

Um Tutorial TCP/IP

Estado deste memorando

Esta RFC¹ é um tutorial a respeito da suíte de protocolos TCP/IP, focado particularmente no encaminhamento de datagramas² IP de um hospedeiro de origem a um hospedeiro de destino, através de um roteador. Aqui não está especificado um padrão da Internet. A distribuição deste memorando é ilimitada.

Tabela de conteúdo

1. Introdução
2. Visão Geral do TCP/IP
3. Ethernet
4. ARP
5. Internet Protocol
6. User Datagram Protocol
7. Transmission Control Protocol
8. Aplicações de Rede
9. Outras informações
10. Referências
11. Relações com outras RFCs
12. Considerações de segurança
13. Endereço dos autores
14. Tradução, Comentários e Ilustrações

1 Introdução

Este tutorial contém apenas uma visão dos pontos principais do TCP/IP, e portanto, o “esqueleto” da tecnologia TCP/IP. Omite-se a história do desenvolvimento e financiamento, os casos de negócio para seu uso, e seu futuro comparado com o ISO OSI. De fato, uma grande quantidade de informação técnica é omitida. O que resta é um mínimo de informação que precisa ser compreendida pelo profissional que trabalha em um ambiente TCP/IP. Esses profissionais incluem os administradores de sistema, os programadores de sistemas e os gerentes de rede.

Este tutorial usa exemplos do ambiente TCP/IP do UNIX; contudo, os pontos principais aplicam-se a todas as implementações do TCP/IP.

Note que o propósito deste memorando é explanação, não definição. Se qualquer dúvida surgir sobre a especificação correta do protocolo, por favor consulte a atual RFC que define o padrão.

1 Sigla para Request for Comments (Requisição de comentários).

2 Isto é, *pacote*.

A próxima seção é uma visão geral do TCP/IP, seguida por descrições detalhadas dos componentes individuais.

2 Visão Geral do TCP/IP

O termo genérico “TCP/IP” normalmente refere-se a tudo ou qualquer coisa relacionada com os protocolos TCP e IP. Isso pode incluir outros protocolos, aplicações, e até mesmo a mídia³ de rede. Exemplos de três protocolos: UDP, ARP e ICMP. Exemplos de três aplicações: TELNET, FTP e RCP. Um termo mais preciso seria “tecnologia internet”. Uma rede que utiliza tecnologia internet é chamada “internet”.

2.1 Estrutura básica

Para entender a tecnologia, você deve primeiro entender a estrutura lógica a seguir:

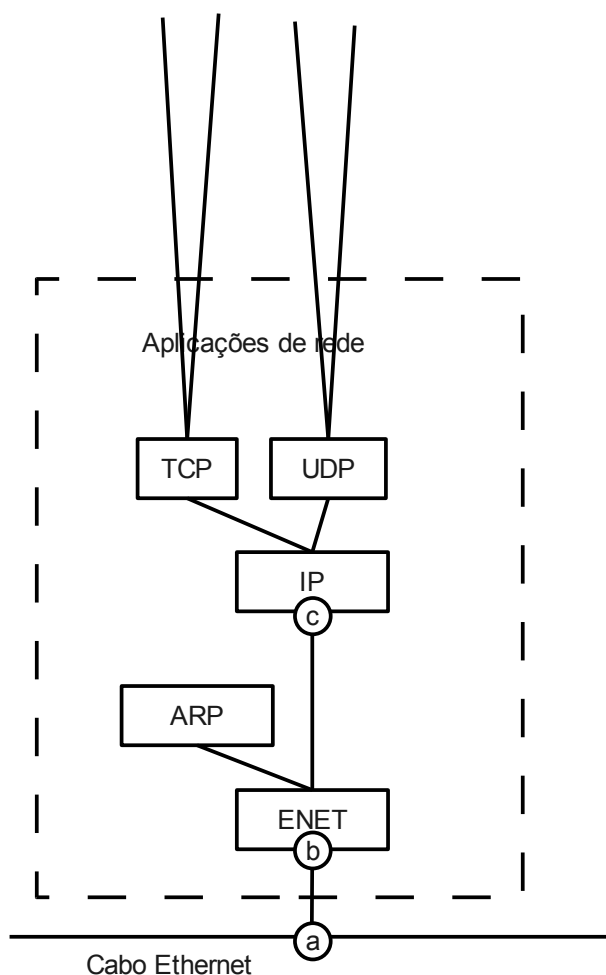


Figura 1: Nó básico de uma rede TCP/IP

Esta é a estrutura lógica dos protocolos em camadas, no interior de um computador em uma

³ Isto é, o meio físico, o enlace, como os cabos, por exemplo.

internet. Cada computador que pode se comunicar usando a tecnologia internet possui uma estrutura lógica. É esta estrutura lógica que determina o comportamento do computador na Internet. Os retângulos representam o processamento dos dados quando passam através do computador; as linhas que conectam os retângulos mostram o caminho dos dados. A linha horizontal na parte inferior representa o cabo Ethernet; o círculo com a letra “a” é o transceptor⁴. O círculo com o “b” representa o endereço Ethernet. O círculo com a letra “c” representa o endereço IP. Entender esta estrutura lógica é essencial para entender a tecnologia internet; esta será referenciada completamente neste tutorial.

2.2 Terminologia

O nome da unidade de dados que flui através de uma internet depende de onde ela está na pilha de protocolos. Em resumo: se ela está em uma Ethernet, é chamada quadro Ethernet; se está entre o controlador Ethernet e o módulo IP é chamado de pacote IP; se está entre o módulo IP e o módulo UDP é chamado de datagrama UDP; se está entre o módulo IP e o módulo TCP é chamado de segmento TCP (mais genericamente, uma mensagem de transporte); e se ela está na aplicação de rede é chamada uma mensagem de aplicação.

Essas definições são imperfeitas. Definições atuais variam de uma publicação para outra. Definições mais específicas podem ser encontradas na RFC 1122, seção 1.3.3.

Um controlador⁵ é um software que se comunica diretamente com o hardware de interface de rede. Um módulo é um software que se comunica com o controlador, com aplicações de rede, ou com outro módulo.

Os termos: controlador, módulo, quadro Ethernet, pacote IP, datagrama UDP, mensagem TCP e mensagem de aplicação, são usados apropriadamente ao longo deste tutorial.

2.3 Fluxo dos Dados

Vamos seguir os dados que fluem através da pilha de protocolos exibida na Figura 1. Para uma aplicação que usa TCP (Transmission Control Protocol – Protocolo de Controle de Transmissão), dados passam entre a aplicação e o módulo TCP. Para aplicações que usam UDP (User Datagram Protocol – Protocolo de Datagrama do Usuário), dados passam entre a aplicação e o módulo UDP. FTP (File Transfer Protocol – Protocolo de Transferência de Arquivos) é uma aplicação típica que usa TCP. Sua pilha de protocolos, neste exemplo, é FTP/TCP/IP/ENET. O SNMP (Simple Network Management Protocol – Protocolo Simples de Gerenciamento de Redes) é uma aplicação que usa UDP. Sua pilha de protocolo neste exemplo é SNMP/UDP/IP/ENET.

O módulo TCP, o módulo UDP e o controlador Ethernet são multiplexadores n-para-1. Como multiplexadores, eles comutam várias entradas em uma saída. Eles são também demultiplexadores 1-para-n. Como demultiplexadores eles comutam uma entrada para várias saídas de acordo com o campo no cabeçalho do protocolo.

4 Isto é, a placa de rede.

5 Inglês: *driver*.

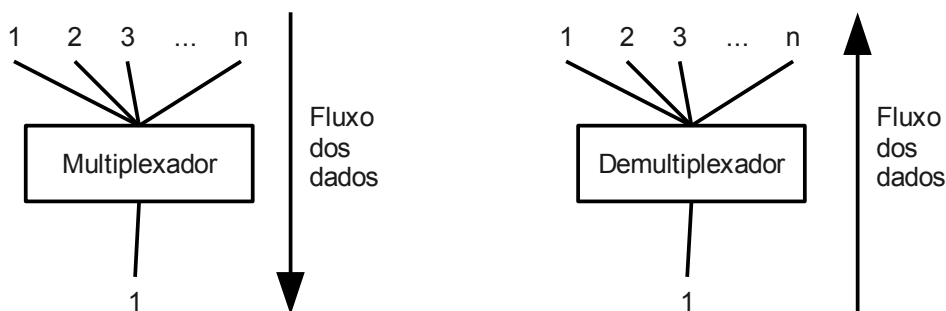


Figura 2: Multiplexador n -para-1 e demultiplexador 1-para- n

Se um quadro Ethernet sobe no driver Ethernet, vindo da rede, o pacote pode ser passado para cima, para o módulo ARP (Address Resolution Protocol – Protocolo de Resolução de Endereço) ou para o módulo IP (Internet Protocol – Protocolo Internet). O valor no campo "tipo" no quadro Ethernet determina para quem o quadro Ethernet é passado: se para o módulo ARP ou IP.

