INTERCONEXÃO DE REDES e o PROTOCOLO IP

Fundamentos

8 jan 2005
Fabio Montoro

O objetivo deste artigo é revisitar os conceitos básicos associados ao protocolo IP, parte do conjunto de protocolos conhecido como TCP-IP, e os protocolos de roteamento, responsáveis pela interconexão de redes, da forma mais clara e objetiva possível, com uma visão voltada para os cenários práticos das redes corporativas.

O artigo está didaticamente organizado em uma sequência tal que o torna apropriado a cursos introdutórios sobre o protocolo IP, cursos básicos na área de redes de computadores e tecnologia da informação e comunicações, treinamentos para técnicos e material de referência em treinamentos sobre esses assuntos.

É recomendável avaliar se esta matéria deve ser ministrada após um curso básico sobre rede local Ethernet, ou uma revisão do assunto, onde o estudante tenha assimilado os conceitos básicos de comunicação na camada 2 do modelo OSI, tais como protocolos de enlace, detecção e correção de erros, tecnologia Ethernet, comutação e multiplexação de dados etc.

CONTEÚDO

PARTE 1 INTERCONEXÃO DE REDES LOCAIS 3

1.1 Introdução 3
1.2 *Bridge* 7
1.3 Roteador 10

1.3.1 Conexões básicas com roteadores 13
1.3.2 Portas do roteador 15
1.3.3 Cabos seriais 16

1.3.4 Princípios do roteamento 18
1.3.5 Arquitetura interna do roteador 20
1.3.6 Atualização do software do roteador 22

PARTE 2 PROTOCOLO IP 23

2.1 Introdução 23
2.2 Pacote IPv4 23
2.3 Fragmentação 25
2.4 TOS – Tipo de Serviço 25
2.5 Compressão de dados 26
2.6 Endereçamento IP 27
2.7 Translação de endereços - NAT 29
2.8 Sub-redes IP 30
2.9 Máscara de sub-rede IP 30
2.10 *Broadcast* 32
2.11 *Multicast* 32
2.11.1 IGMP 33
2.11.2 PIM 33

PARTE 3 PROTOCOLOS DE ROTEAMENTO IP 34
3.1 Protocolo RIP 36
3.2 Protocolo OSPF 39

PARTE 4 CONFIGURAÇÃO DO ROTEADOR 41
4.1 Definição dos endereços IP 41
4.2 Configuração dos endereços no roteador 43
4.3 Definição de rotas no roteador 44
4.4 Sumarização de rotas 45
4.5 Máscara de comprimento variável 46

1 INTERCONEXÃO DE REDES LOCAIS

1.1 INTRODUÇÃO

As redes de computadores vêm sendo classificadas em categorias que estão associadas à funcionalidade ou tecnologia empregada. Na verdade as redes de computadores servem a muitos outros dispositivos além do que se entende por um "computador" tradicional. Podemos ver a rede de computador como uma rede de elementos que se comunicam, independentemente da função ou atividade de cada um. Dizemos que um elemento está em rede quando ele participa da comunidade, recebendo ou enviando mensagens a outros elementos, ou seja, quando ele se comunica.

As categorias tradicionais, e mais comuns, de redes, são: a "rede local" (LAN - Local Area Network) e a "rede de longa distância", (WAN - Wide Area Network).

Há diversas definições para LAN e WAN, sendo que algumas geram polêmicas e não especificam bem o limite entre os dois tipos. Na busca de uma definição que fosse a mais sucinta e exata possível, cheguei a uma que utiliza simplesmente a extensão geográfica da rede, associada ao ambiente de trabalho, com fator diferencial:

> Rede local de computadores é aquela que abrange, no máximo, a área de um prédio.

Alguns autores consideram que dois prédios próximos, interligados, formam uma única rede local. Halsall[1] admite que a rede local pode abranger um prédio ou um grupo de prédios, no entanto não apresenta um limite claro para a extensão da rede. Pela definição sugerida aqui, podemos considerar que são duas redes locais interligadas, quando ela abranger mais de um prédio, independente da forma da interligação utilizada. Stalings[2] diz que uma rede local é aquela onde os dispositivos se encontram dentro de uma "pequena área" (small area). A definição apresentada por Soares[3] é semelhante e utiliza a expressão "pequena região". Tanembaum[4], na segunda edição traduzida, não apresenta exatamente uma definição, mas sim três aspectos característicos da rede local, dentre eles, que a LAN possui "um diâmetro de apenas alguns quilômetros". Enfim, definir nem sempre é fácil. Me parece que a definição apresentada aqui é independente do estado da arte dos equipamentos envolvidos e menos suscetível a polêmicas.

---

[1] HALSALL, FRED; "**Data Communications, Computer Networks and Open Systems**", Fourth Edition, Addison Wesley, Harlow, England, 1996.

[2] STALLINGS, WILLIAM; "**Local and Metropolitan Area Networks**", ", Macmillan Publishing, New York, USA, 1993.

[3] SOARES, LUÍS FERNANDO, LEMOS, GUIDO E COLCHER, SÉRGIO; "**Das LANs e WANs às Redes TAM**", Editora Campus, Rio de Janeiro, RJ, 1995.

[4] TANEBAUM, ANDREW S.; "**Redes de Computadores**", Traduzido da 2ª Ed. Americana, Campus, Rio de Janeiro, RJ, 1994.

Outro conceito que merece ser lembrado é a divisão das tarefas envolvidas em uma comunicação, em atividades hierarquicamente organizadas, chamadas de "camadas", onde cada camada tem suas "responsabilidades". Dessa forma a comunicação completa se faz por vários protocolos organizados em camadas onde cada uma delas tem funções específicas e uma forma definida de se relacionar com as camadas adjacentes. O modelo mais comentado é o OSI. A organização internacional ISO[5] definiu um modelo de relacionamento entre os diversos protocolos que regem uma comunicação, conhecido como modelo OSI (Open Systems Interconnection)[6]. O modelo OSI possui 7 camadas, conforme ilustra a figura 1.1. As camadas são conhecidas pelo nome ou pelo número que representa sua posição na pilha.

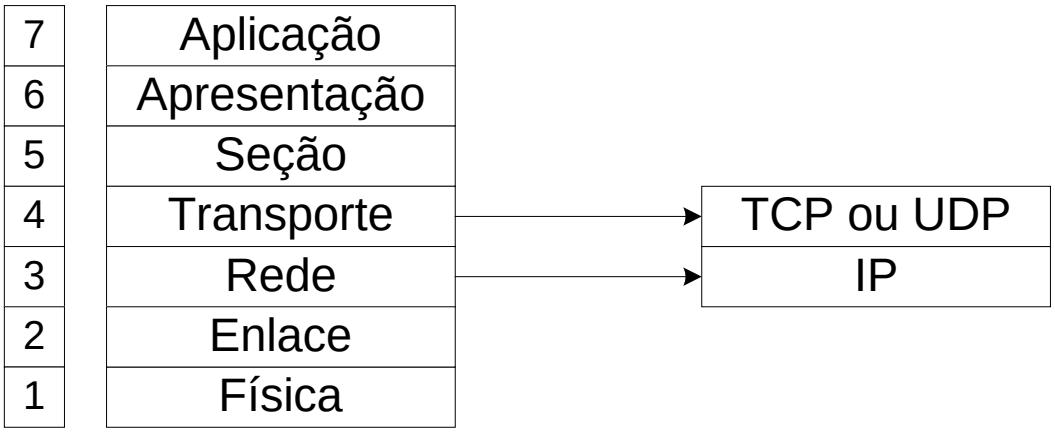


Fig. 1.1: modelo OSI

A ideia do modelo OSI, ou o conceito das 7 camadas, se tornou uma referência de estrutura para os protocolos de comunicação, sendo amplamente utilizada, principalmente no que se refere ao nome e número das camadas. No entanto, a estrutura de uma comunicação não necessariamente utiliza as sete camadas. O TCP-IP, por exemplo, pode ser visto como uma estrutura de 4 ou 5 camadas, onde o aplicativo (camada 7), como por exemplo o HTTP, SMTP, TELNET, DHCP etc, ficam diretamente sobre a camada de transporte (camada 4), UDP ou TCP.

A figura 1.2 mostra a relação entre as camadas do modelo OSI e a estrutura do TCP/IP, em dois exemplos: uma rede local utilizando Ethernet e uma conexão de longa distância utilizando o Frame Relay.

O protocolo Ethernet, outro exemplo, abrange duas camadas, a 1 e a 2, definindo aspectos das interfaces física e elétrica, bem como de transmissão e conexão do enlace.

