Arquitetura TCP/IP

Por André Luís Santos de Aguiar

Índice

1. HISTÓRICO

A arquitetura TCP/IP surgiu com a criação de uma rede patrocinada pelo Departamento de Defesa do governo dos Estados Unidos da América (DoD - Department of Defense). Uma das tarefas essenciais dessa rede seria manter comunicados, mesmo que apenas uma parte, órgãos do governo e universidades, numa ocorrência de guerras ou catástrofes que afetassem os meios de comunicação daquele país. Dessa necessidade, surgiu a ARPANET, uma rede que permaneceria intacta caso um dos servidores perdesse a conexão.

A ARPANET necessitava então de um modelo de protocolos que assegurasse tal funcionalidade esperada, mostrando-se confiável, flexível e de fácil implementação. É então desenvolvida a arquitetura TCP/IP, que se torna um padrão de *fato*.

A ARPANET cresceu e tornou-se a ***rede mundial de computadores - internet***. A utilização (e facilidades) do padrão TCP/IP utilizado pelos fabricantes de outras redes, com a finalidade da conectividade com a internet. A normalização do TCP/IP chegou após a sua utilização em massa.
Hoje, quando se menciona TCP/IP, vem imediata a associação com a ***internet***, ocorrendo de modo idêntico o inverso: a ***internet*** está diretamente relacionada à arquitetura TCP/IP.

2. MODELO TCP/IP

O modelo TCP/IP é constituído basicamente por duas (02) camadas: a camada de rede e a camada de transporte. Tanto a camada de aplicação quanto a camada de interface de rede não possuem uma norma definida, devendo a camada de aplicação utilizar serviços da camada de transporte, a ser definida adiante, e a camada de interface de rede prover a interface dos diversos tipos de rede com o protocolo (promovendo em conseqüência a interoperação entre as diversas arquiteturas de rede — Ethernet, Token Ring, ATM,etc.

1. *Camada de Interface de Rede*

Também chamada camada de abstração de hardware, tem como função principal a interface do modelo TCP/IP com os diversos tipos de redes (X.25, ATM, FDDI, Ethernet, Token Ring, Frame Relay, sistema de conexão ponto-a-ponto SLIP,etc.). Como há uma grande variedade de tecnologias de rede, que utilizam diferentes velocidades, protocolos, meios transmissão, etc. , esta camada não é normatizada pelo modelo, o que provê uma das grandes virtudes do modelo TCP/IP: a possibilidade de interconexão e interoperação de redes heterogêneas.

2. *Camada de Rede (IP)*

A camada de rede é a primeira (normatizada) do modelo. Também conhecida como camada Internet, é responsável pelo endereçamento, roteamento dos *pacotes,* controle de envio e recepção (erros, bufferização, fragmentação, seqüência, reconhecimento, etc.), etc.
Dentre os protocolos da Camada de Rede, destaca-se inicialmente o IP (*Internet Protocol*), além do ARP, ICMP, RARP e dos protocolos de roteamento (RIP ,IGP, OSPF, Hello, EGP e GGP). Demais informações a respeito dos protocolos desta camada, serão descritas adiante.
A camada de rede é uma camada não orientada à conexão, portanto se comunica através de datagramas.

3. *Camada de Transporte*

A camada de transporte é uma camada fim-a-fim, isto é, uma entidade desta camada só se comunica com a sua entidade-par do host destinatário. É nesta camada que se faz o controle da conversação entre as aplicações intercomunicadas da rede.
A camada de transporte utiliza dois protocolos: o *TCP* e o *UDP*. O primeiro é orientado à conexão e o segundo é não orientado à conexão . Ambos os protocolos podem servir a mais de uma aplicação simultaneamente.
O acesso das aplicações à camada de transporte é feito através de *portas* que recebem um número inteiro para cada tipo de aplicação, podendo também tais portas serem criadas ao passo em que novas necessidades vão surgindo com o desenvolvimento de novas aplicações.
A maneira como a camada de transporte transmite dados das várias aplicações simultâneas é por intermédio da multiplexação, onde várias *mensagens* são repassadas para a camada de rede (especificamente ao protocolo IP) que se encarregará de empacotá-las e mandar para uma ou mais interface de rede. Chegando ao destinatário o protocolo IP repassa para a camada de transporte que demultiplexa para as portas (aplicações) específicas.
Quanto aos detalhes dos protocolos desta camada, serão descritos adiante.

