PROTOCOLOS TCP/IP

Resumo

O objetivo deste trabalho é divulgar as principais características do conjunto de protocolos denominados por TCP/IP. O trabalho envolve os itens: abordagem histórica, comparação entre os modelos de camada TCP/IP e o de referência ISO/OSI, breve introdução ao endereçamento IP, suas classes, subredes e finalmente a descrição dos principais protocolos e suas aplicações.

Gostaria de agradecer aos futuros engenheiros, porém já profissionais, Carlil Gibran Fonseca de Macedo e Nilton Costa Braga pelas longas discussões, fundamentais para a melhor compreensão do tema, e pela revisão final do texto.

Índice

1. HISTÓRICO 3

2. MODELO DE REFERÊNCIA ISO/OSI 4

3. MODELO TCP/IP 6

4. ENDEREÇAMENTO IP E CLASSES 7

5. SUBREDES 8

5.1. MÁSCARA DE SUBREDES 9

6. PROTOCOLOS E APLICAÇÕES 10

6.1. PROTOCOLO INTERNET - IP 10
6.2. ADDRESS RESOLUTION PROTOCOL - ARP 12
6.3. INTERNET CONTROL MESSAGE PROTOCOL - ICMP 13
6.4. TRANSMISSION CONTROL PROTOCOL - TCP 14
6.5. USER DATAGRAM PROTOCOL - UDP 14
6.6. PROTOCOLOS DA CAMADA DE APLICAÇÃO 15
6.6.1. File Transfer Protocol - FTP 15
6.6.2. Trivial File Transfer Protocol - TFTP 16
6.6.3. Telnet 16
6.6.4. Simple Network Management Protocol - SNMP 16
6.7. OUTROS PROTOCOLOS E APLICAÇÕES 17

7. CONCLUSÃO 17

REFERÊNCIAS 19

1. Histórico

Nos anos 60, o principal setor estratégico americano, *Department of Defense* – DoD se interessou em um protocolo que estava sendo desenvolvido/utilizado pelas universidades para interligação dos seus sistemas computacionais e que utilizava a tecnologia de chaveamento de pacotes. O interesse do DoD estava no desejo de manter a comunicação entre os diversos sistemas espalhados pelo mundo, no caso de um desastre nuclear. O problema maior estava na compatibilidade entre os sistemas computacionais de diferentes fabricantes que possuíam diferentes sistemas operacionais, topologias e protocolos. A integração e compartilhamento dos dados passou a ser um problema de difícil resolução.

Foi atribuído assim à *Advanced Research Projects Agency* – ARPA a tarefa de encontrar uma solução para este problema de tratar com diferentes equipamentos e diferentes características computacionais. Foi feita então uma aliança entre universidades e fabricantes para o desenvolvimento de padrões de comunicação. Esta aliança especificou e construiu uma rede de teste de quatro nós, chamada ARPANET, e que acabou sendo a origem da Internet hoje.

No final dos anos 70, esta rede inicial evoluiu, teve seu protocolo principal desenvolvido e transformado na base para o TCP/IP (*Transmition Control Protocol / Internet Protocol*). A aceitação mundial do conjunto de protocolos TCP/IP deveu-se principalmente a versão UNIX de Berkeley que além de incluir estes protocolos, colocava-os em uma situação de domínio público, onde qualquer organização, através de sua equipe técnica poderia modificá-los e assim garantir seu desenvolvimento.

Dentre as várias organizações e comitês que participaram deste desenvolvimento e divulgação, podemos destacar *Internet Engineering Task Force* – IETF (http://www.ietf.org) cuja principal função atual é a manutenção e apoio aos padrões da Internet e TCP/IP principalmente através da série de documentos *Request for Comments* - RFC. Estes documentos descrevem as diversas tecnologias envolvidas e servem de base para as novas tecnologias que deverão manter a compatibilidade com as anteriores dentro do possível.

Em resumo, o maior trunfo do TCP/IP é o fato destes protocolos apresentarem a interoperabilidade de comunicação entre todos os tipos de hardware e todos os tipos de sistemas operacionais. Sendo assim, o impacto positivo da comunicação computacional aumenta com o número de tipos computadores que participam da grande rede Internet.

