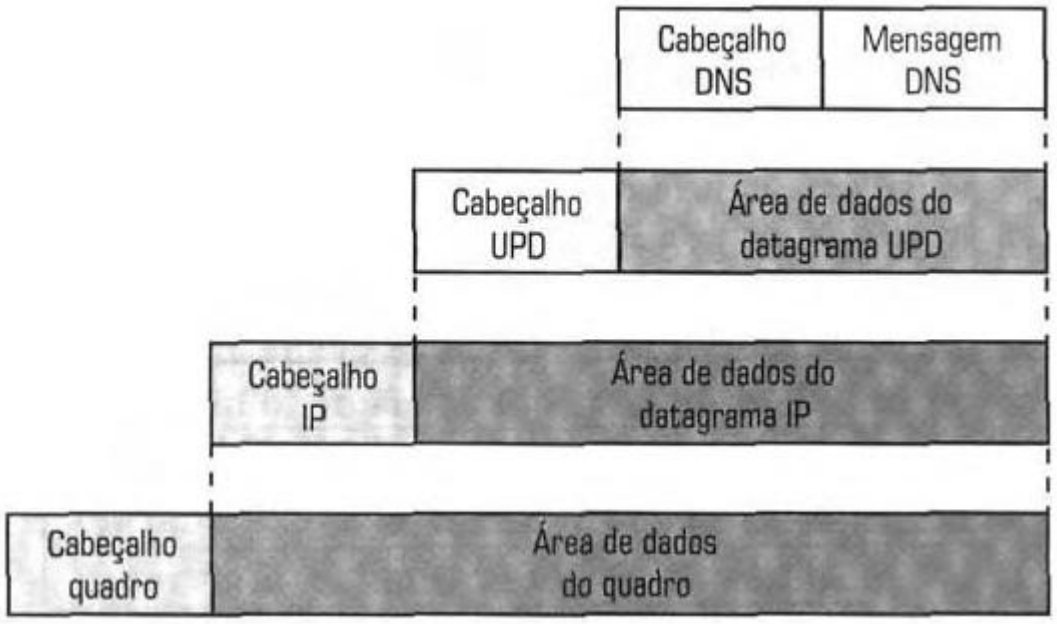
O processo de pesquisa do endereço se inicialmente no servidor **DNS** local (Uma rede TCP deve ter ao menos 1 servidor **DNS**), caso este servidor não realize a **resolução** do nome, esse pedido é passado para o servidor **DNS** logo acima na hierarquia, e assim sucessivamente até localizar ou não o endereço IP.

Afim de diminuir o tráfego na rede, é que ao encontrar um endereço, os servidores mais abaixo na hierarquia armazenam esta informação em ***cache***, que tem um tempo de vida determinado, no sentido de não ficarem desatualizados.

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

DNS – Formato da Mensagem

As mensagens **DNS** são trocadas tipicamente utilizando o protocolo de transporte **UDP**., Abaixo é mostrado o encapsulamento da mensagem:



Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP/IP –Protocolos e Serviços

DNS – Formato da Mensagem

- Identificação – 16 bits
- Parâmetro – 16 bits
- Nº de perguntas – 16 bits
- Nº de respostas – 16 bits
- Nº de autoridades – 16 bits
- Nº de informações– 16 bits
- Seção de perguntas
- Seção de respostas
- Seção de autoridades
- Seção de informações adicionais

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

DNS – Formato da Mensagem

Identificação
Identifica a mensagem **DNS.**

Parâmetros
Identificam o tipo da mensagem, conforme a Tabela a seguir:

Bit	Significado
0	Operação: 0: Pergunta; 1: Resposta
1 a 4	Tipo de Pergunta: 0: Padrão; 1: Reversa; 2: Complementar 1 (obsoleto); 3: Complementar 2 (obsoleto)
5	Resposta de autoridade
6	Mensagem Truncada
7	Recorrência desejada
8	Recorrência disponível
9 a 11	Reservado
12 a 15	Tipo de resposta: 0: Não houve erros; 1: Erro no formato da pergunta; 2: Falha no servidor; 3: Nome inexistente

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

DNS – Formato da Mensagem

Nº de perguntas
Informa o nº de perguntas no campo Seção de Perguntas**.**

Nº de Respostas
Idem para o campo de Respostas.