4. *Camada de Aplicação*

É formada pelos protocolos utilizados pelas diversas aplicações do modelo TCP/IP. Esta camada não possui um padrão comum. O padrão estabelece-se para cada aplicação. Isto é, o FTP possui seu próprio protocolo, o TELNET possui o seu próprio, bem como o SNMP, GOPHER, DNS, etc.
É na camada de aplicação que se estabelece o tratamento das diferenças entre representação de formato de dados.
O endereçamento da aplicação na rede é provido através da utilização de portas para comunicação com a camada de transporte. Para cada aplicação existe uma porta predeterminada.
Demais informações sobre as aplicações serão descritas adiante em um tópico específico.

3. Endereçamento

O endereçamento de datagramas no modelo TCP/IP é implementado pela camada de rede (IP). Uma das informações de controle do datagrama é o endereço IP do destinatário e do emitente.

O endereço IP é formado por um número de 32 bits no formato *nnn.nnn.nnn.nnn* onde cada *nnn* pode variar de 0 até 255 (1 octeto = 8 bits). Os endereços possui uma classificação que varia de acordo com o número de sub-redes e de hosts. Tal classificação tem por finalidade otimizar o roteamento de mensagens na rede.

Os endereços são fornecidos por uma entidade central: NIC (Network Information Center), e devem ser únicos para cada estação (host).
Para o usuário dos serviços de rede, há uma forma mais simples de endereçamento. Através do DNS, são associados um nome a um endereço IP. O funcionamento do DNS será detalhado adiante no tópico 6-APLICAÇÕES.

1. Mapeamento dos Endereços

A única forma de comunicação entre duas máquinas é através do seu endereço físico. Como já visto, o modelo TCP/IP pode interligar redes heterogêneas, portanto não há uma padronização de endereços físicos que pudesse relacionar direta e unicamente uma máquina e seu endereço IP.
Para resolver estes problemas de mapeamento do endereço IP para o endereço físico da rede, é utilizado o protocolo ARP (*Address Resolution Protocol*) que encontra o endereço físico relacionado à um endereço IP fornecido. De igual forma, em se querendo um endereço IP a partir do endereço físico, utiliza-se o protocolo RARP (*Reverse Address Resolution Protocol*).
Há duas categorias de mapeamento. Quando o tamanho do endereço físico é menor ou igual ao tamanho do endereço IP (32 bits), pode-se fazer o endereço físico e o endereço IP iguais. De outra forma, quando o tamanho do endereço físico é maior que o do endereço IP (o endereço Ethernet, por exemplo, tem 48 bits) então é criada uma tabela de mapeamento.

Endereço IP	*Endereço Ethernet*
223.1.2.1	08-00-39-00-2F-C3
223.2.3.1	08-00-10-99-AC-54

Tabela de Mapeamento IP/Ethernet

4. Protocolos

1. Transporte

1. TCP (Transmission Control Protocol)

É o protocolo TCP que faz a comunicação fim-a-fim da rede. É orientado à conexão e altamente confiável independente da qualidade de serviços das sub-redes que servem de caminho. Para a confiabilidade de transmissão, garante a entrega das informações na seqüência em que lhe foi fornecida, sem perda nem duplicação.
Principais funções :

a. Transferência de dados — Através de mensagens de tamanho variável em full-duplex;
b. Transferência de dados urgentes — Informações de controle, por exemplo;
c. Estabelecimento e liberação de conexão — Antes e depois das transferências de dados, através de um mecanismo chamado *three-way-handshake*;
d. Multiplexação — As mensagens de cada aplicação simultânea são multiplexadas para repasse ao IP. Ao chegar ao destino, o TCP demultiplexa as mensagens para as aplicações destinatárias;
e. Segmentação — Quando o tamanho do pacote IP não suporta o tamanho do dado a ser transmitido, o TCP segmenta (mantendo a ordem) para posterior remontagem na máquina destinatária;
f. Controle do fluxo — Através de um sistema de buferização denominada *janela deslizante*, o TCP envia uma série de pacotes sem aguardar o reconhecimento de cada um deles. Na medida em que recebe o reconhecimento de cada bloco enviado, atualiza o buffer (caso reconhecimento positivo) ou reenvia (caso reconhecimento negativo ou não reconhecimento após um *timeout*);
g. Controle de erros — Além da numeração dos segmentos transmitidos, vai junto com o header uma soma verificadora dos dados transmitidos (*checksum*), assim o destinatário verifica a soma com o cálculo dos dados recebidos).
h. Precedência e segurança — Os níveis de segurança e precedência são utilizados para tratamento de dados durante a transmissão.