---

[5] International Organization for Standartization. Organização internacional com sede em Genebra, Suiça. www.iso.ch

[6] Em 1983 a ISO publicou o trabalho intitulado "The Basic Reference Model for Open Systems Interconnetion"

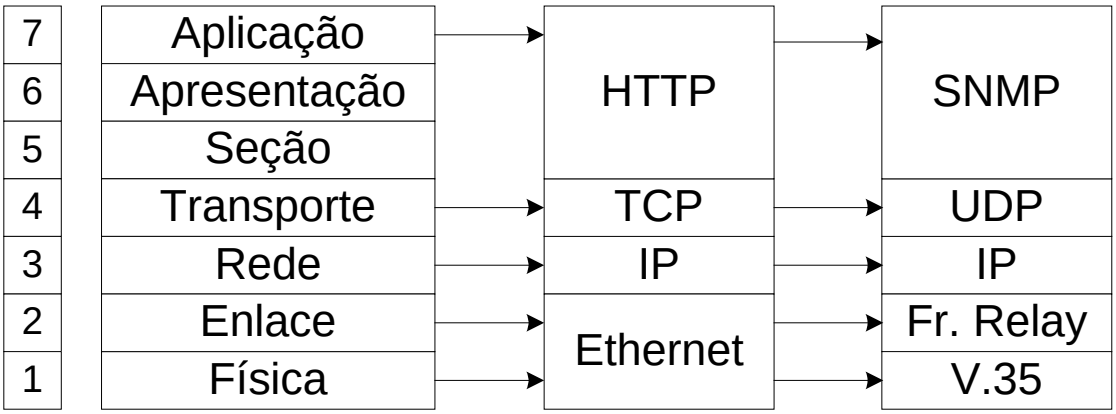


Fig. 1.2: TCP-IP e o modelo OSI

Refira-se à figura 1.3. O pacote do protocolo da camada superior é encapsulado no campo de dados do pacote da camada imediatamente inferior conforme a estrutura de uma comunicação utilizada. Dessa forma todas as informações do protocolo da camada superior, incluindo seus dados e informações de controle, são transportadas de forma transparente pelo protocolo da camada inferior.

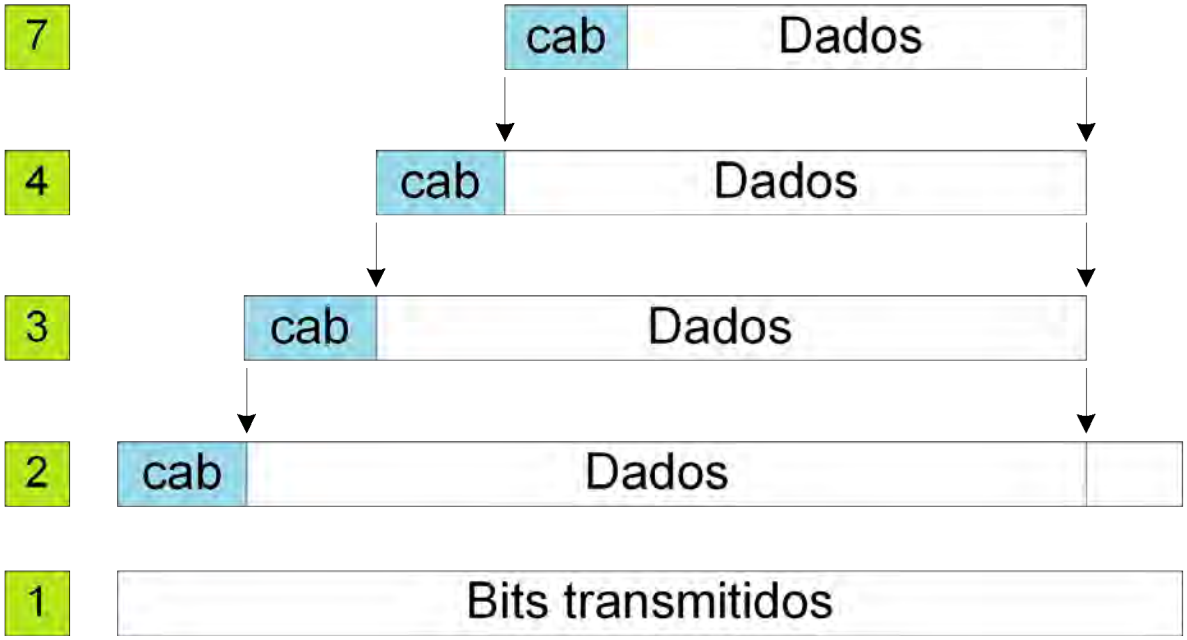


Fig. 1.3: encapsulamento

Os cabeçalhos, indicados por "cab" na figura 1.3, são próprios de cada protocolo na respectiva camada, ou seja, eles são diferentes. Os cabeçalhos contêm as informações de controle necessárias do protocolo a que pertence, tais como endereços do remetente e do destinatário, campos indicando prioridades, etc

Neste artigo abordaremos os princípios de comunicação entre elementos de rede utilizando o protocolo IP (camada de rede, camada 3). Veremos também os protocolos TCP e UDP (camada de transporte, camada 4) e alguns protocolos de aplicação (camada 7) que, juntos com IP, formam o pacote chamado “TCP-IP”.

A camada de rede é a responsável pelo conhecimento dos endereços dos elementos, ou estações da rede, e as possíveis rotas a serem utilizadas nas comunicações.

Vamos considerar, daqui por diante, que estações pertencentes a uma mesma rede local, ou a redes locais distintas, se comunicam utilizando o IP como protocolo de camada de rede, ou seja, toda estação que deseja se comunicar envia seus dados encapsulados em pacotes IP.

A interconexão entre duas redes locais, situadas em localidades distintas, tem por objetivo tornar os recursos de uma, disponíveis às estações da outra e vice-versa.

Para efetivar essa interconexão, é necessário, antes de mais nada, que haja um canal de dados de longa distância entre as duas localidades: um meio dedicado direto, como por exemplo um enlace Ethernet via fibra ótica, um enlace rádio, um enlace em par trançado com modems HDSL, ou uma rede comutada como a rede telefônica, ISDN, uma rede Frame Relay, uma rede TCP-IP etc.

Em seguida, com exceção do enlace Ethernet, que pode ser considerado como uma extensão da rede local, as demais alternativas precisarão de um par de equipamentos de rede (A e B na figura 1.4) que encaminhe os pacotes IP para a rede de longa distância (WAN) – esse equipamento de rede converterá o protocolo Ethernet das redes locais em um protocolo de enlace que opere na interface serial, que é a saída para a rede WAN.

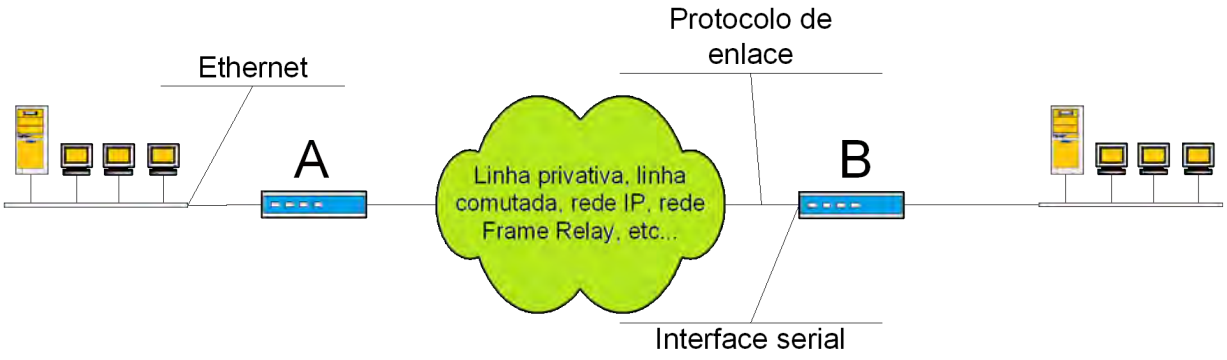


Fig. 1.4: interconexão de duas redes locais

As interfaces seriais (camada física) mais comumente utilizadas nas redes WAN são: EIA-232 e V.35. Os equipamentos de rede, “A” e “B”, ilustrados na figura 1.4, devem ter, no mínimo, uma interface Ethernet e uma serial.

Há duas funções básicas que podem ser executadas pelos equipamentos A e B, ao encaminhar os pacotes IP são: Bridging ou Roteamento.

O equipamento que executa a função “bridging” é chamado de bridge e o equipamento que executa a função “roteamento” é chamado de roteador. Em geral os roteadores também executam a função “bridging”.

Alguns autores utilizam o termo “ponte”, tradução literal de bridge, entretanto, neste artigo, preferi utilizar o termo original do inglês, já consagrado pela comunidade de redes.