2. Modelo de Referência ISO/OSI

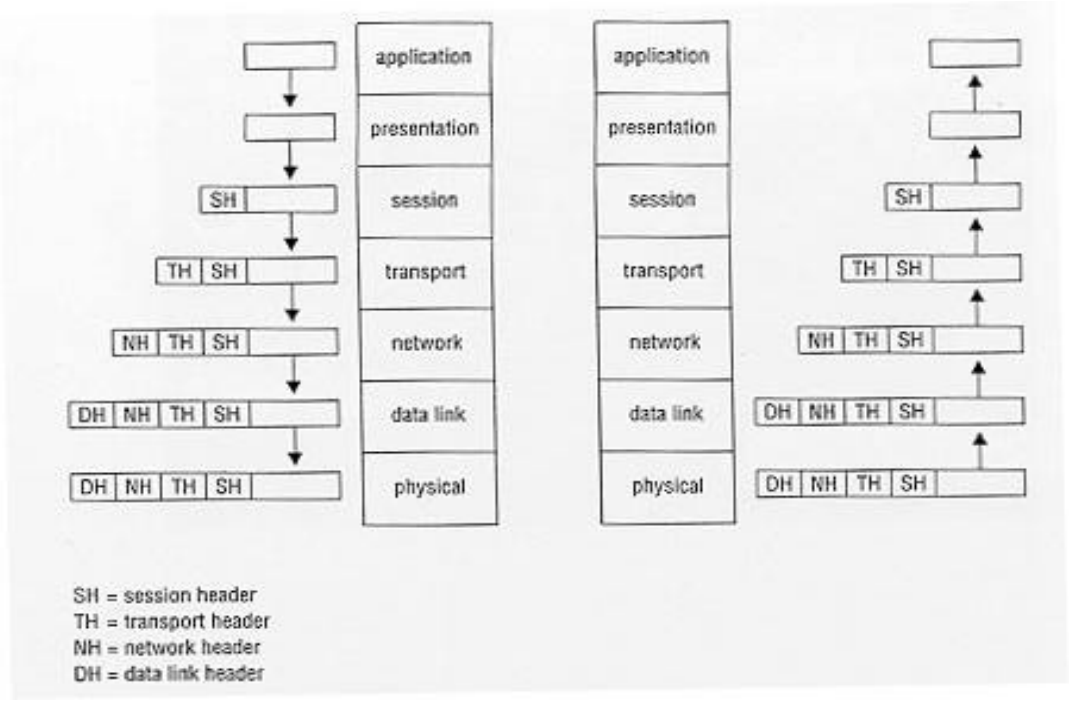
Dentro deste cenário de grande variedade de sistemas operacionais, CPUs, interfaces de rede, tecnologias e várias outras variáveis, e a necessidade de interconexão entre os diversos sistemas computacionais, em 1977, a *International Organization for Standardization* – ISO, criou um sub-comitê para o desenvolvimento de padrões de comunicação para promover a interoperabilidade entre as diversas plataformas. Foi então desenvolvido o modelo de referência *Open Systems Interconnection* – OSI.

É importante observar que o modelo OSI é simplesmente um modelo que especifica as funções a serem implementadas pelos diversos fabricantes em suas redes. Este modelo não detalha como estas funções devem ser implementadas, deixando isto para que cada empresa/organização tenha liberdade para desenvolver.

O comitê ISO assumiu o método “dividir para conquistar”, dividindo o processo complexo de comunicação em pequenas sub-tarefas (camadas), de maneira que os problemas passem a ser mais fáceis de tratar e as sub-tarefas melhor otimizadas. O modelo ISO/OSI é constituído por sete camadas, descritas sucintamente a seguir de cima para baixo:

7	Aplicação	Esta camada funciona como uma interface de ligação entre os processos de comunicação de rede e as aplicações utilizadas pelo usuário.
6	Apresentação	Aqui os dados são convertidos e garantidos em um formato universal.
5	Sessão	Estabelece e encerra os enlaces de comunicação.
4	Transporte	Efetua os processos de sequenciamento e, em alguns casos, confirmação de recebimento dos pacotes de dados.
3	Rede	O roteamento dos dados através da rede é implementado aqui.
2	Enlace	Aqui a informação é formatada em quadros (*frames*). Um quadro representa a exata estrutura dos dados fisicamente transmitidos através do fio ou outro meio.
1	Física	Define a conexão física entre o sistema computacional e a rede. Especifica o conector, a pinagem, níveis de tensão, dimensões físicas, características mecânicas e elétricas, etc.

Cada camada se comunica com sua semelhante em outro computador. Quando a informação é passada de uma camada para outra inferior, um cabeçalho é adicionado aos dados para indicar de onde a informação vem e para onde vai. O bloco de cabeçalho+dados de uma camada é o dado da próxima camada. Observe a figura abaixo que esquematiza isto.



A unidade de informação muda de nome ao longo das camadas de maneira que podemos saber sobre qual camada se está referindo pelo nome destas unidades. A tabela abaixo relaciona os diversos nomes destas unidades de informação ao longo das camadas:

7	Aplicação	Mensagem
4	Transporte	Segmento
3	Rede	Datagrama
2	Enlace	Quadro/*Frame*
1	Física	Bit

Antes do desenvolvimento do modelo de camadas ISO/OSI, o DoD definiu seu próprio modelo de rede conhecido como modelo DoD de rede ou também modelo Internet de rede. Posteriormente este modelo passou a ser conhecido como modelo de camadas TCP/IP, que será descrito a seguir.

3. Modelo TCP/IP

O modelo de camadas ISO/OSI acabou se tornando apenas uma base para praticamente todos os protocolos desenvolvidos pela indústria. Cada desenvolvedor tem uma arquitetura que difere em detalhes as vezes fundamentais no seu desenvolvimento. Sendo assim, é de se esperar uma variação nas descrições do conjunto de protocolos TCP/IP. Apresentaremos a seguir a comparação entre duas possíveis interpretações, esquerda e direita do modelo base ISO/OSI ao centro:

Na figura acima, vemos que a tabela da esquerda apresenta os principais protocolos distribuídos pelas diversas camadas, enquanto que na tabela da direita as funções são o destaque.