1. UDP (User Datagram Protocol)

O UDP é um protocolo mais rápido do que o TCP, pelo fato de não verificar o reconhecimento das mensagens enviadas. Por este mesmo motivo, não é confiável como o TCP.

O protocolo é não-orientado à conexão, e não provê muitas funções: não controla o fluxo podendo os datagramas chegarem fora de seqüência ou até mesmo não chegarem ao destinatário. Opcionalmente pode conter um campo *checksum*, sendo que os datagramas que não conferem este campo ao chegarem no destino, são descartados, cabendo à aplicação recuperá-lo.

1. ***Rede***
    0. **IP (Internet Protocol)**
       A função básica do protocolo IP é o transporte dos blocos de dados por entre as sub-redes até chegar ao destinatário. Durante o tráfego pelas sub-redes, existem componentes denominados *gateways,* que desvia o datagrama IP para outras sub-redes ou para o destinatário, se este fizer parte da sub-rede a que o gateway está conectado.
       Por limitação tecnológica, algumas sub-redes tem capacidade apenas para trafegar pacotes menores (volume de dados menor). Assim, o roteador fragmenta o datagrama original em datagramas menores, que serão restabelecidos futuramente quando possível.
    1. **ICMP (Internet Control Message Protocol)**

O protocolo ICMP é utilizado para transmissão de mensagens de controle ou de ocorrência de problemas. Utiliza o protocolo IP para a transporte das mensagens. Geralmente as mensagens ICMP são geradas pelos gateways, podendo também ser gerada pela estação destinatária.
No caso de problemas com datagramas enviados pela estação de origem, o ICMP inclui no seu datagrama de ocorrências, o cabeçalho além de 64 bits iniciais dos dados do datagrama IP que originou o erro.
As ocorrências do ICMP podem ser:

a.Destinatário inacessível;
b.Ajuste de fonte — Solicita à estação a redução da taxa de emissão de datagramas;
c.Redireção — Rota mais adequada para a estação destinatária (para atualização da tabela de endereço dos roteadores;
d.Eco e Resposta de Eco;
e.Tempo excedido;
f.Problemas de parâmetros;
g.Marca de Tempo e Resposta à Marca de Tempo;
h.Solicitação de informações e Respostas de Informações;
i.Solicitação de Máscara de endereço e Resposta à Mascara de Endereço.

    1. **ARP (Address Resolution Protocol)**
       São utilizados para o mapeamento dinâmico do endereço IP. Quando inicializadas, as estações não possuem uma tabela de endereços IP/físico armazenada. Em vez disso, para cada endereço IP que não esteja na tabela da estação, o protocolo ARP manda uma solicitação via broadcast do endereço físico para o endereço IP determinado. O destinatário que tiver o endereço IP informado responde (à máquina solicitante) seu endereço físico. Nessa ocasião, tanto a tabela da máquina origem quanto a da máquina destinatária são atualizadas com os endereços.
    2. **RARP (Reverse Address Resolution Protocol)**

De forma inversa ao ARP, o RARP procura um endereço IP relacionado a um endereço físico determinado. Geralmente quem mais utiliza tal protocolo são as estações de rede *diskless* que possuem apenas o endereço físico, durante o processo de inicialização.
Para que o RARP funcione, é necessário ao menos um servidor RARP , que possui informações de mapeamento de todas as estações da rede.
Da mesma forma que o ARP, o RARP envia uma mensagem broadcast solicitando o endereço IP. São pesquisados nas tabelas dos servidores o endereço solicitado, sendo então devolvida uma mensagem RARP contento a informação solicitada.
Caso haja mais de um servidor RARP, um deles é determinado como prioritário, onde será feita a primeira pesquisa. Se dentro de um intervalo de tempo não houver respostas, outros servidores iniciarão a pesquisa.

5. Roteamento

É o processo de escolha do caminho pelo qual o pacote deve chegar à estação destinatária. O roteamento pode ser direto ou indireto.

1. ***Roteamento Direto***
   O roteamento direto ocorre quando a estação destinatária do datagrama está na mesma sub-rede física da estação origem. A checagem é feita comparando o endereço IP do emissor e do

destinatário constantes no datagrama IP. Nesse caso o conteúdo do datagrama recebe o endereço físico da estação e é enviado diretamente pela mesma sub-rede.