Nº de Autoridades
Idem para o campo de Autoridades.

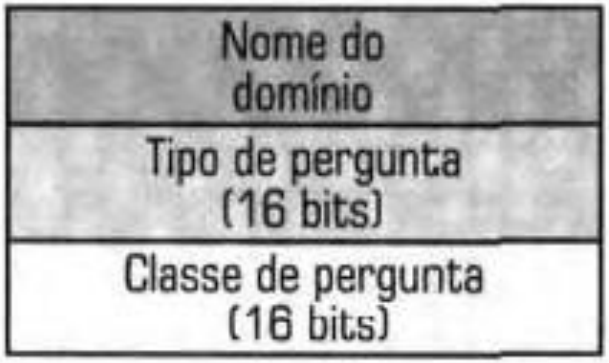
Nº de Informações Adicionais
Idem para o campo de Informações Adicionais.

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP/IP –Protocolos e Serviços

DNS – Formato da Mensagem

Seção Pergunta



Seção Resposta

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

DHCP - Dynamic Host Configuration Protocol

O **DHCP** é um protocolo de serviço TCP/IP que oferece configuração dinâmica de terminais, com concessão de endereços IP de host e outros parâmetros de configuração para clientes de rede.

Resumidamente, o **DHCP** opera da seguinte forma:

1. Um cliente envia um pacote **UDP** em *broadcast* (destinado a todas as máquinas) com um pedido **DHCP**
2. Os servidores **DHCP** que capturarem este pacote irão responder com um pacote com configurações onde constará, pelo menos, um endereço IP, uma máscara de rede e outros dados opcionais, como o gateway, servidores de DNS, etc.

O **DHCP** usa um modelo cliente-servidor, no qual o servidor **DHCP** mantém o gerenciamento centralizado dos endereços IP usados na rede.

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP/IP –Protocolos e Serviços

TELNET

Telnet é um protocolo cliente-servidor usado para permitir a comunicação entre computadores ligados numa rede (exemplos: rede local / LAN, Internet), baseado em TCP. Telnet é um protocolo de login remoto.

O protocolo **Telnet** também permite obter um acesso remoto a um computador. Este protocolo vem sendo gradualmente substituído pelo **SSH**, cujo conteúdo é criptografado antes de ser enviado. O uso do protocolo **Telnet** tem sido desaconselhado, a medida que os administradores de sistemas vão tendo maiores preocupações de segurança. Com o **Telnet** todas as comunicações entre o cliente e o servidor podem ser vistas, inclusive senhas, já que são somente texto aberto, permitindo assim que com o uso de "port-stealing" intercepte a conexão e seus pacotes, fazendo ***hijacking***.

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP/IP –Protocolos e Serviços

FTP – File Transfer Protocol

O **FTP** é um protocolo cliente-servidor usado para, como o próprio nome diz, transferência de arquivos. Os micros clientes necessitam de um programa para terem acesso a um servidor **FTP**, onde pode ser utilizada uma autenticação com usuário e senha. O FTP opera com vários comandos:

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP/IP –Protocolos e Serviços

FTP – File Transfer Protocol

O **FTP** é um protocolo cliente-servidor usado para, como o próprio nome diz, transferência de arquivos. Os micros clientes necessitam de um programa para terem acesso a um servidor **FTP**, onde pode ser utilizada uma autenticação com usuário e senha. O FTP opera com vários comandos:

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP/IP –Protocolos e Serviços

FTP – TFTP

O **FTP** possui uma variante mais simples: **TFTP – Trivial File Transfer Protocol**. Este protocolo é mais simples e rudimentar que o **FTP,** utilizados em tarefas que não exigem muita complexidade, utilizando o protocolo **UDP,** com mensagens de 512 byte, não confirmando o recebimento nem utilizando o conceito de janelas, ao contrário do **FTP** que é encapsulado pelo **TCP.**