Se um pacote IP sobe no IP, a unidade de dados é passada para cima, para o TCP ou UDP, como determinado pelo valor no campo "protocolo" no cabeçalho IP.

Se um datagrama UDP sobe no UDP, a mensagem de aplicação é passada para cima, para a aplicação de rede, baseado no valor no campo "porta" no cabeçalho UDP. Se uma mensagem TCP sobe no TCP, a mensagem de aplicação é passada para cima, para a aplicação de rede, baseado no valor do campo "porta" no cabeçalho TCP.

A multiplexação para baixo é simples de executar, pois para cada ponto inicial há somente um caminho para baixo; cada módulo de protocolo adiciona sua informação no cabeçalho, de modo que o pacote possa ser demultiplexado no computador de destino.

Os dados que vão para fora, a partir das aplicações através do TCP ou UDP, convergem no módulo IP, e ele envia para baixo através do controlador de interface de rede.

Apesar de a tecnologia internet suportar várias mídias de redes diferentes, Ethernet é usada em todos os exemplos deste tutorial, pois ela é a rede física mais comum usada pelo IP⁶. O computador da Figura 1 possui uma conexão Ethernet única. O endereço Ethernet de 6 bytes é único para cada interface em uma Ethernet; está na parte inferior do controlador Ethernet.

O computador também possui um endereço IP de 4 bytes. Este endereço está localizado na parte inferior da interface do módulo IP. O endereço IP deve ser único em uma internet⁷.

Um computador em funcionamento sempre sabe seu endereço IP e endereço Ethernet.

2.4 Duas Interfaces de Rede

Se um computador é conectado a duas Ethernets separadas, ele é parecido com a Figura 3.

⁶ Isso já em 1991!

⁷ Aqui ele está falando de uma rede, e não da Internet inteira, como já deve ter ficado claro. Todavia, vale um comentário a respeito da atribuição de IPs na época: antes da explosão de hospedeiros na Internet e antes da exaustão de números IP, havia a possibilidade de todos os IPs atribuídos serem públicos, uma vez que os endereços privados foram instituídos apenas em 1996, com a RFC-1918.

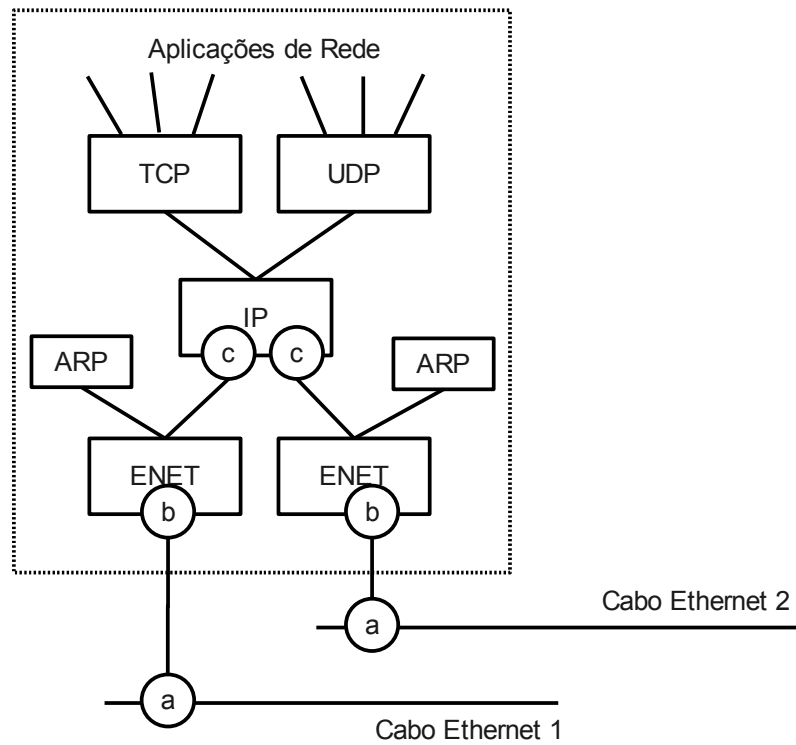


Figura 3: Nó de Rede TCP/IP com duas Ethernets

Por favor observe que este computador possui 2 endereços Ethernet e 2 endereços IP.

Como visto nesta estrutura, em computadores com mais de uma interface física o módulo IP é tanto um multiplexador n-para-m quanto um demultiplexador m-para-n.

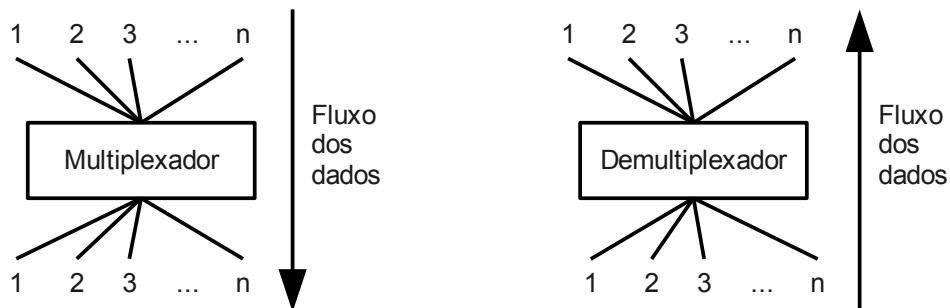


Figura 4: Multiplexador n-para-m e demultiplexador m-para-n

Ele executa a multiplexação em ambas as direções, a fim de acomodar dados que entram e que saem. Um módulo IP com mais de uma interface de rede é mais complexo que nosso exemplo original, em que ele encaminhava dados à rede mais próxima. Dados podem chegar em qualquer interface de rede, e serem enviados para qualquer outra.

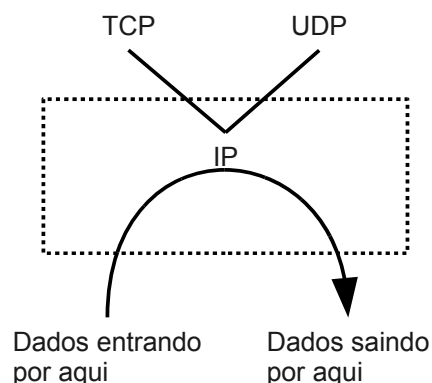


Figura 5: Exemplo de encaminhamento IP em um pacote IP

O processo de enviar um pacote IP para outra rede é chamado de “encaminhamento” de pacotes IP. Um computador que é dedicado a tarefa de encaminhar pacotes IP é chamado “roteador IP”.

Como você pode ver na figura, o encaminhamento de pacote IP nunca toca nos módulos TCP e UDP no roteador IP⁸. Algumas implementações de roteadores IP sequer possuem um módulo TCP ou UDP.

2.5 IP Criando Uma Rede Lógica Simples

O módulo IP é central para o sucesso da tecnologia internet. Cada módulo ou controlador adiciona seu cabeçalho à mensagem e a mensagem é passada para baixo na pilha de protocolos. Cada módulo ou controlador retira o cabeçalho correspondente da mensagem e a mensagem sobe na pilha de protocolos até a aplicação. O cabeçalho IP contém o endereço IP, que cria uma única rede lógica para múltiplas redes físicas. A interconexão de redes físicas é a origem do nome internet. Um conjunto de redes físicas interconectadas que limitam o escopo do pacote IP é chamada de uma "internet".

2.6 Independência de Rede Física

O IP oculta o hardware de rede subjacente para as aplicações de rede. Se você inventar uma nova interface física, você pode colocá-la em serviço implementando um novo controlador, que se conecta à internet sob o IP. Desse modo, as aplicações de rede permanecem intactas e não são vulneráveis a alterações na tecnologia de hardware.