Na tabela da esquerda vemos que o TCP/IP não faz distinção entre as camadas superiores. As três camadas superiores são estritamente equivalentes aos protocolos de processos da Internet. Os processos possuem o nome do próprio protocolo utilizado porém é importante não confundir o protocolo em si com a aplicação que geralmente apresenta uma interface com usuário amigável para utilização do protocolo.

No modelo ISO/OSI, a camada de transporte (4) é responsável pela liberação dos dados para o destino. No modelo Internet (TCP/IP) isto é feito pelos protocolos "ponto a ponto" TCP e UDP que serão descritos posteriormente.

Por fim, o protocolo IP é o responsável pela conexão entre os sistemas que estão se comunicando. Basicamente este protocolo se relaciona com a camada de rede (3) do modelo ISO/OSI. Este protocolo é o responsável principal do movimento da informação na rede. É nesta camada/protocolo que a informação é fragmentada no sistema fonte e reagrupada no sistema alvo. Cada um destes fragmentos podem ter caminhos diferentes pela rede de forma que os fragmentos podem chegar fora de ordem. Se, por exemplo, o

fragmento posterior chegar antes do anterior, o protocolo IP no sistema destino reagrupa os pacotes na seqüência correta.

Na tabela de direita consideramos o TCP/IP como sendo constituído por 4 camadas apenas. A camada superior, camada de aplicação/processo é responsável por permitir que aplicações possam se comunicar através de hardware e software de diferentes sistemas operacionais e plataformas. Muitas vezes este processo é chamado de cliente-servidor. A aplicação cliente em geral está em um equipamento mais simples e com uma boa interface com usuário. Esta aplicação envia requisições à aplicação servidor que normalmente está em uma plataforma mais robusta e que tem capacidade para atender várias requisições diferentes de clientes diferentes.

A camada que segue, camada de Transporte ou “Ponto a Ponto”, tem a função principal de começar e terminar uma conexão e ainda controlar o fluxo de dados e de efetuar processos de correção e verificação de erros.

A camada de rede é a responsável pelo roteamento. Comparativamente ela corresponde no modelo ISO/OSI a camada de Rede (3) e parte da camada Enlace (2). Esta camada é usada para atribuir endereço de rede (IP) ao sistema e rotear a informação para a rede correta. Tem ainda a função de ligação entre as camadas superiores e os protocolos de hardware. Em essência podemos afirmar que sem esta camada, as aplicações teriam que ser desenvolvidas para cada tipo de arquitetura de rede como por exemplo Ethernet ou Token Ring.

A primeira camada, camada Física, não é definida pelo TCP/IP, porém é nítida sua importância em relação à parte física da mídia de comunicação, de bits, de quadros, de endereços MAC, etc.

4. Endereçamento IP e Classes

Como visto anteriormente, a camada do protocolo IP ou protocolo Internet, define um endereço de identificação único e através deste endereço executa serviços de roteamento que basicamente definem o caminho disponível naquele momento para comunicação entre a fonte e o destino.

O protocolo Internet (IP) necessita da atribuição de um endereço Internet (endereço IP) organizado em 4 octetos (bytes). Estes octetos definem um único endereço dividido em uma parte que representa a rede a qual pertence o endereço, em alguns casos a subrede também, e por fim a representação particular daquele sistema na rede.

Alguns endereços possuem significado especial:

- Endereço 0: Significa a própria rede ou sistema. O endereço 0.0.0.35 referencia a estação 35 da rede local. O endereço 127.0.0.0 referencia a estação em análise. O endereço

152.84.40.0 referencia a subrede 40 inteira da rede local do CBPF que pode ser representada por 152.84.0.0.

?? Endereço 127: É conhecido como *loopback* e é utilizado em processos de diagnose. O endereço 127.0.0.1 é o próprio *loopback* da estação em análise.

?? Endereço 255: Este endereço é muito utilizado em mensagens *broadcast* e serviços de anúncio generalizados. Uma mensagem enviada para o endereço 152.84.255.255 irá atingir todos os 255 sistemas de cada uma das 255 subredes da rede local do CBPF.

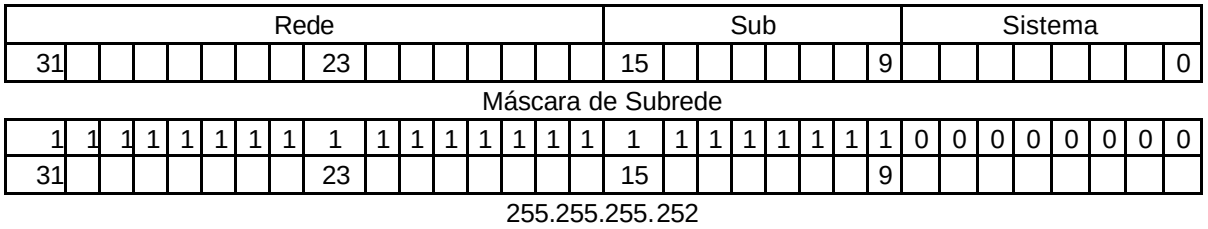
A tabela a seguir relaciona os diversos aspectos relevantes na definição do endereço Internet: o número de sistemas possíveis, os primeiros bits do primeiro octeto e os seus possíveis valores. Os demais octetos podem assumir livremente os valores entre 0 e 255, sempre levando em conta aqueles de significado especial.