2. *Roteamento Indireto*

No caso do roteamento indireto, o emissor deve enviar para o gateway o datagrama com o endereço IP do destinatário. O gateway verificará se o destinatário pertence a uma das sub-redes a ele conectadas, e em caso positivo envia o pacote diretamente para a estação. Caso o gateway não localize o destinatário como um membro de uma das sub-redes a ele conectadas, ele envia o pacote para outro gateway (de acordo com sua tabela de roteamento), que verificará o mesmo, e assim por diante até encontrar o destinatário ou terminar o tempo de vida do pacote.

3. *Algorítmos de Roteamento*

São a forma como os gateways localizam as diversas redes e estações. Podem ser:

a. Roteamento Vector-Distance;

b. Roteamento Link-State (shortest path first)

1. *Protocolos de Roteamento*

Os protocolos de roteamento padronizam a forma como os gateways trocam informações necessárias à execução dos algorítmos de roteamento.

0. EGP (Exterior Gateway Protocol)

Não está vinculado a nenhum algoritmo de roteamento, isto significa que os gateways que se comunicam não necessitam rodar o mesmo algoritmo. Define as informações a serem trocadas entre Gateways Exteriores.

É elaborado para uma rede de sistemas autônomos numa topologia em árvore.

As mensagens são associadas a cada sistema autônomo através de uma identificação no header da mensagem do EGP. Estas mensagens só trafegam em gateways vizinhos.

Dois gateways tornam-se vizinhos quando trocam mensagens de *Aquisição de Vizinho*. Após isso, verificam o estado do vizinho através da mensagem de *Disponibilidade* e através da mensagem *Alcance* identificam quais redes podem ser acessadas a partir do vizinho.

1. RIP (Routing Information Protocol)

Desenvolvido na Universidade de Berkeley - California, permite a troca de informações com o algoritmo *Vector-Distance* em uma sub-rede dotada de difusão de mensagens.

Um gateway executando RIP no modo ativo envia informações a cada 30 segundos ou quando solicitado. As mensagens contém informações de todas as tabela de roteamento do gateway. Estas informações são: O endereço IP da sub-rede e a distância do gateway (quantidade de gateways). As estações e gateways que recebem as mensagens atualizam sua tabela de acordo com o algoritmo vector-distance.

2. OSPF

Foi desenvolvido por um grupo de trabalho da Internet Engineering Task Force, para roteamento de grandes redes.

Utiliza o algoritmo de roteamento SPF e possui várias vantagens:

a. Roteamento de acordo com o tipo de serviço;

b. Balanceamento de carga entre rotas do mesmo tamanho;

c. Definição de rotas específicas para máquinas e redes;

d. Modularização do SA, através da criação de áreas que contém gateways e redes. A topologia de tais áreas são conhecidas apenas nesta área.

e. Definição de uma topologia de rede virtual que abstraia detalhes da rede real;

f. Divulgação de mensagens recebidas de Gateways Exteriores.

Quando gateways OSPF são inicializados, eles verificam junto com os gateways vizinhos, quem será o **gateway mestre**. O Gateway mestra será encarregado da notificação de informações de roteamento para todos os gateways da sub-rede. Como apenas o gateway mestre envia informações, o trafego é reduzido consideravelmente.

6. Aplicações

As aplicações, no modelo TCP/IP, não possuem uma padronização comum. Cada uma possui um RFC próprio.

O endereçamento das aplicações é feito através de portas (chamadas padronizadas a serviços dos protocolos TCP e UDP), por onde são passados as mensagens.

Como já mencionado, é na camada de Aplicação que se trata a compatibilidade entre os diversos formatos representados pelos variados tipos de estações da rede.
A comunicação entre as máquinas da rede é possibilitada através de primitivas de acesso das camadas UDP e TCP. Antes de iniciar o estabelecimento da conexão, são executadas as primitivas **socket,** que cria um ponto terminal de comunicação, e **bind** que registra o endereço da aplicação (número da porta). Para estabelecer a conexão (com o protocolo TCP), a aplicação servidora executa a primitiva **listen** enquanto que a cliente executa **connect**. A aplicação servidora usa o **accept** para receber e estabelecer a conexão. Já o UDP, como não é orientado à conexão, logo após o **socket** e o **bind**, utiliza as primitivas **sendto** e **recvfrom.**