2.7 Interoperabilidade

Se dois computadores em uma internet podem se comunicar, diz-se que são interoperáveis. Usuários de computadores de uso geral se beneficiam da instalação em uma internet, porque há interoperabilidade nos computadores do mercado. Geralmente, quando você compra um computador, você tem interoperabilidade. Se seu computador não tem interoperabilidade, e além

⁸ É claro que hoje isso é uma inverdade. Hoje em dia, no caso de redes privadas em empresas que usam NAT/PAT, os roteadores trabalham no nível dos protocolos TCP e UDP, fazendo troca de portas.

disso a interoperabilidade não pode ser adicionada, ele ocupa um nicho raro e muito específico no mercado.

2.8 Após a visão geral...

Com o plano de fundo definido, podemos fazer as seguintes perguntas:

Quando se envia um pacote IP para fora do computador, como o endereço Ethernet de destino é determinado?

Como é que o IP sabe qual das múltiplas interfaces de rede inferiores usar para enviar um pacote IP?

Como um cliente em um computador alcança um servidor em outro?

Por que tanto o TCP quanto o UDP existem, em vez de apenas um ou outro?

Quais as aplicações de rede que estão disponíveis?

Estas questões serão explanadas, de cada vez, após uma recordação sobre o Ethernet.

3 Ethernet

Esta seção é uma curta revisão sobre a tecnologia Ethernet.

Um quadro Ethernet contém o endereço de destino, endereço de origem, campo "tipo", e os dados.

Um endereço Ethernet possui 6 bytes. Todo dispositivo possui seu próprio endereço Ethernet e escuta por quadros Ethernet com este endereço de destino. Todos os dispositivos também escutam por quadros Ethernet cujo endereço destino é o coringa "FF-FF-FF-FF-FF-FF" (em hexadecimal) chamado de endereço "broadcast".

Ethernet usa CSMA/CD (Carrier Sense and Multiple Access with Collision Detection – Acesso Múltiplo com Detecção de Portadora e Detecção de Colisão). CSMA/CD significa que todos os dispositivos se comunicam em uma mídia simples, que somente um pode transmitir por vez, e que todos eles podem receber simultaneamente. Se 2 dispositivos tentarem transmitir no mesmo instante, uma colisão é detectada na transmissão, e ambos os dispositivos aguardam por um período aleatório (porém curto) antes de tentarem transmitir novamente.

3.1 Uma Analogia Humana

Uma boa analogia da tecnologia Ethernet é um grupo de pessoas falando em um quarto pequeno e completamente escuro. Nesta analogia, a mídia da rede física são as ondas sonoras no ar no quarto em vez de sinais elétricos no cabo coaxial.

Cada pessoa pode ouvir as palavras enquanto outro fala (Detector de Portadora). Todos no quarto têm capacidade igual de conversar (Acesso Múltiplo), mas nenhum deles dá longos discursos, pois são educados. Se a pessoa é mal educada, ela é convidada a retirar-se do quarto (i.e., é jogado fora da rede).

Ninguém fala enquanto outro está falando. Mas se duas pessoas iniciam a conversação ao mesmo

tempo, cada um tem conhecimento disso, pois ouve algo que não disse (Detecção de Colisão). Quando essas duas pessoas percebem esta condição, elas aguardam por um momento, e uma começa a falar. A outra ouve a conversa e aguarda que o primeiro termine antes de começar a falar suas palavras.

Cada pessoa possui um único nome (único endereço Ethernet) para evitar confusão. Cada vez que um deles fala, ele começam a mensagem com o nome da pessoa que estão conversando, seguido do seu próprio nome (o endereço Ethernet de destino e origem, respectivamente), isto é, “Olá Jane, aqui é o Jack, .. blá blá blá ...”. Se o emitente procura falar com todos, ele diz “todos” (endereço de broadcast), isto é, “Olá Todos, aqui é o Jack, ... blá, blá, blá ...).

4 ARP

Quando se envia um pacote IP para fora do computador, como o endereço Ethernet de destino é determinado?

O ARP (Address Resolution Protocol – Protocolo de Resolução de Endereço) é usado para traduzir um endereço IP para um endereço Ethernet. A tradução é feita somente para pacotes IP de saída, isto é, quando o cabeçalho IP e o cabeçalho Ethernet são criados.

4.1 Tabela ARP e Tradução de Endereços

A tradução é realizada com uma consulta a uma tabela. A tabela, chamada tabela ARP, é armazenada na memória e contém uma linha para cada computador. Ela tem uma coluna para o endereço IP e outra para o endereço Ethernet. Quando há uma tradução de um endereço IP para um endereço Ethernet, é realizada uma procura na tabela pelo um endereço IP correspondente. A seguir, um exemplo simplificado de uma tabela ARP:

Endereço IP	Endereço Ethernet
223.1.2.1	08-00-39-00-2F-C3
223.1.2.3	08-00-5A-21-A7-22
223.1.2.4	08-00-10-99-AC-54

Tabela 1: Exemplo de tabela ARP

A convenção humana para escrever o endereço IP de 4 bytes é: cada byte em decimal, separando cada byte com um ponto. Para escrever o endereço Ethernet de 6 bytes, a convenção é: cada byte em hexadecimal, separando bytes com um sinal de menos⁹ ou dois pontos.

A tabela ARP é necessária porque os endereços IP e Ethernet são selecionados de forma independente; você não pode usar um algoritmo para converter um endereço IP em um endereço Ethernet¹⁰. O endereço IP é selecionado pelo gerente de rede baseado na localização do computador

⁹ Isto é, um hífen.

¹⁰ Nos dias de hoje, a operação normal do IPv6 permite que os últimos 64 bits endereço IPv6 seja criado a partir do endereço Ethernet da máquina.

em uma internet. Quando o computador é movido para uma parte diferente de uma internet, o endereço IP deve ser alterado. O endereço Ethernet é selecionado pelo fabricante baseado no espaço de endereços Ethernet licenciados para o fabricante. Quando a interface Ethernet muda, o endereço Ethernet também muda.

4.2 Cenário Típico de Tradução

Durante a operação normal, uma aplicação de rede, como TELNET, envia uma mensagem de aplicação para o TCP; então o TCP envia a mensagem TCP correspondente ao módulo IP. O endereço IP de destino é conhecido pela aplicação, pelo módulo TCO, e pelo módulo IP. Neste ponto o pacote IP foi construído e está pronto para encaminhado para o controlador Ethernet, mas primeiro o endereço Ethernet de destino deve ser determinado.

A tabela ARP é usada para olhar o endereço Ethernet de destino.

4.3 Requisição ARP / Par de Resposta

Mas como a tabela ARP foi preenchida na primeira vez? A resposta é que ela é preenchida automaticamente pelo ARP conforme a necessidade.

Duas coisas acontecem quando a tabela ARP não pode ser usada para traduzir um endereço:

1. Um pacote de requisição ARP com endereço de destino broadcast é enviado para fora do computador, na rede, para todos os computadores.
2. O pacote IP de saída é enfileirado.

Todas as interfaces Ethernet dos computadores recebem o quadro de broadcast Ethernet. Cada controlador Ethernet examina o campo "tipo" no quadro Ethernet e passa o pacote ARP para o módulo ARP. O pacote de requisição ARP diz: "Se o seu endereço IP corresponde com este IP alvo, então por favor me diga seu endereço Ethernet". Um pacote de requisição ARP se parece com isso:

Endereço IP do remetente	223.1.2.1
Endereço ENET do remetente	08-00-39-00-2F-C3
Endereço IP alvo	223.1.2.2
Endereço ENET alvo	<em branco>

Tabela 2: Exemplo de requisição ARP

Cada módulo ARP examina o endereço IP; se o endereço IP alvo corresponde ao seu endereço IP, então ela envia uma resposta diretamente para o endereço Ethernet da origem. O pacote de resposta ARP diz: "Sim, o IP alvo é meu endereço IP, aqui está meu endereço Ethernet". Um pacote de resposta ARP possui o campo remetente/alvo trocados, se comparado com a requisição. Ele se parece com isso:

Endereço IP do remetente	223.1.2.2
Endereço ENET do remetente	08-00-28-00-38-A9
Endereço IP alvo	223.1.2.1
Endereço ENET alvo	08-00-39-00-2F-C3

Tabela 3: Exemplo de resposta ARP

A resposta é recebida pelo computador que era o remetente original. O controlador Ethernet olha o campo Tipo no quadro Ethernet e passa o pacote ARP para o módulo ARP. O módulo ARP examina o pacote ARP e adiciona os endereços IP e Ethernet do remetente à tabela ARP.