Classe	2n	Hosts	Bits Iniciais	Primeiro Octeto
A	24	167.772	0xxx	0-127
B	16	65.536	10xx	128-191
C	8	256	110x	192-223
D	-	-	1110	224-239
E	-	-	1111	240-255

Os endereços **Classe A** são usados para redes muito grandes normalmente ligada a funções educacionais e científicas. Os endereços **Classe B** são usados em redes muito grandes, normalmente atribuídas a instituições que possuíam um perfil disseminador de tecnologia e assim pudessem de alguma forma distribuir suas redes entre instituições e empresas contribuindo assim para o desenvolvimento de uma grande rede mundial. Os endereços **Classe C** são os mais difundidos pois permitem redes de 256 IP's o que parece ser um número conveniente para gerenciamento e implantação de sistemas de informação. Os endereços **Classe D** são reservados para *Multicast* utilizado nas aplicações de Videoconferência, Multimídia, dentre outras, e por fim, os endereços **Classe E** são reservados para experimentação e desenvolvimento.

5. Subredes

A criação de subredes a partir de uma rede primária é um procedimento típico na área de redes. O objetivo desta segmentação é permitir uma melhor performance da rede em termos organizacionais, estruturais e funcionais.



A idéia básica é acrescentar alguns bits à identificador de rede do endereço Internet. Os endereços permitidos são aqueles formados pelos bits restantes do octeto. Veja figura anterior.

5.1. Máscara de Subredes

Conforme descrito na figura anterior, o identificador de redes e subredes, a máscara de subrede, também é composta por 4 octetos. A máscara é formada por bits 1 nos campos que caracterizam o endereço de rede, e bits 0 nos campos relativos ao *host*.

Considere uma Classe C com cada posição representada por um único bit de um endereço de 32bits:

R -> Rede H -> *Host*
RRRRRRRR.RRRRRRRR.RRRRRRRR.HHHHHHHH

Se esta Classe C for dividida em 8 subredes com 32-2(rede e broadcast)=30 hosts em cada uma delas, a máscara será 255.255.255.224 ou ainda /27 e sua representação fica:

RRRRRRRR.RRRRRRRR.RRRRRRRR.RRRHHHHH
11111111.11111111.11111111.11100000

Em um outro exemplo queremos fazer 64 subredes com 4-2=2 *hosts* permitidos por subrede. Neste caso a máscara seria 255.255.255.252 ou ainda /30 com a seguinte representação:

RRRRRRRR.RRRRRRRR.RRRRRRRR.RRRRRRHH
11111111.11111111.11111111.11111100

O mesmo raciocínio pode ser empregado em uma Classe B ou Classe A, mudando somente a relação entre bits 1 e bits 0, ou em outras palavras muda o octeto em análise. No caso de 2 subredes na Classe B teremos 255.255.128.0 ou /17 representadas por:

RRRRRRRR.RRRRRRRR.RHHHHHHH.HHHHHHHH
11111111.11111111.10000000.00000000

Vale ressaltar aqui uma operação simples implementada por todos algoritmos de roteamento que é o AND lógico entre a máscara de subrede e o

endereço do host. Se o endereço tiver os mesmos bits 1 da máscara então este endereço pertence a subrede em análise e portanto o pacote pode ser enviado através de *broadcast* na subrede. Se diferir, então o pacote deve ser enviado ao *gateway*, pois certamente pertence a outra subrede.

6. Protocolos e Aplicações

Neste capítulo abordaremos os principais protocolos que compõem o conjunto TCP/IP de protocolos. Alguns destes protocolos são confundidos pela própria aplicação que os utiliza. Sendo assim, adiante haverá uma seção de Protocolos de Aplicação.

6.1. Protocolo Internet - IP

O protocolo Internet é definido na camada 3 do modelo ISO/OSI. Esta camada é responsável pelo endereçamento dos pacotes de informação dos dispositivos origem e destino e possível roteamento entre as respectivas redes, se diferentes. Este roteamento é executado através do IP.

Como visto anteriormente, o endereço IP é composto de 4 octetos, que são divididos em parte rede e parte dispositivo, chamados de identificadores de rede e de *host*, de acordo com o tipo de classe definido pelos primeiros bytes do primeiro octeto, e/ou subrede, definida pelo número de máscara.

Este protocolo, usando a parte rede do endereço ou identificador de rede, pode definir a melhor rota através de uma tabela de roteamento mantida e atualizada pelos roteadores.

Este protocolo recebe os dados da camada superior (transporte) na forma de segmentos. Ocorre então o processo de fragmentação e os conjuntos de dados passam a se chamar datagramas. Estes datagramas são então codificados para envio à camada inferior (física) para encaminhamento no meio físico.