1. ***TELNET (Terminal Virtual)***
   É um protocolo que permite a operação em um sistema remoto através de uma sessão de terminal. Com isso, a aplicação servidora recebe as teclas acionadas no terminal remoto como se fosse local. Utiliza a porta **23** do TCP.
   O TELNET oferece três serviços: Definição de um terminal virtual de rede, Negociação de opções (modo de operação, eco, etc.) e Transferência de dados.
2. ***FTP (File Transfer Protocol)***
   Provê serviços de transferencia, renomeação e eliminação de arquivos, além da criação, modificação e exclusão de diretórios. Para sua operação, são mantidas duas conexões: uma de dados e outra de controle. Não implementa segurança, o que deixa para o TCP, exceto as requisições de senhas de acesso a determinados arquivos (ou servidores FTP).
   As transferências de arquivos podem ser no modo TEXTO, onde há conversões de codificação para o sistema destinatário, e o modo BINÁRIO, onde não há nenhuma conversão e todos os bytes são transferidos como estão.
3. ***SNMP (Simple Network Management Protocol)***
   É utilizado para trafegar as informações de controle da rede. De acordo com o sistema de gerenciamento da arquitetura TCP/IP, existem o **agente** e o **gerente** que coletam e processam, respectivamente, dados sobre erros, problemas, violação de protocolos, dentre outros.
   Na rede existe uma base de dados denominada MIB (Management Information Base) onde são guardadas informações sobre hosts, gateways, interfaces individuais de rede, tradução de endereços, e softwares relativos ao IP, ICMP, TCP, UDP, etc. Através do SNMP pode-se acessar os valores dessas variáveis, receber informações sobre problemas na rede, armazenar valores, todos através da base do MIB.
4. ***DSN (Domain Name System)***
   O DNS é um mecanismo para gerenciamento de domínios em forma de árvore. Tudo começa com a padronização da nomenclatura onde cada nó da arvore é separado no nome por pontos. No nível mais alto podemos ter: COM para organizações comerciais, EDU para instituições educacionais, GOV para instituições governamentais, MIL para grupos militares, ORG para outras organizações.
   O DSN possui um algoritmo confiável e eficiente para tradução de mapeamento de nomes e endereços
5. ***SMTP (Simple Mail Tansfer Protocol)***
   Implementa o sistema de correio eletrônico da internet, operando não orientado à conexão, provê serviços de envio e recepção de mensagens do usuário. Tais mensagens são armazenadas num servidor de correio eletrônico onde o usuário destinatário está cadastrado, até que este solicite-a, quando são apagadas da área de transferência do sistema originador.
   O SMTP divide a mensagem em duas partes: corpo e cabeçalho que são separados por uma linha em branco. No cabeçalho existem uma seqüência de linhas que identificam o emissor, o destinatário, o assunto, e algumas outras informações opcionais.
6. ***RPC (Remote Procedure Call)***
   Implementa mecanismos de procedimentos de chamada remota, úteis no desenvolvimento de aplicações cliente-servidor com um nível maior de abstração.
   Um aplicação utiliza o RPC para fazer interface das suas funções. Assim as funções chamadas pelas aplicações são repassadas ao RPC que monta uma mensagens correspondente e envia para processamento remoto. O servidor, então processa as mensagens, executa a rotina e devolve os resultados para o RPC da estação, que reestrutura os dados e repassa à aplicação. Tudo isso implementa uma função virtualmente local, transparente para a aplicação.
7. ***NFS (Network File System)***

O NFS supre uma deficiência do FTP que não efetua acesso on-line aos arquivos da rede. Desenvolvido pela SUN Microsystems, tem acesso através da porta 2049 do UDP.
O NSF cria uma extensão do sistema de arquivos local, transparente para o usuário, e possibilita várias funções como as seguintes:

a. Criação e modificação de atributos dos arquivos;
b. Criação, leitura, gravação, renomeação e eliminação de arquivos;
c. Criação, leitura e eliminação de diretórios;
d. Pesquisa de arquivos em diretórios;
e. Leitura dos atributos do sistema de arquivos.

Um dos problemas do NFS é que não suporta acesso compartilhado aos arquivos, portanto tais preocupações devem estar a cargo da aplicação.
O NFS utiliza o UDP, portanto tem embutidas várias rotinas de segurança para suprir a deficiência do protocolo.

7. Bibliografia

- Arquiteturas de Redes de Computadores OSI e TCP/IP - BRISA - Organização e coordenação Tereza Cristina Melo de Brito Carvalho - Makron Books - 1994
- Computer Networks 3rd Edition - Andrew S Tanenbaun
- RFC1180
- Comunicação de Dados - Luiz Alves - Makron Books, 1994