A tabela atualizada agora se parece com isso:

Endereço IP	Endereço Ethernet
223.1.2.1	08-00-39-00-2F-C3
223.1.2.2	08-00-28-00-38-A9
223.1.2.3	08-00-5A-21-A7-22
223.1.2.4	08-00-10-99-AC-54

Tabela 4: A tabela ARP depois da resposta

4.4 Continuação do cenário

A nova tradução está agora automaticamente instalada na tabela, apenas milissegundos depois do requisitado. Como você se lembra no passo 2 anteriormente, o pacote IP de saída é enfileirado. A seguir, a tradução do endereço IP para o endereço Ethernet foi efetuada olhando-se na tabela ARP, e o quadro Ethernet é transmitido na Ethernet. Portanto, com os novos passos 3, 4 e 5, o cenário para o computador remetente é:

1. Um pacote de requisição ARP com endereço de destino broadcast é enviado para fora do computador, na rede para todos os computadores.
2. O pacote IP de saída é enfileirado.
3. A resposta ARP chega com a tradução de endereços IP para Ethernet, indo para a tabela ARP.
4. Para o pacote IP enfileirado, a tabela ARP é usada para traduzir o endereço IP para o endereço Ethernet.
5. O quadro Ethernet é transmitido na Ethernet.

Em resumo, quando a tradução está faltando na tabela ARP, um pacote IP é enfileirado. Os dados da tradução são rapidamente preenchidos por meio de Requisições/Respostas ARP e o pacote IP enfileirado é transmitido.

Cada computador possui uma tabela ARP separada para cada interface Ethernet existente. Se o computador alvo não existe, não haverá resposta ARP e não haverá entrada na tabela ARP. O IP

descartará os pacotes IP de saída enviados para aquele endereço.

Muitas implementações do IP e do ARP não enfileiram pacotes IP enquanto aguardam por uma resposta ARP. Ao contrário, o pacote IP é descartado e recuperado a partir do pacote IP perdido que fica no módulo TCP¹¹ ou na aplicação de rede UDP¹². A recuperação é realizada por esgotamento de tempo e retransmissão. Uma mensagem retransmitida é enviada com sucesso para fora na rede porque a primeira cópia da mensagem já tinha sido a causa da tabela ARP ser preenchida.

5 Internet Protocol

O módulo IP é central para a tecnologia internet e a essência do IP nas tabelas de roteamento. O IP usa uma tabela na memória para criar todas as decisões sobre roteamento de pacotes IP. O conteúdo da tabela de roteamento é definida pelo administrador de rede. Enganos bloqueiam a comunicação¹³.

Entender como a tabela de roteamento é usada é entender interconexão de redes. A compreensão é necessária para se ter sucesso na administração e manutenção da rede IP.

A tabela de roteamento é melhor entendida se primeiro tivermos uma visão geral de roteamento, seguindo de endereços de redes IP, e então olhando para os detalhes.

5.1 Roteamento Direto

A figura abaixo é uma pequena internet com 3 computadores: A, B e C. Cada computador possui a mesma pilha de protocolos TCP/IP da Figura 1. Cada interface Ethernet dos computadores possuem seus respectivos endereços Ethernet. Cada computador tem seu endereço IP atribuído à interface IP pelo gerente da rede, que também atribuiu um número IP de rede à Ethernet.

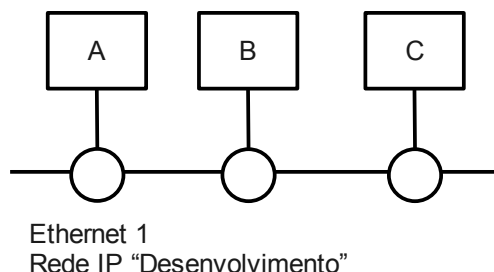


Figura 6: Uma rede IP

Quando A envia um pacote IP para B, o cabeçalho IP contém o endereço IP de A como endereço IP de origem, e o cabeçalho Ethernet contém o endereço Ethernet de A como endereço Ethernet de origem. Além disso, o cabeçalho IP contém o endereço IP de B como o endereço IP de destino e o cabeçalho Ethernet contém o endereço Ethernet de B como endereço Ethernet de destino.

11 O que está sendo dito aqui é que quando um pacote IP é descartado, o módulo TCP recebe a resposta de tempo esgotado e retransmite os mesmos dados, que ficam no buffer temporário no módulo do TCP. É uma funcionalidade típica do TCP retransmitir pacotes por tempo esgotado.

12 É interessante notar que o UDP não oferece retransmissão: isso precisa ser implementado na aplicação. Inteligentemente, os autores desta RFC observaram bem isso, como não poderia deixar de ser, é claro.

13 "Mistakes block communication". Primeira ocorrência do termo nesta RFC.

Endereço	Origem	Destino
Cabeçalho IP	A	B
Cabeçalho Ethernet	A	B

Tabela 5: Endereços no quadro Ethernet para um pacote IP de A para B

Nesta situação simples, o IP é sobrecarregado, pois o IP pouco adiciona ao serviço oferecido pelo Ethernet. Além disso, o IP ainda adiciona custo: processamento extra da CPU e consumo de banda de rede é gerado, além da transmissão e a análise de cabeçalho IP.

Quando o módulo IP de B recebe o pacote IP de A, ele compara o endereço IP de destino contra o seu próprio, observando se há correspondência; então, passa o datagrama para o protocolo de nível superior.

Esta comunicação entre A e B usa roteamento direto.

5.2 Roteamento Indireto

A figura abaixo é uma visão mais realista de uma internet. Ela é composta por 3 Ethernets e 3 redes IP conectadas por um roteador IP, chamado “computador D”. Cada rede IP tem 4 computadores; cada computador tem seu próprio endereço IP e endereço Ethernet.

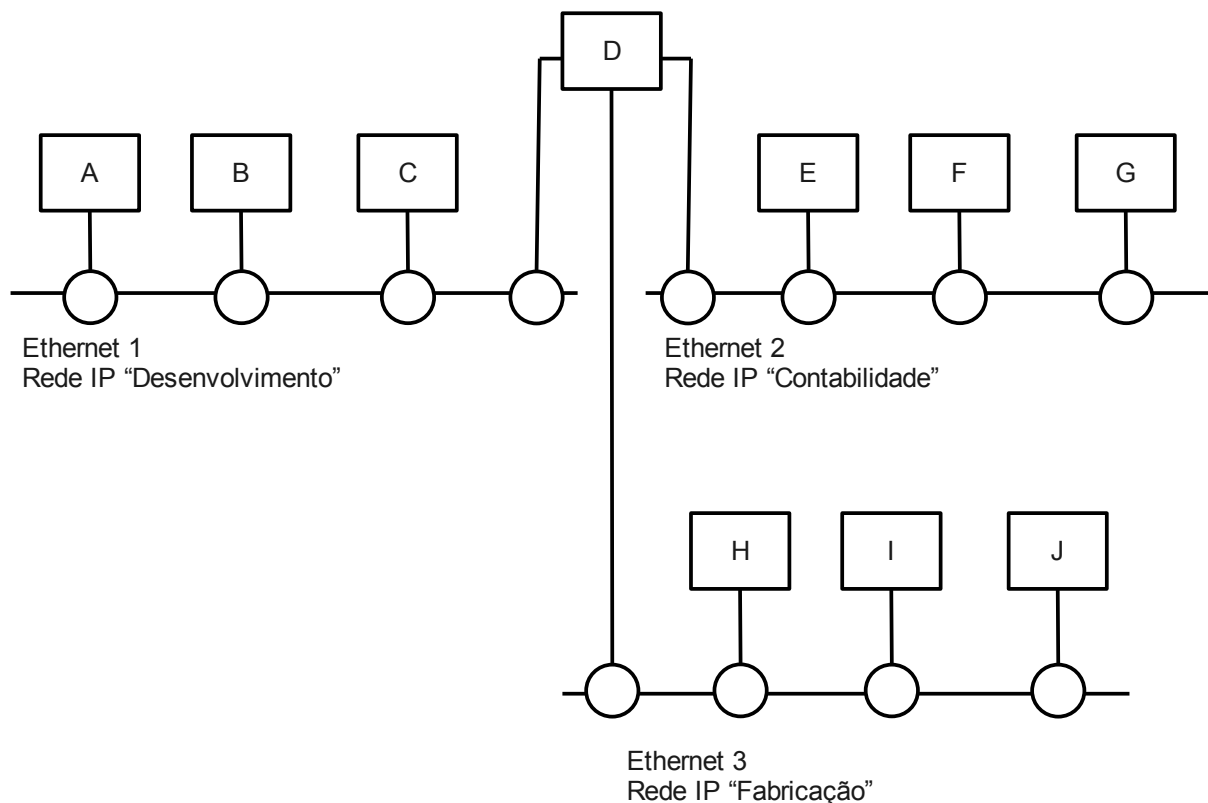


Figura 7: Três redes IP; uma internet

Com exceção do computador D, cada computador possui uma pilha de protocolos TCP/IP parecida com a Figura 1. O computador D é um roteador IP; ele é conectado a todas as 3 redes e, portanto, possui 3 endereços IP e 3 endereços Ethernet. O computador D tem uma pilha de protocolos TCP/IP similar ao da Figura 3, exceto pelo fato de que ele possui 3 módulos ARP e 3 drivers Ethernet, em vez de 2. Observe que o computador D tem apenas um módulo IP.