Adotaremos neste artigo a palavra “pacote” para denotar o conjunto de bits de dados que são transmitidos juntos, de forma independente, por um protocolo, qualquer que seja o protocolo ou a camada a que ele pertença. Em geral o pacote Ethernet é chamado de frame, mas aqui o chamaremos de “pacote Ethernet”.

Em uma rede local Ethernet, cada dispositivo possui um endereço próprio e único, denominado MAC (***M**edia **A**ccess **C**ontrol address*), que já vem definido de fábrica.

1.2 BRIDGE

A função bridging interliga dois segmentos de rede local preservando os endereços da camada Ethernet, ou seja, cada segmento de rede toma conhecimento dos endereços Ethernet do outro.

Ao equipamento que executa especificamente a função bridging dá-se o nome de “bridge transparente” ou simplesmente “bridge”. Em geral os roteadores também executam a função bridging.

A bridge comuta os pacotes camada 2 entre duas de suas portas e, por isso, também é chamada de “comutador Ethernet” ou “switch”.

A bridge mais simples é aquela que possui duas interfaces Ethernet.

A especificação IEEE 802.1 define as funções e o modo de operação de uma bridge e considera o seguinte:

- Cada porta da bridge lê todos os pacotes Ethernet recebidos.
- O equipamento deve armazenar o endereço MAC do remetente desses pacotes em uma tabela. A tabela deve conter o endereço MAC e a porta na qual o pacote foi recebido.
- Para transmitir um pacote, o equipamento deve consultar a tabela e verificar em qual porta está o endereço MAC do destinatário.
    - ✓ Se o endereço constar da tabela, transmite o pacote somente pela respectiva porta.
    - ✓ Se o endereço não constar da tabela, transmite o pacote em todas as portas.
    - ✓ Se a porta for a mesma pela qual chegou o pacote, este será descartado.

A bridge possui um buffer de saída em cada porta a fim de manter os pacotes a serem transmitidos em fila de espera, caso necessário.

A bridge utilizada para interligar dois segmentos de rede local através de uma rede WAN é conhecida como “bridge remota” ou “bridge serial”. Na configuração mais simples, a bridge remota possui uma porta LAN (Ethernet), que se conecta ao segmento de rede, e uma porta WAN (interface serial), que se conecta ao equipamento de transmissão. Esse tipo de bridge adota um protocolo de enlace na porta serial, para garantir a integridade dos dados, que pode ser HDLC, Frame Relay ou PPP, por exemplo.

A aplicação da bridge remota é conectar dois segmentos de rede distantes mas seu funcionamento é similar ao da bridge local: ambas executam a função bridging

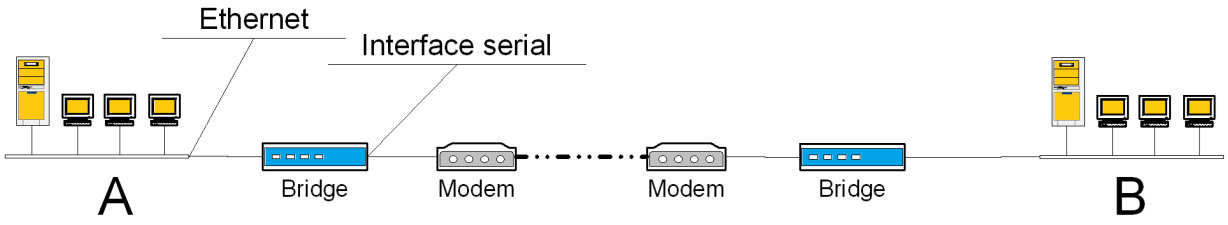


Fig. 1.5: bridge remota

A bridge remota, após concluir que deve transferir o pacote Ethernet para a interface serial, utiliza um protocolo de enlace WAN para enviar os dados.

Normalmente a porta serial tem uma velocidade mais baixa que a porta Ethernet. Se a bridge receber uma rajada de pacotes e seu buffer da porta serial não tiver capacidade para armazenar os pacotes a transferir, haverá perda de pacotes.

As bridges podem ter várias portas LAN e WAN.

Dois segmentos de rede, interligados por uma bridge, se comportarão como uma única rede local, ou seja, todos os usuários de um segmento terão acesso aos endereços Ethernet do outro segmento. Todos os broadcasts alcançarão as estações dos dois lados.

A bridge encapsula os pacotes Ethernet em pacotes de um protocolo de enlace WAN, por exemplo, o HDLC. Utiliza-se o termo “encapsular” quando o pacote do protocolo encapsulado é totalmente montado na parte de dados do protocolo encapsulante.

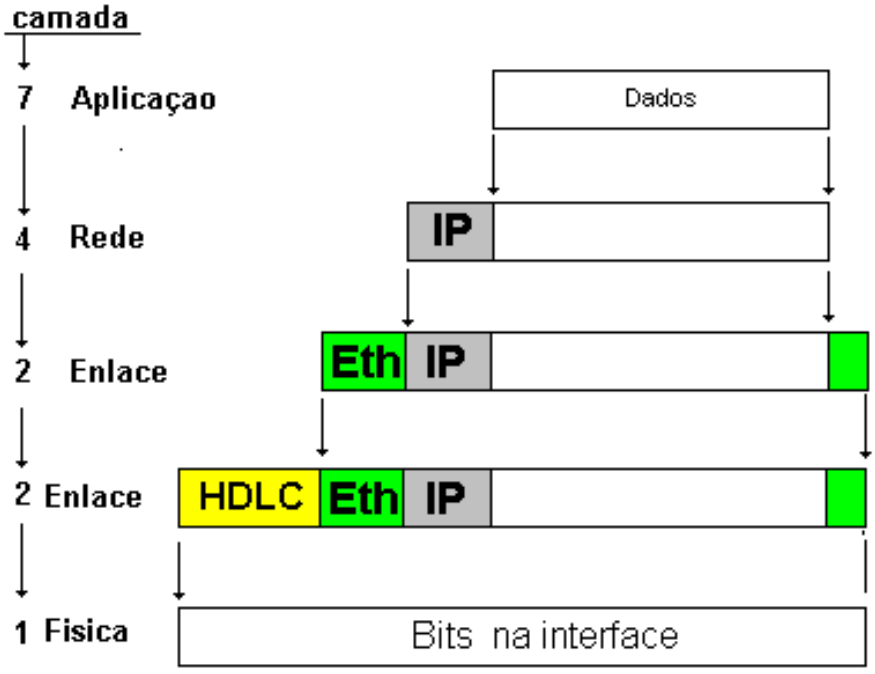


Fig. 1.6: Bridge remota: encapsula pacote da camada 2 em pacote da camada 2

O pacote HDLC é transmitido até a bridge na outra extremidade, que extrai o pacote Ethernet e o transmite em sua rede local. Então, as bridges transportaram o pacote Ethernet de uma rede para outra, sem qualquer manipulação adicional, preservando o endereço Ethernet .

Como o nome sugere, a bridge estabelece uma ponte entre as duas redes.

Digamos que uma estação da rede “A” transmita para uma estação da rede “B” (figura 1.3).

A figura 1.6 ilustra como os dados do protocolo da camada superior (camada 7) vão da estação transmissora até a saída serial da bridge: inicialmente os dados do protocolo superior são encapsulados, na estação transmissora, em um pacote IP; em seguida o pacote IP é encapsulado em um pacote Ethernet, ganhando um cabeçalho e um campo de paridade no final e é transmitido na rede local “A”; o pacote Ethernet trafega pela rede local até chegar na interface Ethernet da bridge; em seguida o pacote Ethernet é encapsulado pela bridge em um pacote HDLC, que é transmitido pela rede WAN pelo modem. Na recepção ocorre o processo inverso, em direção à estação receptora da rede “B”.

1.3 ROTEADOR

O roteador atua em uma camada superior à da bridge, na escala hierárquica dos protocolos: a camada de rede. O roteador recebe o pacote da camada 2 (Ethernet) e extai, de seu campo de dados, o pacote de nível superior (IP) e descarta o pacote da camada 2. O roteador verifica o endereço de destino no pacote camada 3, encapsula o pacote camada 3 em um pacote de protocolo camada 2 e o encaminha à interface correspondente.