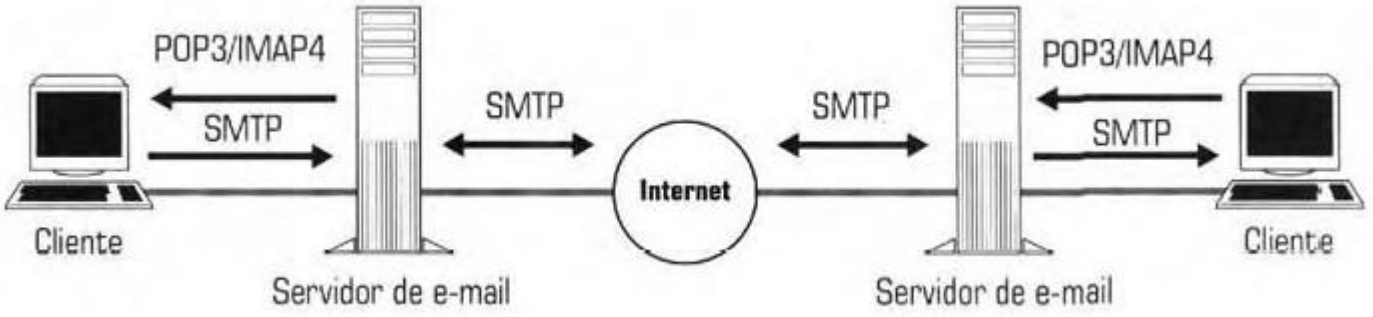
Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP/IP –Protocolos e Serviços

SMTP – Simple Mail Transfer Protocol

O **SMTP** é o protocolo padrão para envio de e-mails através da Internet. É um protocolo relativamente simples, baseado em texto simples, onde um ou vários destinatários de uma mensagem são especificados (e, na maioria dos casos, validados) sendo, depois, a mensagem transferida. Esse protocolo usa a porta **25** numa rede **TCP**.

O **SMTP** é um protocolo de envio apenas, o que significa que ele não permite que um usuário descarregue as mensagens de um servidor. Para isso, é necessário um cliente de email com suporte ao protocolo **POP3** ou **IMAP**, que é o caso da maioria dos clientes atuais.



Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP/IP –Protocolos e Serviços

POP3 e IMAP

O **Post Office Protocol** (**POP3**) é um protocolo utilizado no acesso remoto a uma caixa de correio eletrônico, permitindo que todas as mensagens contidas numa caixa de correio eletrônico possam ser transferidas seqüencialmente para um computador local. Aí, o utilizador pode ler as mensagens recebidas, apagá-las, responder-lhes, armazená-las, etc.

O funcionamento do protocolo **POP3** diz-se ***off-line***, uma vez que o processo suportado se baseia nas seguintes etapas:

1. É estabelecida uma ligação **TCP** entre a aplicação cliente de e-mail (***User Agent - UA***) e o servidor onde está a caixa de correio (***Message Transfer Agent - MTA***)
2. O utilizador autentica-se;
3. Todas as mensagens existentes na caixa de correio são transferidas seqüencialmente para o computador local;
4. As mensagens são apagadas da caixa de correio (opcionalmente, o protocolo pode ser configurado para que as mensagens não sejam apagadas da caixa de correio; **se esta opção não for utilizada, deve-se utilizar sempre o mesmo computador para ler o correio eletrônico, para poder manter um arquivo das mensagens**);
5. A ligação com o servidor é terminada;
6. O utilizador pode agora ler e processar as suas mensagens (***off-line***).

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP/IP –Protocolos e Serviços

POP3 e IMAP

A característica off-line do protocolo **POP3** é particularmente útil para utilizadores que se ligam à Internet através de redes públicas comutadas, em que o custo da ligação é proporcional ao tempo de ligação (ex: a rede telefônica convencional ou a rede **RDIS**). Com o **POP3**, a ligação apenas precisa de estar ativa durante a transferência das mensagens, e a leitura e processamento das mensagens pode depois ser efetuada com a ligação inativa.

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP/IP –Protocolos e Serviços

POP3 e IMAP

IMAP (***Internet Message Access Protocol***) é um protocolo de gerenciamento de correio eletrônico superior em recursos ao **POP3** - protocolo que a maioria dos provedores oferece aos seus assinantes. A última versão é o **IMAP4**. O mais interessante é que as mensagens ficam armazenadas no servidor e o internauta pode ter acesso a suas pastas e mensagens em qualquer computador, tanto por **webmail** como por cliente de correio eletrônico (como o Mozilla Thunderbird, Outlook Express ou o Evolution).