Na tabela abaixo relacionamos as diversas partes (9) constituintes de um datagrama, o número de bits e função ou descrição.

O primeiro campo, Cabeçalho, contém informação sobre a versão do número IP (ipv4 ou ipv6) e o tipo de serviço (ToS), muito usado em aplicações que necessitem de Qualidade de Serviço (QoS).

O segundo campo, Comprimento, informa o comprimento do datagrama incluindo dados e cabeçalho.

O terceiro campo, Fragmentação, instrui ao protocolo, como reagrupar datagramas quando chegam após um processo de fragmentação muito comum em interfaces defeituosas e tráfego intenso.

O quarto campo, *Time to Live* – TTL, informa o número de roteadores que podem redirecionar o datagrama. O valor é decrementado até zero a cada roteador quando então o datagrama é descartado, impedindo a criação de *loops* e assim garantindo estabilidade ao processo de roteamento.

	1	2	3	4	5	6	7	8	9
Bits	32	16	16	8	8	16	32	32	xxx
Descrição	Cabeçalho	Comprimento	Fragmentação	TTL	Protocolo TCP ou UDP	Verificação de Erros	Endereço Fonte	Endereço Destino	Dados

O quinto campo, informa qual protocolo deverá receber o datagrama na próxima camada. Se o valor deste campo for 6, TCP, se 7, UDP. Estes protocolos serão descritos posteriormente.

O sexto campo, Verificação de Erro, seleciona que processo será utilizado na detecção de erros: *Cyclical Redundance Check* – CRC ou *Frame Check Sequence* – FCS.

Os próximos campos, sétimo e oitavo, Endereço Fonte e Endereço Destino, 32 bits cada, caracterizam por completo toda informação sobre endereçamento necessária ao processo de roteamento.

O último campo contém os dados, a informação na realidade, e tem tamanho livre porém definido pelo tipo de rede sendo o MTU igual a 1500kbytes.

Todas as informações necessárias para que o IP possa se comunicar com o resto da rede estão distribuídas nestes campos, principalmente naqueles relativos ao endereçamento. É importante observar que a camada de rede utiliza estes endereços lógicos de 4x8bits, para definir as redes existentes e como conseguir obter informação delas. Entretanto, para que os dados cheguem aos *hosts* é necessário um outro tipo de endereço: endereço *Media Access Control* - MAC ou Ethernet.

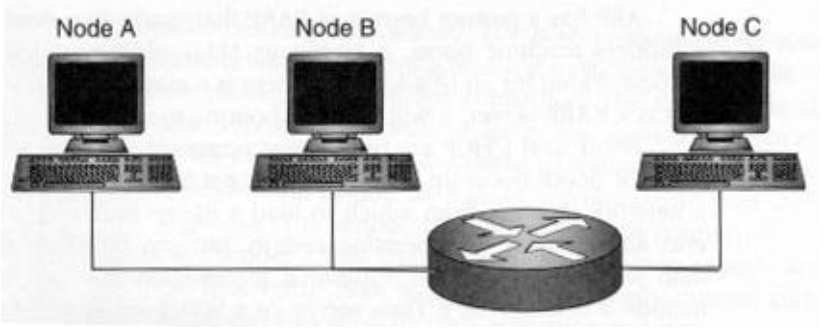
O TCP/IP define um protocolo, ARP, que caracteriza e relação entre o endereço IP e o endereço MAC. Falaremos a seguir sobre este protocolo.

6.2. Address Resolution Protocol - ARP

Na realidade, a troca de dados entre dispositivos IP é efetuada através do endereço MAC - *Media Access Control*, ou endereço Ethernet ou ainda endereço Físico. De maneira bem simplificada, podemos considerar o protocolo ARP como sendo um *broadcast* no segmento de rede perguntando qual é o endereço MAC do dispositivo que tem um certo IP.

Vamos considerar a figura abaixo através de dois exemplos típicos: comunicação no mesmo segmento de rede e em redes distintas.

Vamos considerar primeiramente uma aplicação no computador A enviando dados para o computador B, considere por simplicidade um serviço PING de A para B. O primeiro passo é determinar se A e B pertencem ao mesmo segmento de rede. Isto é feito através do simples algoritmo que compara o resultado de uma operação AND lógico entre os IP e a sua respectiva máscara: mesmo resultado mesma rede, resultados diferentes redes diferentes. No caso A e B são vizinhos de um mesmo segmento.



Na construção do datagrama, a aplicação sabe os endereços MAC e IP da fonte A e somente o endereço IP do destino B. Para descobrir o endereço MAC de B o protocolo ARP envia um *broadcast* a todos os dispositivos do segmento perguntando ao dono do IP B o seu endereço MAC. Por sua vez, o dispositivo dono do IP, envia também por *broadcast*, ou seja, para todos, o seu endereço MAC. Todos os dispositivos do segmento acrescentam na sua tabela ARP (IPxMAC), também chamada de *proxycache* ARP, este registro relativo ao B, que permanece durante um certo tempo. Finalmente, o dispositivo A envia o quadro (*frame*) destinado ao dispositivo B. Neste exemplo o mesmo quadro é enviado para B e a interface do roteador deste segmento, porém somente o dispositivo B irá abrir o quadro até a última camada pois somente ele tem o endereço MAC destino. Observe que se houvesse outros dispositivos no segmento, eles passariam a conhecer também o endereço MAC de B de maneira que se quiserem enviar algo à B posteriormente, não seria mais necessário um *broadcast* ARP.