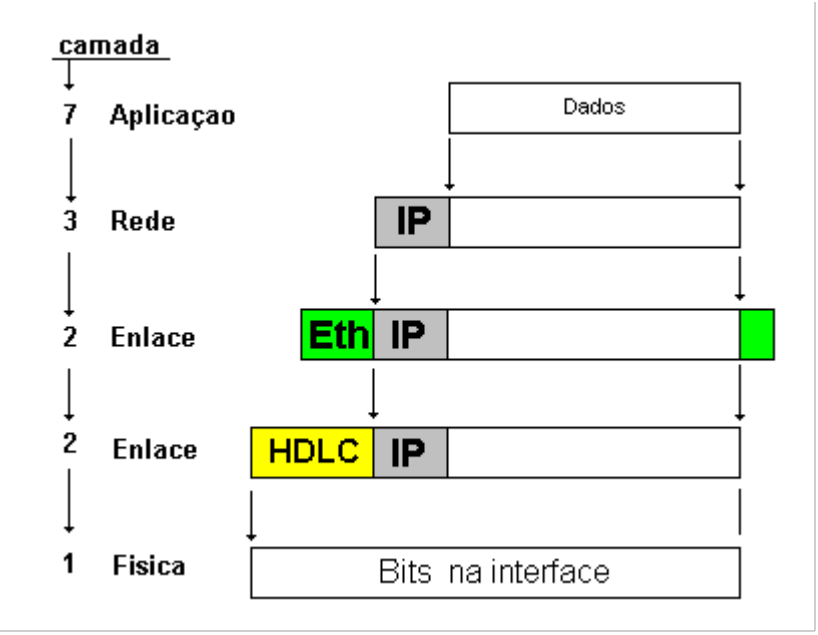


Fig. 1.7: o roteador monta pacote da camada 3 (IP) em pacote da camada 2 (HDLC)

Com o roteador há uma redução da quantidade de bits a transmitir, em relação à bridge, já que o overhead (cabeçalho e terminação) do Ethernet é descartado durante o encapsulamento no pacote de enlace, como demonstra a figura 1.7. Por outro lado, o roteador precisa ter capacidade de processamento suficiente para efetuar essa tarefa.

Suponhamos as duas redes “A” e “B” da figura 1.8, cada uma com suas estações: A1, A2, A3..., e B1, B2, B3.....etc, respectivamente. As duas redes estão ligadas por um roteador.

Suponha que a estação A1 deseja enviar dados para a estação B4. O aplicativo da estação A1 entrega os dados para o protocolo camada 3 (IP). O protocolo camada 3 monta um pacote colocando o endereço "B4" como destinatário e "A1" como remetente.

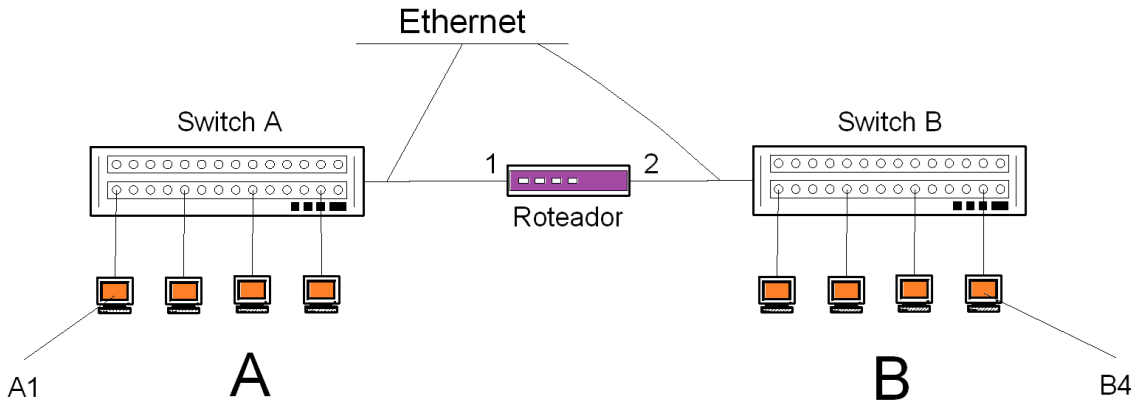


Fig. 1.8: roteador unindo duas redes locais LAN

O protocolo camada 3, que roda na estação A1, sabe que a estação "B4" fica fora da rede "A" e que deve enviar o pacote ao roteador da rede. Então o protocolo camada 2 residente em A1 monta um pacote Ethernet direcionando-o para o roteador (também chamado de *gateway*): no pacote Ethernet coloca "a1" como remetente e "r" como destinatário, onde “a1” e “r” são os endereços Ethernet da estação A1 e do roteador, respectivamente. A estação A1 então transmite o pacote Ethernet para o switch, que passa o pacote para a porta que está o roteador.

O roteador recebe o pacote pela porta Ethernet 1 e remove as informações da camada 2. Em seguida consulta sua tabela interna de roteamento e descobre que pacotes para a rede "B" devem ser enviados pela porta Ethernet 2.

O roteador sabe que o endereço "B4" da camada 3 corresponde ao endereço Ethernet "b4" na rede “B”. Então monta o pacote Ethernet colocando no cabeçalho "b4" como destinatário e "r" como remetente e joga na rede "B".

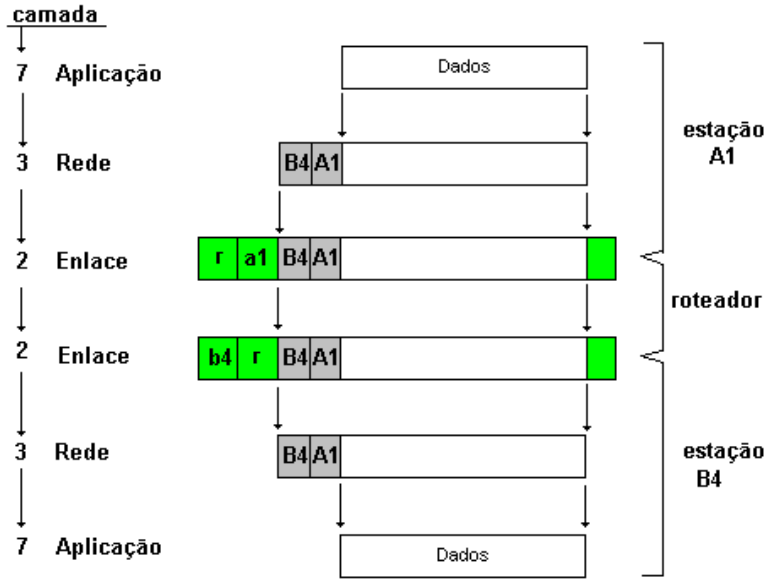


Fig. 1.9: encapsulamentos no roteador com saída LAN

Todas as estações da rede “B” recebem o pacote. A estação destinatária B4, através de seu protocolo camada 2, identifica que o pacote é dela, retira o cabeçalho de camada 2 e envia os dados para o protocolo da camada 3.

Finalmente, o protocolo camada 3 da estação "B4" passa os dados ao seu aplicativo.

A situação na qual o roteador interliga duas redes locais através de uma rede de longa distância é ilustrado pela figura 1.10. Compare esta figura com a figura 1.8.