O gerente de rede atribuiu um único número, chamado número IP da rede, a cada uma das Ethernets. Os números IP das redes não são mostrados neste diagrama, apenas os nomes das redes.

Quando o computador A envia um pacote IP ao computador B, o processo é idêntico ao exemplo anterior da rede simples. Qualquer comunicação entre computadores localizados em uma rede IP única corresponde ao exemplo de roteamento direto discutido anteriormente.

Quando os computadores D e A se comunicam, eles fazem uma comunicação direta. Quando o computador D e E se comunicam, eles fazem uma comunicação direta. Quando os computadores D e H se comunicam, eles fazem uma comunicação direta. Isso acontece porque cada um desses três pares de computadores está na mesma rede IP.

Porém, quando o computador A se comunica com um computador do outro lado do roteador IP, a comunicação não é mais direta. Esta comunicação é chamada “indireta”.

Esse roteamento de pacotes IP é realizado pelos módulos IP e acontece de maneira transparente para o TCP, UDP e aplicações de rede.

Se A envia um pacote a E, o endereço IP de origem e o endereço Ethernet de origem são os de A. O endereço IP de destino é E, porém, como o módulo IP de A está enviando o pacote para D fazer o encaminhamento, o endereço Ethernet de destino é o de D.

Endereço	Origem	Destino
Cabeçalho IP	A	E
Cabeçalho Ethernet	A	D

Tabela 6: Endereços no quadro Ethernet e no pacote IP de A para E (antes de D)

O módulo IP de D recebe o pacote IP, e subindo-o, examina o endereço IP de destino; então ele diz: "Este não é meu endereço IP". Fazendo isso, envia o pacote IP diretamente para E.

Endereço	Origem	Destino
Cabeçalho IP	A	E
Cabeçalho Ethernet	D	E

Tabela 7: Endereços no quadro Ethernet e no pacote IP de A para E (depois de D)

Resumindo: na comunicação direta, tanto o endereço IP de origem como o endereço Ethernet de origem é o do remetente, e o endereço IP de destino, assim como o endereço Ethernet de destino, é o do destinatário. Na comunicação indireta, os endereços IP e Ethernet não fazem par, como nesta

forma.

Este exemplo de internet é muito simples. Redes reais frequentemente são complicadas por muitos fatores, resultando em múltiplos roteadores IP e alguns tipos de redes físicas. Este exemplo de internet poderia acontecer no caso de o gerente de rede separar uma Ethernet grande, para localizar tráfego Ethernet de broadcast.

5.3 Regras de Roteamento no Módulo IP

Essa visão geral do roteamento mostrou que funciona, mas não como funciona. Agora vamos examinar as regras, ou algoritmo, usado pelo módulo IP.

- Para um pacote IP de saída, entre com o IP a partir camada superior; então o IP deve decidir se deve enviar o pacote IP diretamente ou indiretamente, e o IP deve escolher uma interface de rede inferior. Essas escolhas são feitas consultando-se a tabela de roteamento.
- Para um pacote IP de entrada, entre com o IP a partir da camada inferior; então o IP deve decidir se deve encaminhar o pacote IP ou passá-lo para a camada superior. Se o pacote IP deve ser encaminhado, ele é tratado como um pacote IP de saída.
- Quando um pacote IP de entrada chega ele nunca é encaminhando novamente através da mesma interface de rede.

Essas decisões são feitas antes de o pacote IP ser entregue à interface inferior, e antes de a tabela ARP ser consultada.

5.4 Endereços IP

O gerente de rede atribui endereços IP aos computadores de acordo com a rede IP que cada computador estava anexado. Uma parte do endereço IP de 4 bytes é o número IP da rede, e outra parte é o número IP do computador (ou IP do hospedeiro). Para o computador na Tabela 1, com endereço IP 223.1.2.1, o número de rede é 223.1.2, e o número do hospedeiro é o número 1.

A porção do endereço que é usada para numeração da rede e para numeração do hospedeiro é definido pelos bits superiores no endereço de 4 bytes. Todos os exemplos de endereços IP neste tutorial são do tipo classe C, significando que os 3 bits¹⁴ superiores indicam que 21 bits são o número da rede, e 8 bits são o número do hospedeiro. Isso permite 2.097.152 redes de classe C, possuindo 254 hospedeiros em cada rede.

O espaço de endereços IP é administrada pela NIC¹⁵ (Network Information Center – Centro de Informações de Rede). Todas as internets que são conectadas à única Internet mundial devem usar números de rede atribuídos pelo NIC. Se você configurar sua própria internet e se não pretende conectá-la à Internet, você ainda deveria obter seus números de rede da NIC. Se você escolher o seu próprio número, corre o risco de confusão e caos, quando eventualmente sua internet for conectada a outra internet.

14 Conforme consta, endereços de classe C começam com os bits 110. Esses são os três bits iniciais que definem que o endereço é de classe C.

15 Hoje em dia é administrado pela IANA - Internet Assigned Numbers Authority.

5.5 Nomes

As pessoas referem-se aos computadores por nome, não números. Um computador chamado "alfa" poderia ter o endereço IP 223.1.2.1. Para pequenas redes, a tradução de nome para endereço é muitas vezes mantida em cada computador, no arquivo "hosts"¹⁶. Para grandes redes, o arquivo de dados de tradução é armazenado em um servidor e acessado através da rede quando necessário. Algumas linhas para o arquivo pode se parecer com isso:

```
223.1.2.1      alfa
223.1.2.2      beta
223.1.2.3      gama
223.1.2.4      delta
223.1.3.2      epsilon
223.1.4.2      iota
```

O endereço IP é a primeira coluna, e o nome do computador é a segunda coluna.

Em muitos casos, você pode instalar arquivos "hosts" idênticos em todos os computadores. Você pode notar que só existe uma entrada para "delta" no arquivo, mesmo ele tendo 3 endereços IP. Delta pode ser alcançado com qualquer dos seus endereços IP; não importa se apenas um é usado. Quando delta recebe um pacote IP e olha o endereço de destino, ele reconhece qualquer dos seus endereços IP.

Também podem ser dados nomes a redes IP. Se você possui 3 redes IP, seu arquivo "networks"¹⁷, que documenta esses nomes, poderia se parecer com algo assim:

```
223.1.2      desenvolvimento
223.1.3      contabilidade
223.1.4      fabrica
```

O número IP da rede está da primeira coluna, e o nome, na segunda.

A partir deste exemplo, você pode ver que alfa é o computador número 1 da rede desenvolvimento, beta é o computador número 2 da rede desenvolvimento e assim por diante. Você também pode dizer que alfa é "desenvolvimento.1", beta é "desenvolvimento.2", e assim por diante.

O arquivo "hosts" acima é adequado para usuários, mas o gerente da rede provavelmente substituirá a linha para delta por:

```
223.1.2.4      devnetrouter      delta
223.1.3.1      facnetrouter
223.1.4.1      accnetrouter
```

Essas três novas linhas para o arquivo "hosts" toma, para cada endereço IP de delta, um nome

¹⁶ Basendo-se no UNIX. Por exemplo, até hoje, o arquivo que mantém a tradução local de nome para endereço no Linux é /etc/hosts.

¹⁷ Idem; nos Linux de hoje, por exemplo, o arquivo é /etc/networks.

significativo. De fato, o primeiro endereço IP listado possui 2 nomes; “delta” e “devnetrouter” são sinônimos. Na prática, “delta” é o nome de propósito geral para o computador, e os outros 3 nomes são usados somente quando da administração da tabela de roteamento IP.