Outra vantagem deste protocolo é o compartilhamento de caixas postais entre usuários membros de um grupo de trabalho. Além disso, é possível efetuar pesquisas por mensagens diretamente no servidor, utilizando palavras-chaves.
Tem, no entanto, alguns inconvenientes:
O número de mensagens possível de se armazenar depende do espaço limite que nos é atribuído para a caixa de correio;

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP/IP –Protocolos e Serviços

POP3 e IMAP

Caso o servidor **IMAP** esteja numa localização remota, pela Internet, e não numa rede local **LAN**, é necessário estar ligado à Internet todo o tempo que quisermos consultar ou enviar mensagens, podendo não ser adequado a quem utiliza a Internet através de ligação telefônica **Dial-up**, devido aos custos associados.

No entanto, a maioria dos clientes de e-mail oferecem a possibilidade de criar uma cópia local (offline) das mensagens contidas em uma ou várias pastas (e.g. Inbox (Recebidas), Sent (Enviadas), etc.). Sendo assim, toda vez que você dispuser de uma conexão (estiver online) sua cópia local será sincronizada com o servidor de e-mail. Existem também algumas outras vantagens, como por exemplo: Ativar e desativar "flags" (marcações que indicam características de uma mensagem), que podem, inclusive, ser definidas pelo usuário. Com o **POP3**, estas marcações são registradas pelo cliente, de forma que, se a mensagem for aberta por um segundo cliente, as mesmas podem não ter seu "status" indicado corretamente. O **IMAP** permite a gravação das "flags" junto às caixas-postais, assegurando que, independente de qual cliente se acesse, as mensagens terão as mesmas corretamente atribuídas.

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP/IP –Protocolos e Serviços

HTTP - Hypertext Transfer Protocol

O **HTTP** é um protocolo de aplicação responsável pelo tratamento de pedidos e respostas entre cliente e servidor na **World Wide Web**. Ele surgiu da necessidade de distribuir informações pela Internet e para que essa distribuição fosse possível foi necessário criar uma forma padronizada de comunicação entre os clientes e os servidores da Web e entendida por todos os computadores ligados à Internet. Com isso, o protocolo **HTTP** passou a ser utilizado para a comunicação entre computadores na Internet e a especificar como seriam realizadas as transações entre clientes e servidores, através do uso de regras básicas.

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP/IP –Protocolos e Serviços

HTTP - Funcionamento

Um sistema de comunicação em rede possui diversos protocolos que trabalham em conjunto para o fornecimento de serviços. Para que o protocolo **HTTP** consiga transferir seus dados pela Web, é necessário que os protocolos **TCP** e **IP** tornem possível a conexão entre clientes e servidores através de ***sockets*** **TCP/IP**.

O **HTTP** utiliza o modelo cliente-servidor, como a maioria dos protocolos de rede, baseando-se no paradigma de requisição e resposta. Um programa requisitante (cliente) estabelece uma conexão com um outro programa receptor (servidor) e envia-lhe uma requisição. O servidor responde. Após o envio da resposta pelo servidor, encerra-se a conexão estabelecida.

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

TCP/IP –Protocolos e Serviços

HTTP - Mensagem

O protocolo **HTTP** faz a comunicação entre o cliente e o servidor por meio de mensagens. O cliente envia uma mensagem de requisição de um recurso e o servidor envia uma mensagem de resposta ao cliente com a solicitação. Os dois tipos de mensagens existentes no protocolo utilizam um formato genérico para a transferência de entidades.

Uma mensagem, tanto de requisição quanto de resposta, é composta, conforme por uma linha inicial, nenhuma ou mais linhas de cabeçalhos, uma linha em branco obrigatória finalizando o cabeçalho e por fim o corpo da mensagem, opcional em determinados casos.

Fonte: Redes de Computadores – Curso Completo, Gabriel Torres.

Dados de Contato


79 9949 4098


pedro@pyxistec.com.br


psneto@emsergipe.com

pedro.pyxistec@gmail.com


http://www.facebook.com/pedro.neto.se


pedropyxis


http://lattes.cnpq.br/4891420246888248