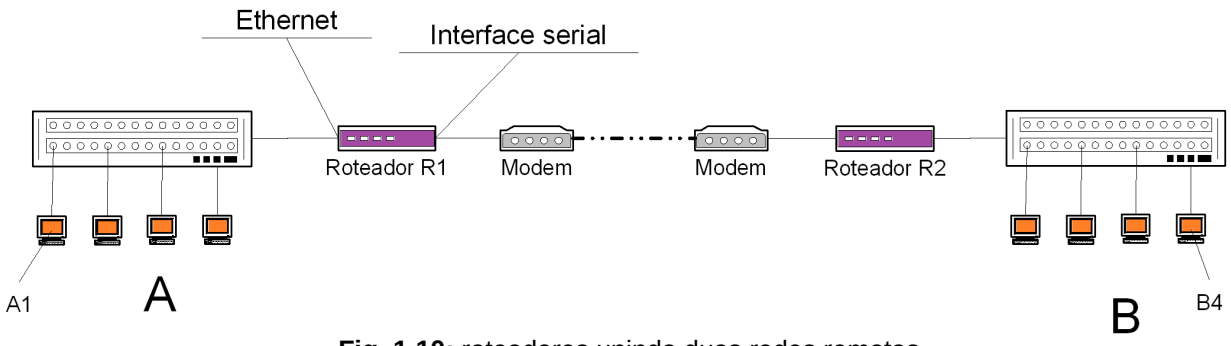


Fig. 1.10: roteadores unindo duas redes remotas

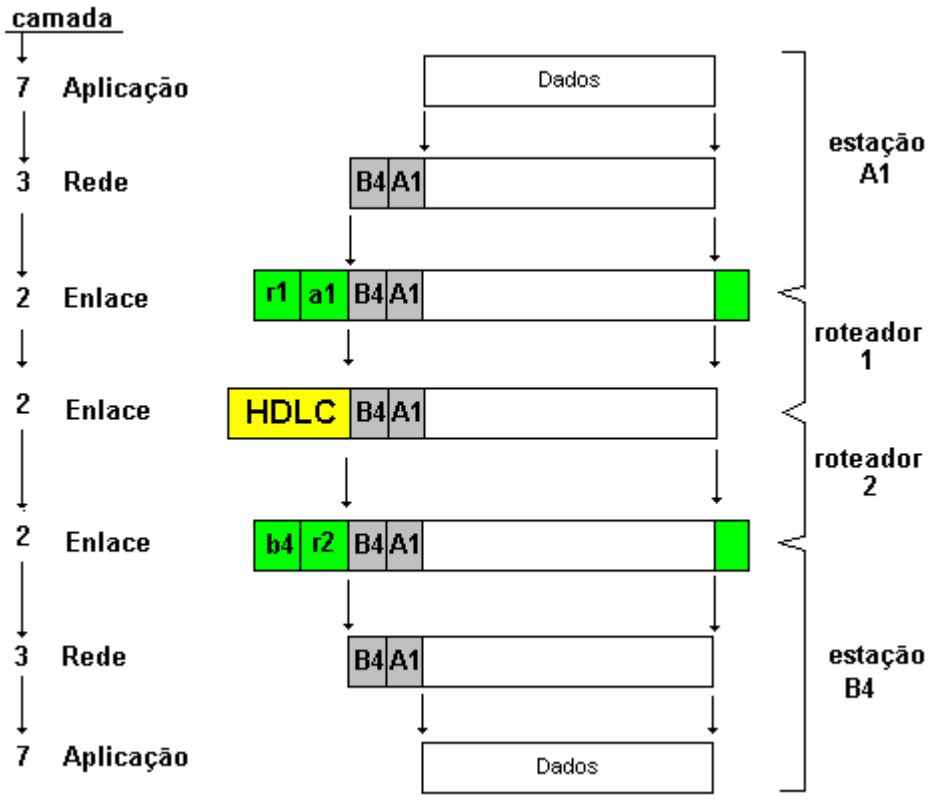


Fig. 1.11: encapsulamentos nos roteadores com saída WAN

A figura 1.11 mostra como ficam os encapsulamentos nesse caso, onde se utiliza roteadores com saída WAN. O roteador R1 extrai, analisa e encapsula os dados da camada 3 no pacote de enlace da porta WAN. Os campos de controle do pacote

camada de enlace anterior (Ethernet) são descartados. A bridge remota não analisa os dados da camada superior e simplesmente encapsula o pacote Ethernet inteiro no pacote de enlace WAN.

1.3.1 CONEXÕES BÁSICAS COM ROTEADORES

A alternativa mais simples é aquela onde dois roteadores se ligam por uma linha privativa (LP) por meio de equipamentos de transmissão como modems, por exemplo.

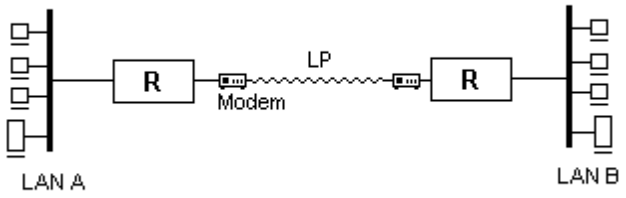


Fig.1.12: conexão de roteadores via LP.

Uma alternativa de conexão, para o caso de comunicação esporádica, é aquela em que os roteadores se ligam através da rede telefônica comutada. Quando o roteador tem dados a transmitir, aciona modem que disca para a localidade remota onde outro modem, configurado em resposta automática, atende e completa a conexão.

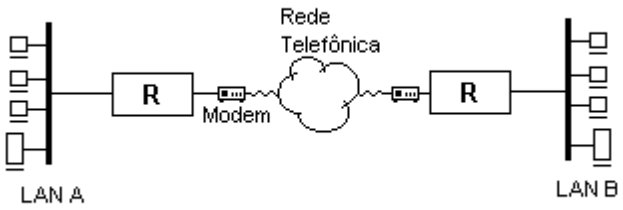


Fig.1.13: conexão de roteadores via linha discada.

Uma terceira alternativa de conexão utiliza redes públicas ou privativas de comutação de pacotes, como o Frame Relay, por exemplo.

Nesse caso cada localidade possui um roteador ligado a um modem, ou outro equipamento de transmissão, que tem acesso à rede através de uma LP (Linha Privativa). Essa alternativa estabelece uma rota virtual permanente entre os dois roteadores.

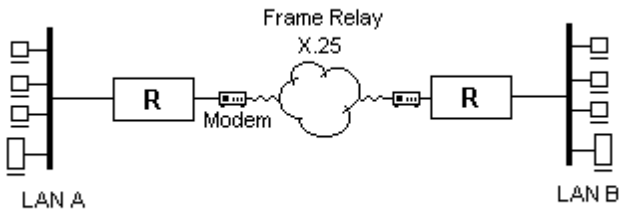


Fig.1.14: conexão de roteadores via rede de comutação de pacotes.

Uma quarta alternativa de conexão, resultante das anteriores, mas que tem muita aplicação na prática, é aquela que, além da conexão via rede de comutação de pacotes, possui também uma conexão via rede telefônica comutada ou ISDN. Nessa configuração podemos ter duas aplicações:

- Banda sob demanda
- Dial backup

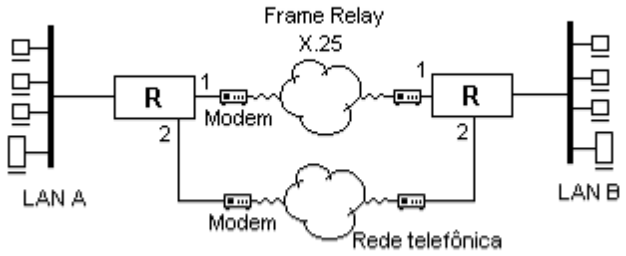


Fig.1.15: banda sob demanda e dial-backup

No caso da banda sob demanda, como ilustra a figura 1.15, o roteador vai acionar sua porta nº 2 se a porta nº 1 não conseguir dar vazão ao tráfego demandado.

No caso de dial backup, o roteador vai acionar sua porta nº 2 se o enlace da porta nº 1 cair (por problema no modem ou na linha). Nos dois casos a porta nº 2 aciona o modem local que disca para o remoto, configurado em resposta automática.

1.3.2 PORTAS DO ROTEADOR

A quantidade e os tipos de portas do roteador são suas características mais importantes. A próxima tabela ilustra um roteador típico, de pequeno porte.

Tabela 1.1: Portas de um roteador

Tipo de porta	Quantidade
Serial síncrona	3
Serial assíncrona	1
Ethernet 10 Mbps	1
Ethernet 100 Mbps	0

Cada porta possui algumas características técnicas que devem ser observadas. No caso das portas do tipo Ethernet, a velocidade máxima está associada ao padrão normativo: 10, 100 ou 1000 Mbps, normalmente para cabo tipo UTP (há também portas Ethernet para fibra ótica). No caso das portas seriais, o padrão e a velocidade de operação são as duas principais características.

A tabela 1.2 ilustra alguns exemplos de portas seriais, com valores típicos de velocidade oferecidos comercialmente.

Tabela 1.2: Exemplos de interfaces seriais

Padrão da interface / sincronismo	Faixa de Velocidades
V.24 com sincronismo interno	Até 28 kbps
V.24 com sincronismo externo	Até 80 kbps
V.35 com sincronismo interno	Até 1544 kbps
V.35 com sincronismo externo	Até 2048 kbps
V.24 assíncrono	Até 115 kbps

Pelo exemplo da tabela 1.2, nota-se que a velocidade máxima da interface pode depender do tipo de sincronismo utilizado.

É comum um fabricante dizer que seu roteador tem uma porta T1 ou E1, querendo com isso dizer que a porta opera até 1544 kbps ou 2048 kbps respectivamente.

Outros aspectos primários, físicos e elétricos dos roteadores disponíveis comercialmente, a serem considerados, constam na tabela 1.3.

Tabela 1.3: Aspectos primários importantes a observar nos roteadores

Aspecto	Comentários

Possui encaixes (slots) para placas opcionais com portas adicionais ?	*Slot* é um espaço do equipamento onde pode ser encaixado um módulo ou placa opcional para expandir a sua capacidade. Essa característica é importante se houver uma previsão de expansão.
Conector da porta exige cabo adaptador especial ?	Normalmente sim. Os roteadores e outros equipamentos de comunicação de dados possuem conectores menores em seu chassis (DB25, mini-DB26, mini-DB50, mini-DB68), a fim de acomodar diversas interfaces em um único conector do chassis. Assim a porta pode se conectar a diferentes interfaces apenas usando o cabo adaptador adequado.
Pode ser alimentado com 110 e 220 Volts de forma automática ?	Essa característica é importante no Brasil pois encontramos as duas alternativas.
Possui kit (orelhas) para instalar em *rack* ?	Alguns roteadores não vêm com esse acessório, que deve ser pedido separadamente.