Esses arquivos são usados pelos comandos de administração de rede e aplicações de rede para fornecer nomes significativos. Eles não são requeridos para a operação na internet, mas tornam essa operação mais fácil para nós.

5.6 Tabela de Roteamento IP

Como o IP sabe qual interface inferior usar quando envia um pacote IP para fora do computador? O IP olha na tabela de roteamento usando uma chave de procura do número IP da rede, que foi extraído do campo endereço IP de destino.

A tabela de roteamento contém uma linha para cada rota. As colunas primárias da tabela de roteamento são: número IP da rede, flag direto/indireto, endereço IP do roteador, e número da interface. A tabela é consultada pelo IP para cada pacote IP de saída.

Em muitos computadores a tabela de roteamento pode ser modificada com o comando “route”. O conteúdo da tabela de roteamento é definido pelo gerente de rede, pois é o gerente de rede quem atribui os endereços IP aos computadores.

5.7 Roteamento Direto em Detalhes

Para explicar como ele é usado, vamos olhar em detalhes as situações de roteamento que revimos anteriormente.

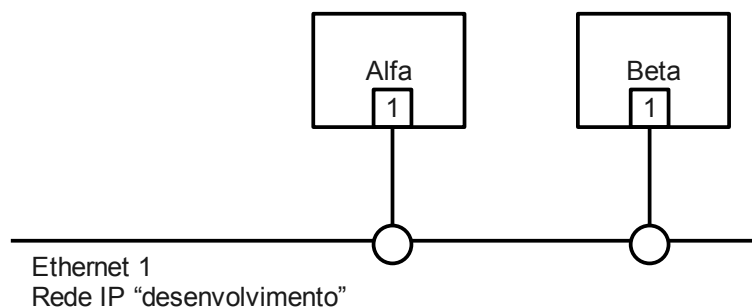


Figura 8: Visão superficial da uma rede IP

A tabela de roteamento dentro de alfa se parece com essa:

Rede	Flag direto/indireto	Roteador	Número da interface
desenvolvimento	direto	<em branco>	1

Tabela 8: Exemplo de tabela de roteamento simples

Esta tabela pode ser vista em muitos sistemas UNIX¹⁸ com o comando “netstat -r”. Com esta rede

¹⁸ Como o Linux, por exemplo.

simples, todos os computadores possuem tabelas de roteamento idênticas.

Para discussão, a tabela é impressa novamente, porém sem o número da rede traduzido para seu nome.

Rede	Flag direto/indireto	Roteador	Número da interface
223.1.2	direto	<em branco>	1

Tabela 9: Exemplo de tabela de roteamento simples

5.8 Cenário Direto

Alfa está enviando um pacote IP para beta. O pacote IP está no módulo IP de alfa, e seu IP de destino é beta, ou 223.1.2.2. O IP extrai a porção de rede deste endereço IP e faz uma varredura na primeira coluna da tabela, olhando por uma correspondência. No caso dessa rede, ele encontrou uma correspondência na primeira entrada.

As outras informações na entrada indicam que computadores nessa rede podem ser alcançados diretamente através da interface número 1. A tabela ARP termina a tradução para o endereço IP de beta, e então o quadro Ethernet é enviado diretamente para beta via interface número 1.

Se uma aplicação tenta enviar um dado para um endereço IP que não está na rede desenvolvimento, o IP será incapaz de procurar uma correspondência na tabela de roteamento. O IP então descarta o pacote IP. Muitos computadores fornecem uma mensagem de erro “Rede não alcançável”.

5.9 Roteamento Indireto em Detalhes

Agora, vamos dar uma olhada mais de perto em um cenário de roteamento mais complicado do que o que examinamos anteriormente.

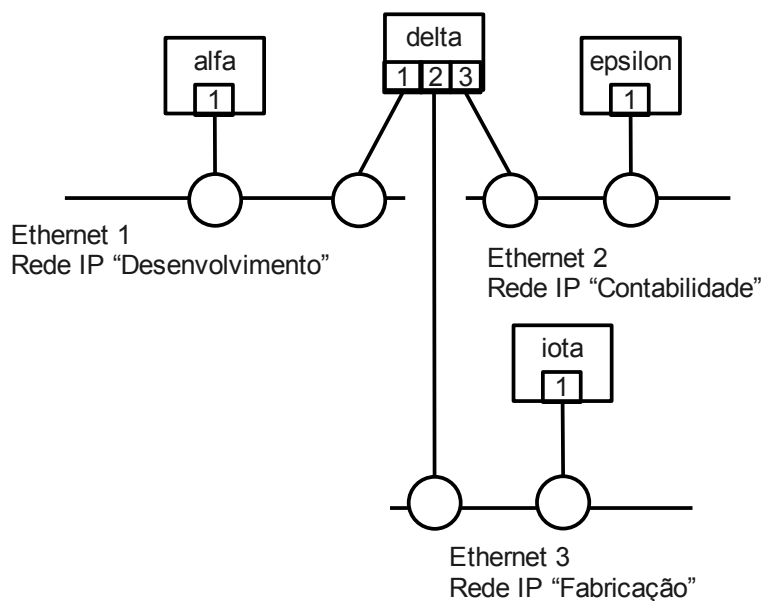


Figura 9: Visão superficial de três redes IP

A tabela de roteamento dentro de alfa se parece com isso:

Rede	Flag direto/indireto	Roteador	Número da interface
desenvolvimento	direto	<em branco>	1
contabilidade	indireto	devnetrouter	1
fabricação	indireto	devnetrouter	1

Tabela 10: Tabela de roteamento de alfa

Para discussão, a mesma tabela é impressa novamente usando número em vez de nomes:

Rede	Flag direto/indireto	Roteador	Número da interface
223.1.2	direto	<em branco>	1
223.1.3	indireto	devnetrouter	1
223.1.4	indireto	devnetrouter	1

Tabela 11: Tabela de roteamento de alfa com números

O roteador na tabela de roteamento de alfa é o endereço IP da conexão de delta à rede desenvolvimento.

5.10 Cenário Indireto

Alfa está enviando um pacote IP para epsilon. O pacote IP está no módulo IP de alfa e o endereço IP

de destino é epsilon (223.1.3.2). O IP extrai a porção de rede do endereço IP (223.1.3) e faz uma varredura na primeira coluna da tabela, olhando por uma correspondência. Uma correspondência é encontrada na segunda entrada.

Esta entrada indica que os computadores na rede 223.1.3 podem ser alcançados através do roteador IP devnetrouter. O módulo IP de alfa então faz uma tradução na tabela ARP pelo endereço IP de devnetrouter e envia o pacote IP diretamente para devnetrouter através da interface número 1 de alfa. O pacote IP conterá o endereço de destino de epsilon.

O pacote IP chega à interface de delta na rede desenvolvimento e é passado para o módulo IP de delta, acima. O endereço IP de destino é examinado, e porque ele não corresponde com qualquer dos endereços IP de delta, delta decide por encaminhar o pacote IP.

O módulo IP de delta extrai a porção da rede do endereço de destino IP (223.1.3) e faz uma varredura na tabela de roteamento por uma ocorrência no campo rede. A tabela de roteamento de delta se parece com isso:

Rede	Flag direto/indireto	Roteador	Número da interface
desenvolvimento	direto	<em branco>	1
fabricação	direto	<em branco>	3
contabilidade	direto	<em branco>	2

Tabela 12: Tabela de roteamento de delta

Abaixo, a tabela de roteamento é impressa novamente, sem a tradução para nomes.

Rede	Flag direto/indireto	Roteador	Número da interface
223.1.2	direto	<em branco>	1
223.1.3	direto	<em branco>	3
223.1.4	direto	<em branco>	2

Tabela 13: Tabela de roteamento de delta com números

A correspondência é encontrada na segunda entrada. IP então envia o pacote IP diretamente para epsilon através da interface número 3. O pacote IP contém o endereço de destino IP de epsilon e o endereço de destino Ethernet de epsilon.

O pacote IP alcança epsilon e é passado para o módulo IP de epsilon, acima. O endereço de destino IP é examinado, e então o pacote IP é passado para a camada de protocolos superior.