Vamos agora considerar que a comunicação seja entre os dispositivos A e C. Primeiramente o dispositivo A determina que C pertence a outro

segmento através do algoritmo comparativo de operações AND. O dispositivo A então envia os dados para o *gateway* que é a interface do roteador. Para isto o protocolo ARP é utilizado para descobrir o endereço MAC da interface da mesma maneira que no caso anterior. Observe que o endereço MAC destino é do roteador porém o IP destino continua sendo do dispositivo C. Quando o roteador recebe os dados, ele procura pela rede à qual pertence o IP destino na sua tabela de roteamento e assim roteia para interface deste segmento. O roteador irá utilizar o protocolo ARP para determinar o endereço MAC do dispositivo C que será anexado ao cabeçalho da camada de enlace, como MAC destino e o seu próprio como MAC origem. É importante observar que os IPs origem (A) e destino (C) permanecem inalterados durante todo o processo. Quando o dispositivo C finalmente recebe a mensagem oriunda de A, o processo de volta é simplificado pois os diversos endereços MAC continuam nas tabelas dos dispositivos envolvidos (C, roteador e A).

Estes dois exemplos simples mostram o funcionamento e importância do protocolo ARP que na realidade só é usado para manter a tabela IP/MAC de cada dispositivo atualizada.

6.3. Internet Control Message Protocol - ICMP

O ICMP é um protocolo de mensagens de controle usado para informar outros dispositivos de importantes situações das quais podemos citar como exemplo: fluxo de mensagens maior que a capacidade de processamento de um dispositivo; parâmetro *Time To Live* – TTL; e mensagens de redirecionamento. Abordaremos rápida e separadamente cada um destes três exemplos.

Eventualmente um roteador pode estar recebendo mais informação do que pode processar, sendo assim ele passa a contar com controle de fluxo, enviando uma mensagem *source quench* para o dispositivo origem para que ele pare ou diminua o fluxo de dados. Esta mensagem é enviada pelo protocolo ICMP.

O segundo caso evolve o parâmetro TTL que basicamente é o número de *hops* (roteadores) total que uma informação pode percorrer. Ele é decrementado a cada *hop* e quando chega a zero, o roteador descarta o datagrama e envia uma mensagem à fonte informando que a informação não chegou ao seu destino, utilizando o ICMP.

O terceiro caso é a mensagem de redirecionamento ICMP, que é utilizada quando o roteador determina que um caminho melhor existe para o pacote que acabou de ser enviado assim mesmo. Neste caso a implementação do protocolo de roteamento pode definir um novo caminho de acordo com este melhor caminho. Alguns sistemas operacionais de roteamento não consideram esta mensagem e continuam enviando dados pelo pior caminho.

Uma aplicação típica deste protocolo é o PING, muito utilizado para determinar se um determinado dispositivo está ativo em uma rede, já que esta aplicação testa o sistema de transporte do TCP/IP.

6.4. Transmission Control Protocol - TCP

O protocolo IP, camada de rede (3), envia dados para rede sem a preocupação de verificar a chegada dos respectivos datagramas. Os protocolos da camada acima, *host-host* ou transporte (4), especificamente TCP, definem a maneira para tratar datagramas perdidos ou corruptos. Além disto, TCP é responsável pela segurança na transmissão/chegada dos dados ao destino e também define todo o processo de início de conexão e multiplexação de múltiplos protocolos da camada de aplicação (7) em uma única conexão, otimizando assim a conexão múltipla de aplicações com o mesmo destino.

O protocolo TCP é orientado a conexão sendo isto claramente observado no processo de inicialização da conexão. O TCP aplica o algoritmo *three-way handshake* ou *three-fold* nesta inicialização. Este algoritmo pode ser comparado com o ato de telefonar onde em um primeiro momento um número é discado, posteriormente alguém atende dizendo “alô” e por fim a pessoa que ligou começa a falar, enviando dados.

Na realidade, o dispositivo fonte envia uma seqüência de números que iniciará o envio de segmentos (vide final da seção 2), início de uma conexão SYN. Sendo assim o dispositivo destino passa a conhecer esta seqüência. O dispositivo destino responde com sua própria segundai de números e portanto o dispositivo fonte passa por sua vez, a conhecer a seqüência do destino, viabilizando assim a conexão pois os dispositivos envolvidos, fonte e destino, sabem as respectivas seqüências numéricas. Esta segunda etapa é conhecida como *acknowledgment* ou ACK. Na terceira e última etapa, o dispositivo fonte emite o seu sinal ACK informando que começará a enviar dados.