1.3.3 CABOS SERIAIS

Como foi mencionado na tabela 1.3, normalmente os roteadores (e também outros equipamentos de comunicação) utilizam cabos seriais especiais que possuem um conector padronizado na extremidade que vai se conectar ao modem e um conector menor na extremidade que vai se conectar ao próprio roteador. Cada fabricante possui seus cabos proprietários. A extremidade que se conecta ao modem deve apresentar todas as características da interface padronizada que o cabo representa (físicas, elétricas e operacionais). Em geral o conector do lado do roteador possui mais pinos, permitindo que o usuário mude o tipo de interface do roteador apenas trocando o cabo. Essa facilidade de configuração física da interface é interessante mas nem todos os equipamentos a oferecem – alguns equipamentos exigem, além da troca do cabo, a troca de uma placa de interface interna.

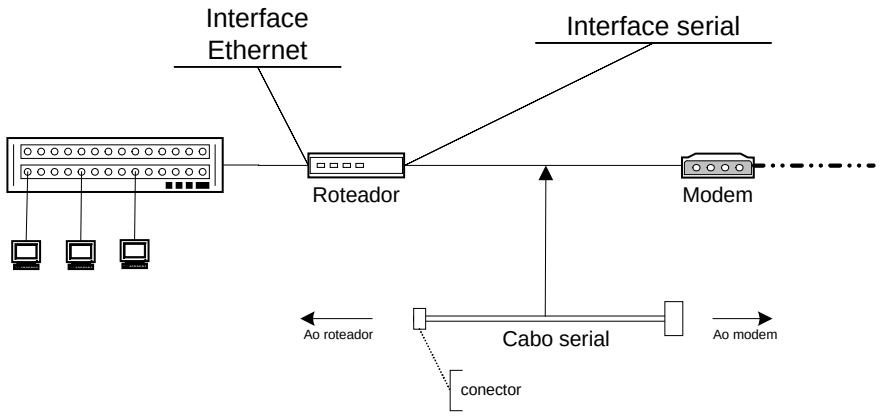


Fig.1.16: cabo serial

A tabela 1.4 mostra os padrões mais comuns de interface serial, qual norma define a especificação mecânica do conector, qual norma define a funcionalidade da interface, qual é o conector utilizado e quantos pinos ele possui.

Tabela 1.4: Padrões de interfaces seriais

Padrão	Mecânica	Funcional	Conector	Pinos
EIA/TIA-232	EIA232D	EIA232D	DB25	25
ITU-V.35	ISO2593	V35	M34	34
ITU-V.36	ISO4902	V36	DB37	37
ITU-X.21	ISO4903	X24	DB15	15
EIA/TIA-449	EIA449	EIA449	DB37	37
EIA/TIA-530	EIA530A	EIA530A	DB25	25
EIA/TIA-562	EIA232D	EIA232D	DB25	25

Além do aspecto do padrão, a interface pode estar configurada para se comportar como DCE (Equipamento de Comunicação de Dados) ou como DTE (Equipamento Terminal de Dados), com relação ao fluxo dos sinais. Alguns fabricantes possuem cabos diferentes para cada comportamento da interface, por exemplo: o fabricante pode ter um cabo V.35 DTE e outro V.35 DCE. Normalmente a interface do roteador opera no modo DTE e a do modem opera no modo DCE. Quem opera no modo DCE normalmente fornece o sinal de sincronismo.

É comum se conectar dois roteadores diretamente quando se deseja efetuar um teste ou configuração. Nesse caso um roteador deve se comportar como DTE e o outro como DCE e, então, deve-se usar dois cabos diferentes interligados como ilustra a fugura 1.17.

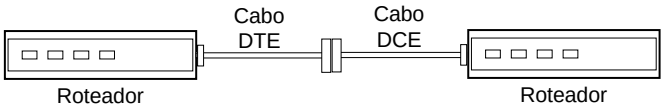


Fig.1.17: ligação direta entre dois roteadores

1.3.4 PRINCÍPIOS DO ROTEAMENTO

O roteamento é uma função da camada de rede (camada 3) e, portanto, o roteador opera de forma específica conforme o protocolo da camada de rede que deve ser roteado.

A função do roteador é remeter o pacote (camada de rede) para a rede destinatária e, portanto, precisa decidir em que direção deve enviar esse pacote. Se o roteador possui somente duas portas, como vimos até agora, a decisão é bem simples, mas, no caso geral, o roteador pode ter várias portas.

O roteador pode ser configurado de forma estática, com as rotas possíveis ou seguir um protocolo de roteamento que descubra as rotas possíveis negociando com os roteadores vizinhos e identificando as possíveis rotas. Durante essas negociações cada roteador "aprende" com seus vizinhos onde estão as outras redes. A figura 1.18 mostra 7 roteadores interligando 10 redes ("A" até "J").

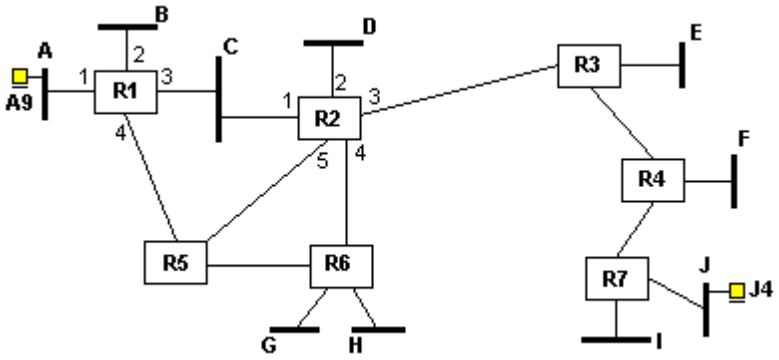


Fig. 1.18: Interligação de redes com roteadores

Se a estação A9 da rede "A" , envia um pacote ao roteador R1, destinado à estação "J4", da rede "J", como o roteador R1 vai saber para onde mandar esse pacote, supondo que o roteador R1 acaba de ser conectado à rede e foi ligado pela primeira

vez (ou seja, ele não possui essa informação armazenada ou configurada internamente) ?

Vamos representar os pacotes no formato <destinatário ; remetente>, em termos dos endereçamentos. Quando o roteador R1 recebe o pacote <J4;A9> ele deve decidir para onde enviar: para a rede “B”, pela porta 2, para o roteador R2 pela porta 3 ou para o roteador R5 pela porta 4.

Um dos objetivos do protocolo de roteamento é permitir que os diversos roteadores mantenham suas tabelas de roteamento, que indicarão para onde enviar o pacote recebido, após conhecer o endereço destino.

O roteador R1 toma imediatamente sua decisão se a rede destino constar em sua tabela de roteamento, que tem o aspecto mostrado a seguir, onde “métrica” é a distância até a rede destino medida em enlaces de camada 2.

Tabela 1.5: Tabela de roteamento de R1

Destino	Próximo roteador	Porta	métrica
A	Direto	1	1
B	Direto	2	1
C	Direto	3	1
D	R2	3	2
E	R2	3	3
F	R2	3	4
G	R5	4	3
H	R5	4	3
I	R2	3	5
J	R2	3	5

A viagem do pacote <j4;A9> terá as seguintes etapas:

1) O software de camada de rede, residente na estação A9, sabe que J4 reside fora da rede “A” porque seu endereço de rede indica outra rede. Então envia o pacote (encapsulado em um pacote Ethernet) ao roteador R1. Em geral se define um roteador (normalmente denominado *defaut gateway*) no software de rede da estação.
2) Ao receber o pacote Ethernet, o roteador R1 extrai o pacote camada 3 do pacote camada 2. Consulta sua tabela de roteamento e vê que deve enviá-lo ao roteador R2 pela porta 3.

3) Como a porta 3 é uma porta Ethernet, R2 encapsula o pacote camada 3 em um pacote Ethernet com o endereço MAC do roteador R2, e transmite na rede “C”.
4) O roteador R2 recebe o pacote Ethernet e extrai o pacote <J4;A9>. A partir desse ponto o processo vai se repetindo: R2, consultando sua tabela de roteamento, verifica que deve enviar o pacote ao roteador R3, pelo enlace serial da porta 3. Então R2 encapsula o pacote <J4;A9> em um pacote camada 2 (HDLC, por exemplo) e o transmite para R3.
5) O processo se repete até o pacote chegar a R7, que o encapsula em um pacote Ethernet e transmite pela rede “J” para o endereço MAC da estação J4.
6) A estação J4 recebe o pacote Ethernet de R7, extrai <J4;A9> e entrega ao protocolo camada 3.
7) O protocolo camada 3, residente na estação J4, nota que recebeu dados da estação A9, remotamente residente na rede “A”.