5.11 Sumário de Roteamento

Quando um pacote IP viaja através de uma internet grande, ele pode passar por muitos roteadores IP antes que ele alcance o destino. O caminho que leva não é determinado por uma origem central,

sendo o resultado da consulta de cada tabela de roteamento usadas na viagem. Cada computador define apenas o próximo salto na viagem, e confia que o próximo computador a enviar o pacote IP agirá da mesma maneira.

5.12 Gerenciando os Roteadores

Manter corretas as tabelas de roteamento em todos computadores em uma internet grande é uma tarefa difícil; a configuração de rede é modificada constantemente pelos gerentes de rede, a fim de atender as mudanças necessárias. Enganos nas tabelas de roteamento podem bloquear a comunicação¹⁹ de forma que são dolorosamente tediosos para diagnosticar.

Mantendo uma configuração de rede simples, segue-se um longo caminho em direção a criação de uma internet confiável. Por exemplo, o método mais direto para atribuição de redes IP à Ethernet é atribuir um número de rede IP único para cada Ethernet.

Ajuda também está disponível a partir de certos protocolos e aplicações de rede. ICMP (Internet Control Message Protocol - Protocolo de Controle de Mensagens da Internet) pode reportar muitos problemas de roteamento. Para pequenas redes, a tabela de roteamento é preenchida manualmente em cada computador pelo administrador de rede. Para redes grandes, o administrador de rede automatiza a operação manual por meio de um protocolo de roteamento²⁰ para distribuir rotas através da rede.

Quando um computador é movimentado de uma rede IP para outra, o endereço IP deve mudar. Quando um computador é removido de uma rede IP, seu endereço antigo torna-se inválido. Essas mudanças requerem atualizações frequentes nos arquivos "hosts". Este pequeno arquivo pode tornar-se difícil para manter até mesmo em redes de tamanho médio. O Sistema de Nomes de Domínios (DNS) ajuda a resolver esse problema.

6 User Datagrama Protocol

UDP é um dos dois protocolos que residem no topo do IP. Ele oferece serviço para aplicações de rede dos usuários. Exemplos de aplicações de rede que usam UDP são: Network File System (NFS - Sistema de Arquivos de Rede) e Simple Network Management Protocol (SNMP - Protocolo de Gerenciamento de Redes Simples). O serviço é pouco mais que uma interface para o IP.

UDP é um serviço de entrega de datagrama não orientado à conexão, que não garante entrega. O UDP não mantém uma conexão fim a fim com o módulo UDP remoto; ele meramente empurra o datagrama para fora do computador através da rede e aceita datagramas entrantes que vêm da rede.

O UDP adiciona dois valores aos que são providos pelo IP. Um é a informação de multiplexação entre aplicações baseado no número de porta. O outro é uma soma de verificação para checar a integridade dos dados.

6.1 Portas

Como um cliente em um computador alcança o servidor em outro?

¹⁹ Segunda ocorrência de "Mistakes block communication".

²⁰ Um dos protocolos de roteamento existentes em 1991 era o RIP v1.

O caminho da comunicação entre uma aplicação e o UDP é através de portas UDP. Essas portas são numeradas, começando-se de zero. Uma aplicação que oferece serviço (o servidor) aguarda por mensagens vindas em uma porta dedicada específica ao serviço. O servidor aguarda pacientemente por qualquer cliente que lhe requerer serviço.

Por exemplo, o servidor SNMP, chamado de agente SNMP, sempre aguarda na porta 161. Só pode haver um SNMP por computador, já que ele usa somente a porta UDP número 161. Esse número de porta é bem conhecido; ele é um número fixo, um número atribuído da internet. Se um cliente SNMP procura serviço, ele envia requisições para a porta número 161 do UDP no computador destino.

Quando uma aplicação envia um dado para fora através do UDP, ele chega na extremidade como uma única unidade. Por exemplo, se uma aplicação faz 5 escritas na porta UDP, a aplicação na extremidade fará 5 leituras a partir da porta UDP. Além disso, o tamanho de cada escrita corresponde ao tamanho de cada leitura.

O UDP preserva o limite da mensagem definido pela aplicação. Ele nunca junta duas mensagens de aplicação seguidas ou divide uma mensagem de aplicação única em partes.

6.2 Soma de verificação

Um pacote IP entrante com um campo "tipo" no cabeçalho IP indicando UDP é passado acima, para o módulo UDP, pelo IP. Então o módulo UDP recebe o datagrama UDP a partir do IP, e examina a soma de verificação UDP. Se a soma de verificação for zero, significa que a soma de verificação não foi calculada pelo remetente e pode ser ignorada. Isso significa que o módulo UDP do computador remetente pode ou não gerar somas de verificação. Se a Ethernet é a única rede entre os dois módulos UDP comunicantes, então você não precisa de somas de verificação. Todavia, é recomendado que a geração de somas de verificação esteja sempre habilitada, já que em algum ponto no futuro uma mudança na tabela de roteamento pode enviar dados através de uma mídia de baixa confiabilidade.

Se a soma de verificação é válida (ou zero), o número da porta de destino é examinado; e se uma aplicação está vinculada a essa porta, uma mensagem de aplicação é enfileirada para que a aplicação a leia. De outra maneira, o datagrama UDP é descartado. Se os datagramas UDP entrantes chegam mais rapidamente do que a aplicação pode ler, e se a fila é preenchida ao valor máximo, os datagramas UDP são descartados pelo UDP. O UDP continuará a descartar datagramas UDP até que haja espaço na fila.

7 Transmission Control Protocol

TCP provê um serviço diferenciado do UDP. TCP oferece um fluxo de bytes orientados para conexão, em vez de serviço de entrega sem conexão. TCP garante entrega, ao passo que o UDP, não.

TCP é usado por aplicações de rede que requerem entrega garantida e não se incomodam com tempos esgotados e retransmissões. As duas aplicações de redes mais comuns que usam TCP são o File Transfer Protocol (FTP - Protocolo de Transferência de Arquivos) e o TELNET. Outras

aplicações TCP populares incluem o sistema X-Window²¹, rcp (cópia remota) e os comandos da família "r-". A grande capacidade do TCP não funciona sem custo: ele requer mais CPU e largura de banda na rede. As entranhas do módulo TCP são bem mais complicadas do que as do módulo UDP.

De forma semelhante ao UDP, aplicações de rede TCP conectam-se a portas TCP. Números de portas bem definidos são dedicados para aplicações específicas. Por exemplo, o servidor TELNET usa a porta número 23. O cliente TELNET pode procurar o servidor simplesmente conectando-se a porta 23 do TCP no computador especificado.

Quando a aplicação inicia usando TCP, o módulo TCP no computador cliente e o módulo TCP no computador servidor comunicam-se um com o outro. Esses dois módulos TCP terminais contém informação de estado que definem um circuito virtual. Este circuito virtual consome recursos em ambos os terminais TCP. O circuito virtual é *full duplex*²²; dados podem ir em ambas as direções simultaneamente. As aplicações escrevem dados na porta TCP; esses dados atravessam a rede e são lidos pela aplicação na extremidade.

O TCP empacota o fluxo de bytes da forma que quiser; ele não mantém os limites entre os dados. Por exemplo, se uma aplicação faz 5 escritas na porta TCP, a aplicação no outro lado poderia fazer 10 leituras para pegar todos os dados. Ou ela poderia pegar todos os dados em uma única leitura. Não há correlação entre o número e tamanho das escritas de um lado e o número e tamanho das leituras do outro lado.

TCP é um protocolo de janela deslizante, com esgotamento de tempo e retransmissões. Dados que saem devem ser confirmados pelo TCP pela outra ponta. Confirmações podem ser carregadas dentro dos dados. Ambos os terminais podem controlar o fluxo um do outro, deste modo prevenindo um estouro de buffer.

Como em todos os protocolos de janela deslizante, este protocolo tem um tamanho de janela. O tamanho da janela determina a quantidade de dados que podem ser transmitido antes que a confirmação seja requerida. Para o TCP, essa quantidade não é um número de segmentos TCP, e sim um número de bytes.

8 Aplicações de Rede

Porque tanto o TCP quanto o UDP existem, em vez de apenas um ou outro?