Assim como o IP, o TCP precisa saber qual o protocolo de aplicação da última camada que receberá os dados. Isto é feito através da codificação das portas. Ao todo são 65.535 (64k) portas, sendo que de 0 à 1024 são portas definidas e portanto só podem ser usadas por aplicações que utilizem os respectivos protocolos. As portas de 1024 à 65535 são atribuídas dinamicamente. Existem exceções que podem ser ignoradas nesta discussão.

6.5. User Datagram Protocol - UDP

Existem situações em que o dispositivo origem não precisa da garantia de chegada dos dados no dispositivo destino, como exemplo podemos citar alguns tipos de Videoconferência. Nestes casos, o TCP é substituído pelo UDP que é um protocolo que não é orientado a conexão, ou seja, não necessita estabelecer uma conexão entre origem e destino antes de enviar os dados. Este protocolo não verifica nem se o dispositivo destino está *on line*.

Na realidade o protocolo UDP empacota os dados e os envia para camada inferior (rede 3) para que o protocolo IP dê prosseguimento ao envio dos dados. Estes pacotes, segmentos, apesar de serem numerados antes de serem enviados, não sofrem nenhuma verificação de chegada ao destino.

Assim como fizemos um paralelo entre TCP e o telefone, podemos comparar o UDP com o correio regular. Preparamos uma carta, envelopamos, selamos e colocamos no correio na esperança de que chegue ao seu destino.

Assim como o TCP, o UDP também é um protocolo da camada de transporte (4), porém diferentemente não gera mensagens ICMP.

6.6. Protocolos da Camada de Aplicação

Como foi visto anteriormente, o conjunto de protocolos TCP/IP estão distribuídos ao longo das camadas superiores se comparados com o modelo ISO/OSI. Dentre estes, existem muitos protocolos que atuam na última camada (Aplicação). Abordaremos a seguir os mais utilizados pela comunidade.

6.6.1. File Transfer Protocol - FTP

A aplicação FTP foi uma das primeiras aplicações na hoje chamada Internet. A base é o protocolo FTP que tem como principal função a transferência de arquivos entre dispositivos nos formatos ASCII e Binário. É uma aplicação do tipo cliente/servidor e em uma situação típica a aplicação cliente FTP utiliza o protocolo TCP para estabelecer uma conexão com o servidor remoto. Os servidores podem disponibilizar áreas só de leitura para *download* de arquivos compartilháveis ou leitura/escrita para áreas públicas sem restrição.

Normalmente estes servidores permitem conexão autenticada, *login*/senha, com usuários cadastrados para acesso em áreas do servidor restritas ou ainda usuário *anonymous* ou mesmo *ftp*, com senha livre, normalmente o e-mail, para posterior contato. É importante observar que neste processo de autenticação o *login*/senha trafegam pela rede sem criptografia facilitando assim eventuais infortúnios como a utilização de analisadores de tráfego. Normalmente nos casos onde a autenticação é necessária se emprega servidores de FTP criptografados, sendo o *Security Shell* - SSH um dos mais populares.

Quando um cliente começa a negociar uma conexão com um servidor FTP, uma porta é escolhida e enviada para posterior conexão. O servidor, por sua vez, recebe a requisição pela porta padrão 20. A resposta do servidor é enviada pela porta 21 endereçada pela porta escolhida pelo cliente. A utilização do conceito de portas permite desta forma, que um mesmo servidor receba várias requisições pois a resposta é endereçada à diferentes portas escolhidas por cada cliente.

6.6.2. Trivial File Transfer Protocol - TFTP

Este protocolo é utilizado principalmente para transferir arquivos de configuração ou mesmo do sistema operacional entre um computador e um equipamento, roteadores, comutadores, *bridges*, impressoras, etc. A aplicação também é do tipo cliente/servidor sendo normalmente o equipamento o cliente e o computador o servidor.

Ao invés de TCP, este protocolo utiliza UDP pois apresenta a possibilidade de acesso, normalmente para configuração, à equipamentos importantes em situações críticas como por exemplo quando um roteador fica inacessível por não suportar mais conexões TCP no caso de um ataque externo.

Servidores de TFTP não possuem autenticação sendo normalmente utilizados através de uma conexão direta na porta serial ou auxiliar do equipamento para garantir confiabilidade e segurança na transferência dos arquivos. Existem várias aplicações TFTP disponibilizadas de maneira compartilhada na Internet.

6.6.3. Telnet

Esta aplicação também do tipo cliente/servidor utiliza o protocolo TCP. É utilizada para conexão remota em computadores para execução de aplicações específicas muitas das vezes desenvolvidas pelo próprio usuário. Também usada para configuração e monitoramento remoto de equipamentos, como roteadores por exemplo. Como não transfere arquivos, é comum a utilização de aplicações FTP ou TFTP em conjunto.

Da mesma forma que o FTP, existe a necessidade de autenticação e portanto todos os problemas relativos a segurança também estão presentes. Da mesma forma, existem aplicações Telnet criptografadas compartilhadas na Internet.