1.3.5 ARQUITETURA INTERNA DO ROTEADOR

Como a maioria dos equipamentos de comunicação de hoje, o roteador possui uma arquitetura interna baseada em um ou mais microprocessadores. Refira-se à figura 1.19. O bloco "Processador" representa a CPU do roteador, responsável pelo controle total do equipamento, que executa o programa de operação (também chamado de sistema operacional ou *firmware*) do roteador. O *firmware* fica residente em uma memória não volátil do tipo Flash (que pode ser regravada eletricamente). Quando se liga o equipamento, o *firmware* é transferido da Flash para uma memória RAM volátil, onde é executado (a RAM possui um tempo de acesso muito menor que o da Flash) – essa operação é conhecida como *bootstrap* ou simplesmente *boot* do equipamento. Uma outra memória RAM, não volátil, também chamada de NVRAM, é normalmente utilizada para guardar as configurações do roteador (alguns roteadores também guardam as configurações na Flash ou em EEprom). O bloco "IO" é composto dos circuitos de interfaces seriais, Ethernet, etc, com os ambientes externos. Excluindo-se aqueles muito pequenos, os roteadores normalmente possuem capacidade de receber módulos opcionais, que, por exemplo, podem adicionar portas extras ao modelo básico.

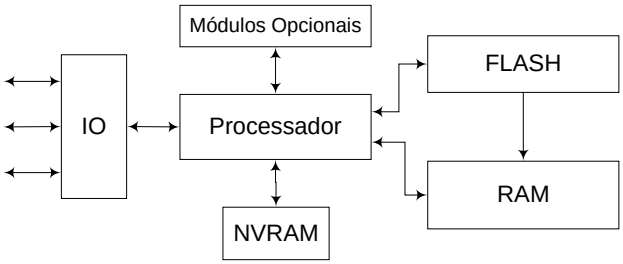


Fig. 1.19: Arquitetura interna do roteador

A memória RAM, além de abrigar o *firmware* em execução, também deve ter espaço para as filas de pacotes que chegam em cada uma de suas portas, para

armazenar informações temporárias utilizadas durante a operação, para guardar estruturas de dados, etc. Quanto maior for o espaço para as filas, menos pacotes serão perdidos por congestionamento do processador ou dos canais de saída. Quando o processador e o *hardware* associado estão operando em seu limite, ou os canais não conseguem dar vazão aos dados, os pacotes adicionais devem ficar esperando em filas, que ocupam memória RAM.

O espaço de RAM de um roteador, é um parâmetro importante, normalmente divulgado pelos fabricantes. O espaço de RAM necessário à operação do roteador, dentre outros aspectos, depende dos protocolos que estarão ativos.

Na memória Flash se armazena, além do programa executável, do roteador, outros arquivos de configuração, de ajuda (*help*), senhas, licenças de uso, etc. Outro parâmetro interessante é o espaço de memória Flash.

Há roteadores com RAM e Flash de tamanhos fixos, mas há também aqueles com possibilidade de expansão dessas memórias, a fim de incorporar novas facilidades, como processamento de protocolos especiais, voz, vídeo, etc.

A tabela 1.6 ilustra alguns exemplos de roteadores comercialmente disponíveis. A tabela mostra as quantidades de portas seriais, Ethernet (E), quantidade de portas de voz analógica (Va) e voz digital (Vd), espaços mínimo e máximo das memórias Flash e RAM, o processador principal utilizado e a capacidade de processamento em pacotes por segundo.

A performance do roteador vai depender, entre outros aspectos, de sua capacidade de processamento. Essa característica é usualmente divulgada pelos fabricantes para orientar o projetista a escolher o roteador com a capacidade adequada para a aplicação em questão.

A capacidade de processamento de um roteador normalmente também está associada à uma versão específica de software operacional.

Tabela 1.6: Exemplos de roteadores

Modelo	Portas				Flash [Mbyte]	RAM [Mbyte]	Processador	Capacidade [pps]
	Seriais	E	Va	Vd				
SDM-8200	1	1	-	-	1	4	Risc QUICC 25 MHz	800
VG320	1-3	1	0-4	-	2	4-12	Risc 68360	800
SDM-9350	4	1	0-4	-	2	4-8	Risc QUICC 25 MHz	900
SDM-8300	3	1	-	-	1	4-8	Risc 68360	1.000

Cisco 2501	1-4	2	-	-	8	4-16	68030 20MHz	1.000
Cisco 2610	0-8	1	-	0-30	8-16	24-64	MPC860 40 MHz	1.200
SDM-8300T	3	1	-	-	4	4-8	Risc i960	1.400
Cisco 3620	0-8	8	0-4	0-30	8-32	32-64	Risc R4700 80M	1.500
Cisco 3640	0-16	1	0-4	0-30	8-32	32-128	Risc R4700 100M	2.000
SDM-9360	2	1	0-8	0-30	8	4-16	MPC860 33 MHz	2.500
Cisco 3660	0-8	2	0-8	0-30	8-16	32-256	Risc RM5271 225M	4.000
SDM-9380	1-3	1	0-8	0-60	8-16	8	PPC 603e 266 MHz	10.000
Cisco 4500	0-12	1	-	-	4-16	16-32	Risc Orion 100 MHz	10.000

1.3.6 ATUALIZAÇÃO DO SOFTWARE DO ROTEADOR

Alguns roteadores possuem mais de um software operacional disponível comercialmente em virtude do fabricante oferecer opções de protocolos com os quais o roteador pode operar. Alguns protocolos menos comuns são fornecidos em imagens de software diferentes.

Ao longo da vida útil do equipamento o fabricante pode publicar novas versões de um determinado software, incorporando alterações e melhorias. Havendo interesse em atualizar o software do roteador (*upgrading*) para a nova versão, o responsável pela rede deverá providenciar o arquivo com o novo software (também chamado de imagem do software) e carregá-lo roteador. Na primeira vez que o roteador for desligado e ligado a nova versão do software entra em operação.

Há particularidades de fabricante para fabricante. Em geral é possível armazenar mais de uma imagem na memória Flash do roteador e definir qual imagem será utilizada pelo roteador após sua inicialização.

2 PROTOCOLO IP

2.1 INTRODUÇÃO

O IP (*Internet Protocol*) é um protocolo da camada de rede, que oferece um serviço do tipo datagrama não orientado a conexão, sem garantia de que o pacote transmitido vá chegar ao destino. Cada pacote transmitido é tratado independentemente - não há um controle da sequência dos pacotes, sendo possível receber pacotes IP fora da ordem em que foram transmitidos. O protocolo IP oferece um serviço não confiável. As principais especificações do protocolo IP constam na RFC-791 publicada em setembro de 1981, mas outras RFCs, como a RFC-1812 (Requisitos para Roteadores IPv4) de junho de 1995, também contém especificações sobre o protocolo IP.

O protocolo IP faz parte, juntamente com outros protocolos de Internet, do pacote conhecido como TCP-IP. As RFCs ou *Request For Comments* são os documentos oficiais do pacote TCP-IP e estão disponíveis na Internet[7].

Se, por acaso, um roteador (nó da rede) não puder tratar o pacote IP, ele o descarta e envia uma mensagem de erro ao nó remetente, utilizando o protocolo ICMP (*Internet Control Message Protocol*). O pacote ICMP é encapsulado em um pacote IP. Qualquer outra providência de tratamento de erro, fica por conta do protocolo de nível superior, como o TCP, por exemplo.

O protocolo IP, utilizado atualmente é conhecido como IPv4, ou versão 4. Uma versão mais recente, o IPv6, especificada na RFC-2460, de dezembro de 1998, foi criada para eliminar algumas limitações do IPv4. No entanto, o IPv4 é o padrão atual do mercado.

2.2 PACOTE IPV4

O pacote de dados do protocolo IP versão 4 é formado pelo cabeçalho (*header*) e pelos dados propriamente dito.

O cabeçalho pode ter de 20 a 60 bytes. O comprimento mínimo de 20 bytes é o normal. Há uma previsão para até 40 bytes de opções, que raramente são utilizadas.

A figura 2.1 mostra o pacote IP, onde os campos têm os seguintes significados:

Versão: versão do protocolo. Atualmente a versão é 4. Costuma-se chamar esse protocolo de IPv4. A nova versão, emergente, é o IPv6.

[7] Por exemplo: *www.cis.ohio-state.edu/cgi-bin/rfc/rfc-791.html*

Compr header: comprimento do cabeçalho, em conjuntos de 4 bytes. Como o campo possui apenas 4 bits, isso limita o comprimento do cabeçalho a 60 bytes.

TOS: tipo de serviço.

Comprimento Total do Pacote: comprimento total do pacote em bytes. Como esse campo possui 16 bits, teoricamente o pacote IP pode ter até 65535 bytes.

ID: identificação do pacote. Essa numeração é atribuída seqüencialmente a cada pacote gerado.