Eles fornecem serviços diferentes. Muitas aplicações são implementadas para usar um ou outro. Você, o programador²³, escolhe o protocolo que melhor atende a suas necessidades. Se você precisa de um serviço de entrega de fluxo confiável, o TCP pode ser melhor. Se você precisa de um serviço de datagrama, o UDP pode ser melhor. Se você precisa de eficiência sobre circuitos de caminho longo, o TCP pode ser melhor. Se você precisa de eficiência sobre redes rápidas com baixa latência, o UDP pode ser melhor. Se você não precisa cair em alguma dessas categorias, então a "melhor" escolha não está clara. Porém, aplicações podem ser criadas para suprir as deficiências de uma escolha. Por exemplo, se você escolhe UDP e precisa de confiabilidade, então a aplicação deve

21 Hoje em dia, X.Org

22 Isto é, de via dupla.

23 Na época, ser programador era uma honra, pois as pessoas que entendiam de informática tinham prazer em colocar a mão na massa. Infelizmente hoje a moda é ser engravatado, fazer diagramas e documentar, em vez de programar.

prover confiabilidade. Se escolhe TCP e precisa de um serviço orientado a registros, então a aplicação deve inserir marcadores no fluxo de bytes para delimitar registros.

Quais aplicações de rede estão disponíveis?

Essa lista é muito grande. O número está crescendo continuamente. Muitas das aplicações existem desde o início da tecnologia internet: TELNET e FTP. Outras são relativamente novas: X-Window e SNMP. A seguir, uma breve descrição das aplicações mencionadas neste tutorial.

8.1 TELNET

TELNET oferece uma capacidade de login remoto sobre TCP. A operação e aparência é similar ao teclado de discagem através de uma central telefônica. Na linha de comando o usuário digita "telnet delta" e recebe um prompt de comando do computador chamado "delta".

TELNET trabalha bem; ele é uma aplicação antiga e tem uma interoperabilidade generalizada. Implementações do TELNET normalmente trabalham em sistemas operacionais diferentes. Por exemplo, um cliente TELNET por estar em um VAX/VMS e o servidor em um Unix System V.

8.2 FTP

O File Transfer Protocol (FTP - Protocolo de Transferência de Arquivos), que é tão antigo quanto o TELNET, também usa TCP e tem uma interoperabilidade generalizada. A operação e aparência é como se você entrasse por TELNET em um computador remoto. Mas em vez de digitar seus comandos usuais, você deve se contentar com uma pequena lista de comandos para listar diretórios e coisas assim. Comandos FTP permitem que você copie arquivos entre computadores.

8.3 rsh

Remote Shell (rsh ou remsh - Shell Remoto) é apenas um entre uma família de comandos UNIX estilo remoto. O comando copy do Unix, o cp, torna-se rcp. O comando "quem está logado em", who, torna-se rwho. A lista continua e é referida coletivamente como comandos da família "r", ou os comando "r*" (r asterisco).

Os comandos r* trabalham principalmente entre sistemas UNIX, sendo designados para interação entre hospedeiros confiáveis. É dada pouca consideração à segurança, mas ele provê um ambiente conveniente ao usuário.

Para executar o comando "cc file.c" no computador remoto chamado delta, digite "rsh delta cc file.c". Para copiar o arquivo "file.c" para delta, digite "rcp file.c delta:". Para logar em delta, digite "rlogin delta", e se você administrou os computadores de uma certa maneira, você poderá não ser apresentado a um prompt pedindo sua senha.

8.4 NFS

Network File System (Sistema de Arquivos de Rede), primeiramente desenvolvido pela Sun Microsystems Inc, usa o UDP e é excelente para montar sistemas de arquivos Unix em múltiplos computadores. Uma estação de trabalho sem disco pode acessar o disco rígido do servidor, como se

o disco estivesse localmente na estação de trabalho. Uma única cópia do disco para o banco de dados do mainframe "alfa" pode ser usado pelo mainframe "beta", se o sistema de arquivos do banco de dados está montado com o NFS em "beta".

NFS adiciona uma carga significativa a uma rede, possuindo uma usabilidade pobre em enlaces lentos, mas os benefícios são enormes. O cliente NFS é implementado no kernel²⁴, permitindo que todas as aplicações e comandos usem o disco NFS montado como se ele fosse um disco local.

8.5 SNMP

Simple Network Management Protocol (SNMP - Protocolo Simples de Gerenciamento de Rede) usa UDP e é designado para uso pelas estações centrais de gerenciamento de rede. É um fato bastante conhecido que, se dados insuficientes forem dados, um gerente de rede pode detectar e diagnosticar problemas de rede. As estações centrais usam SNMP para coletar esses dados a partir de outros computadores na rede. O SNMP define o formato dos dados; ele prepara-os de uma forma que uma estação central ou um gerente de rede os interprete.

8.6 X-Window

O X Windows System usa o protocolo X-Window sobre TCP para desenhar janelas em exibidores bitmap de estações de trabalho. X Window é muito mais que um utilitário para desenhar janelas; ele é uma filosofia inteira de modelagem de uma interface com o usuário.

9 Outras Informações

Muita informação sobre tecnologia internet não está incluída neste tutorial. Esta seção lista informações que são considerada o próximo nível de detalhes para o leitor que deseja aprender mais.

- Comandos administrativos: arp, route, e netstat
- ARP: entrada permanente, entrada pública, entrada com tempo esgotado, spoofing²⁵
- Tabela de roteamento IP: entrada de hospedeiro, gateway padrão²⁶, subredes
- IP: contador time-to-live²⁷, fragmentação, ICMP
- RIP, loops de roteamento
- Domain Name System

24 Isto é, o núcleo do sistema operacional; o que ele quer dizer é que não há necessidade de instalar o NFS, pois o próprio sistema operacional (no caso, os Unix da época, e hoje em dia, o Linux por exemplo) traz suporte nativo ao NFS; quer dizer também que, do ponto de vista das aplicações e dos comandos, o NFS se comporta de forma transparente.

25 Spoofing é uma técnica de explorar uma vulnerabilidade das redes, que consiste em falsificar o endereço Ethernet de origem.

26 Gateway padrão hoje em dia é definido como o roteador de próximo salto que os hospedeiros usam para encaminhar pacotes para fora da rede.

27 Tempo de vida (time-to-live, TTL) é o conceito que especifica quando um pacote deve ser descartado, baseado no número de saltos que ele já efetuou.

10 Referências

1. Comer, D., "Internetworking with TCP/IP Principles, Protocols, and Architecture", Prentice Hall, Englewood Cliffs, New Jersey, U.S.A., 1988.
2. Feinler, E., et al, DDN Protocol Handbook, Volume 2 and 3, DDN Network Information Center, SRI International, 333 Ravenswood Avenue, Room EJ291, Menlow Park, California, U.S.A., 1985.
3. Spider Systems, Ltd., "Packets and Protocols", Spider Systems Ltd., Stanwell Street, Edinburgh, U.K. EH6 5NG, 1990.

11 Relação com outras RFCs

Esta RFC é um tutorial, e não pode ser ATUALIZADA ou se tornar OBSOLETA por qualquer outra RFC.

12 Considerações de Segurança

Existem considerações de segurança dentro da suíte de protocolos TCP/IP. Para muitas pessoas essas considerações são problemas sérios, para outras não são; isso depende dos seus requerimentos de usuário.

Esse tutorial não discute essas questões, mas se você quer aprender mais, poderia começar com o tópico Spoofing ARP, eentão ir à seção "Considerações de Segurança" na RFC 1122, que irá conduzi-lo a mais informações.

13 Endereço dos Autores

Theodore John Socolofsky

Spider Systems Limited

Spider Park

Stanwell Street

Edinburgh EH6 5NG

United Kingdom

Phone:

from UK 031-554-9424

from USA 011-44-31-554-9424

Fax:

from UK 031-554-0649

from USA 011-44-31-554-0649

EMail: TEDS@SPIDER.CO.UK

Claudia Jeanne Kale
12 Gosford Place
Edinburgh EH6 4BJ
United Kingdom

Phone:

from UK 031-554-7432

from USA 011-44-31-554-7432

EMail: CLAUDIAK@SPIDER.CO.UK

14 Tradução, comentários e ilustrações

Esta é uma tradução não oficial da RFC para o português, e, como tal, não garantimos a absoluta integridade com a RFC original. O objetivo desta tradução é ajudar aos interessados no assunto. Em caso de dúvida, a RFC original deve ser consultada.

As ilustrações foram refeitas.

Os comentários não fazem parte da RFC original, sendo introduzidos para esclarecer algum trecho que julgou-se necessário.

A tradução foi feita por:

Gustavo Lopes de Oliveira Santos

Abril, 2010

Email: gustavolopes@planoemfoco.com

Acesse o Blog do Plano em Foco! <http://blog.planoemfoco.com>