6.6.4. Simple Network Management Protocol - SNMP

Este protocolo utiliza UDP para fazer gerência de equipamentos, sendo o protocolo base de todas as principais plataformas de gerenciamento, CiscoWorks - CISCO, HPOpenView - HP, SunNetManager - SUN, Transcend – 3COM, SCOTTY – TU Braunschweig, MRTG, dentre outras. Sua primeira versão possuía muitas falhas relativas a segurança e portanto era alvo certo dos *hackers* para invasão às redes. Apesar disto, sua utilização cresceu a ponto de se tornar o protocolo padrão das principais plataformas.

O funcionamento das aplicações está vinculado ao envio/recebimento periódico de mensagens, equipamentos/computadores respectivamente, que contém valores de parâmetros relevantes para monitoramento, análise e posterior configuração por parte dos equipamentos. Estas informações são

armazenadas em forma de base de dados chamada *Management Information Base* – MIB.

É possível configurar as aplicações para que enviem avisos através de e-mails, de sinais visuais e sonoros, Tc, aos gerentes de rede quando situações críticas ocorrerem, como por exemplo a mudança de estado de uma porta de um roteador, nível de tráfego fora dos limites, percentagem de processamento perto do limite, dentre outras.

6.7. Outros Protocolos e Aplicações

Existem vários outros protocolos que pertencem ao grupo TCP/IP dos quais podemos citar: SMTP, DNS, NFS, HTTP, RIP, *Rlogin*, *X Windows*, *Packet Internet Groper* – PING, *Traceroute*. Abordaremos rapidamente alguns deles.

Domain Name Server – DNS: também chamada de *Name Service*, esta aplicação relaciona endereços IP com os seus respectivos nomes atribuídos a dispositivos da rede.

Simple Mail Transfer Protocol – SMTP: este protocolo é utilizado nos serviços básicos de envio de mensagens.

Network File System – NFS: este sistema foi desenvolvido pela Sun Microsystems e permite que computadores possam "montar" discos ou parte deles (diretórios) de dispositivos remotos e operá-los como se fossem locais.

HyperText Transfer Protocol – HTTP: este protocolo é a base do ambiente *World Wide Web* que basicamente permite a leitura dinâmica e interativa de documentos constituídos de texto, imagens e som.

Routing Information Protocol – RIP: o conceito de roteamento é uma característica presente nos protocolos TCP/IP. O protocolo RIP é utilizado pelos dispositivos da rede, principalmente roteadores, para troca de informações de roteamento.

Dentre aqueles citados, é importante observar que os dois últimos, PING e *Traceroute*, são muito utilizados no monitoramento de conectividade entre dispositivos TCP/IP. No primeiro é possível o envio de pacotes em número e tamanho variáveis e o recebimento de sua respectiva estatística. O segundo revela o caminho percorrido por um pacote entre os dispositivos origem e destino parametrizado pelo tempo de resposta.

7. Conclusão

TCP/IP não é um protocolo único, é uma coleção de protocolos com arquitetura distribuída em 4 camadas que se distribuem sobre as camadas do modelo OSI: aplicação, *host-host*, rede e física.

A camada física não é descrita na arquitetura TCP/IP apesar de ser a base para a comunicação entre a aplicação e a rede. O protocolo IP é a base da arquitetura pois atribui endereços lógicos aos dispositivos e às redes e assim consegue definir o caminho para levar os pacotes da origem ao destino.

TCP e UDP são protocolos da camada de transporte e tem como função principal a entrega de dados (segmentos) aos dispositivos destinos. O TCP é um protocolo orientado à conexão e assim garante que os dados cheguem na ordem certa ao seu destino. O UDP ao contrário, é não orientado a conexão e não garante a chegada dos dados ao destino.

Existem vários outros protocolos e aplicações que utilizam conexões TCP/IP e UDP/IP, e que não foram abordados aqui por simplicidade apenas.

A importância do conjunto de protocolos TCP/IP está totalmente ligada ao sucesso da Internet. Estes protocolos, apesar de suas limitações em termos de roteamento, cada vez mais, estão se tornando a base de aplicações que são disponibilizadas e necessárias à Internet.

O sucesso deste conjunto de protocolos implica inclusive no sucesso ou não da aplicação de outras tecnologias de comunicação. Atualmente podemos citar a tecnologia ATM como sendo uma das tecnologias que necessitam de artifícios de software para suportar aplicações IP.

O grande e crescente número de aplicações IP garante uma sobrevida ainda sem previsão de término à este conjunto de protocolos que já entraram para a história das comunicações. Atualmente, “falar TCP/IP” é condição básica para que um dispositivo entre na grande rede.

Referências

✍✍"CCNA Certification – Routing Basics for CISCO Certified Network Associates Exam 640-407", R. N. Myhre, Prentice-Hall, ISBN: 0-13-086185-5, 1999

✍✍"TCP/IP Network Administration", C. Hunt, O'Reilly Associates, ISBN: 1-56592-322-7, second edition, December 1997.kklpkmn o—k-plkm06hyujmm

✍✍ "Using Linux – The Most Complete Reference"; J. Tackett, D. Gunter e L. Brown; QUE Corporation, ISBN: 0-7897-01000-6, 1995.

✍✍"Understanding TCP/IP – Appendix A", http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ap1.htm, April 2000.