Flags: 3 bits de flags. Um dos bits indica se o pacote pode ser fragmentado.

Offset de fragmento: usado quando o pacote IP é um fragmento do pacote IP original. Indica a posição do fragmento, no seu pacote original, em passos de 8 bytes, sem contar o cabeçalho. Portanto, o menor fragmento deve ter 8 bytes.

TTL: *Time to Live*. Especifica a quantidade máxima de roteadores pelos quais o pacote pode passar. Cada roteador, por onde o pacote passa, decrementa esse campo de uma unidade. Quando o campo chega em zero o pacote é descartado.

Protocolo: este campo especifica qual protocolo está encapsulado no pacote IP. Alguns valores definidos são:

1 = ICMP
6 = TCP
8 = EGP (obsoleto)
17 = UDP
89 = OSPF

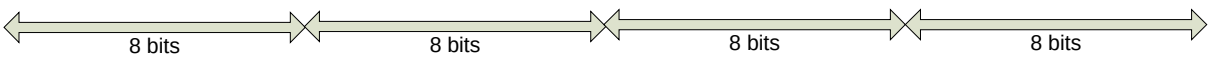
Checksum: assinatura de conferência do cabeçalho

Remetente: endereço do remetente

Destinatário: endereço do destinatário

Opções: Nem todos os equipamentos suportam esse campo, que é pouco utilizado.

Dados: campo de comprimento variável, que vai acomodar o pacote encapsulado ou um fragmento de um pacote IP original.



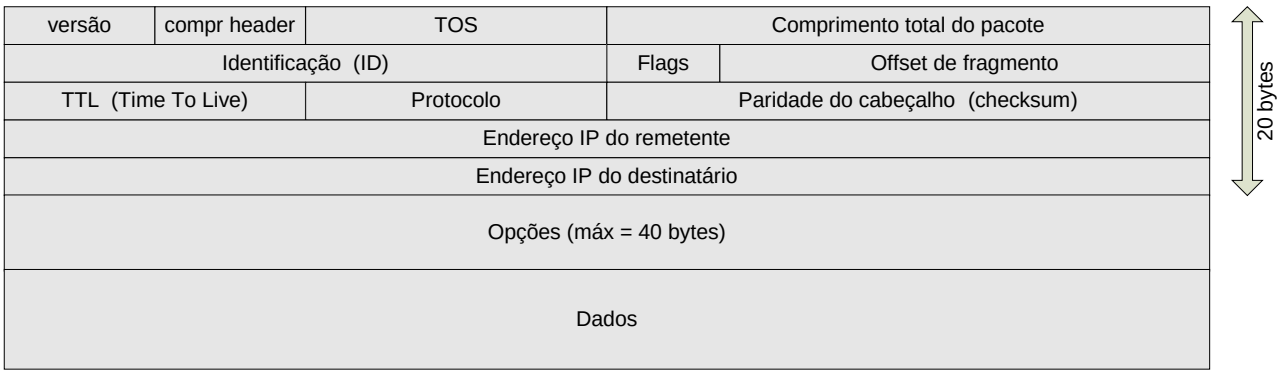


Fig. 2.1: Pacote do protocolo IPv4

2.3 FRAGMENTAÇÃO

Uma das principais características do protocolo IP é a capacidade de fragmentação: dividir o datagrama oriundo do protocolo da camada superior, de forma transparente a ele, para transmiti-lo sob a forma de vários pacotes IP, recompondo o datagrama original na recepção.

No trajeto o pacote IP pode encontrar redes onde há um limite para o tamanho do pacote. Por exemplo, o pacote Ethernet deve ter no máximo 1500 bytes no campo de dados. A esse limite dá-se o nome de MTU (*Maximum Transmission Unit*). Antes de transmitir dados por uma porta o roteador verifica qual é o MTU dessa porta e, se for o caso, fragmenta os dados. Uma vez fragmentado, o datagrama original só é recomposto em seu destino final.

Em uma comunicação IP os pacotes podem ser recebidos fora de ordem mas os pacotes resultantes de fragmentação são remontados corretamemente devido à informação de offset de fragmentação.

2.4 TOS - Tipo de Serviço

Esse campo do pacote IP tem a finalidade de permitir mecanismos de qualidade de serviço (QoS) nas redes. No protocolo IP há basicamente dois esquemas de QoS: um utiliza os três primeiros bits, chamados de *IP Precedence*, permitindo definir até 8 níveis de prioridade (0 a 7); o outro, conhecido como DiffServ, utiliza 6 bits e permite até 64 níveis de prioridade (0 a 63), ou DSCPs (*Differenciated Services Code Points*).

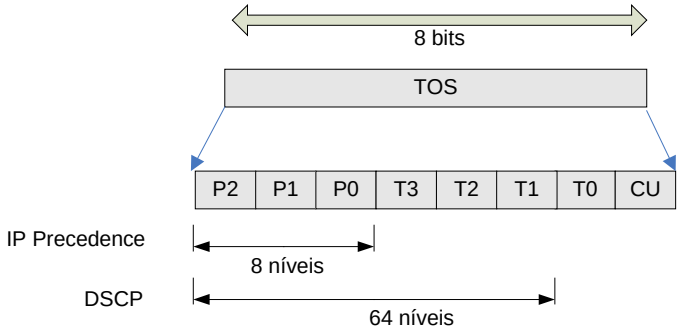


Fig. 2.2: Campo TOS

2.5 COMPRESSÃO DE DADOS

A compressão de dados é uma forma de aumentar a eficiência na transmissão. Há três formas básicas de compressão de dados para o protocolo IP:

- só do cabeçalho
- só dos dados
- dos dados e cabeçalho

A primeira opção faz a compressão somente do cabeçalho e só se torna interessante para pacotes com poucos dados.

A segunda faz somente a compressão dos dados, deixando os endereços em claro para serem interpretados nos nós de comutação intermediários.

A terceira faz a compressão de todo o pacote, o que exige um processamento adicional nos nós intermediários para resolver o cabeçalho e poder rotear o pacote.

Há duas formas básicas de se implementar a compressão: por software, na estação de trabalho ou no servidor, ou por firmware, no roteador. No caso da compressão ser implementada internamente ao roteador, normalmente ela deve ser executada por um processador rápido, do tipo DSP por exemplo, a fim de não impactar no desempenho do processador principal e, consequentemente, diminuir a performance do equipamento. Há diversos algoritmos no mercado.

A utilização da compressão normalmente é mais vantajosa para enlaces de maior velocidade, considerando o mesmo processador e que o tempo de processamento por pacote praticamente não muda, seja qual for a velocidade com que ele vai sair pela interface. A figura 2.3 mostra esse efeito, considerando o tempo de transmissão de 1024 pacotes com 513 bytes.

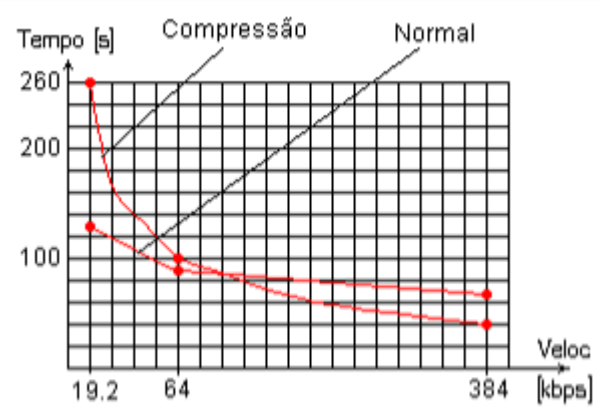


Fig. 2.3: Tempo de transmissão com e sem compressão

2.6 ENDEREÇAMENTO IP

Cada estação (também chamada de *host*) em um ambiente IP tem um endereço próprio. O endereço IP possui 32 bits, ou 4 bytes, e é dividido em 5 classes: A, B, C, D e E. As classes A, B e C são utilizadas para representar estações na rede, a classe D é usada para endereçamentos especiais de *multicasting* e a classe E é reservada.

O primeiro bit zero define a que classe pertence o endereço: se o primeiro bit zero estiver na posição 1, a classe é "A", se estiver na posição 2 é classe "B", etc.

O endereço possui duas partes: "*Net*", que é o endereço da rede e "*Host*", que é o endereço da estação. Conforme a classe, os espaços para Net e Host variam, como ilustra a figura 2.4.

A notação binária para o endereço IP nem sempre conveniente e por isso pouco utilizada na prática.

Normalmente o endereço é representado por 4 números decimais separados por um ponto. A tabela 2.1 mostra os endereços possíveis para cada classe. Os endereços de rede com todos os bits iguais (zero ou um) não são permitidos.

A quantidade máxima de hosts em uma rede é dada por $(2^n - 2)$, onde n é a quantidade de bits zero do campo destinado ao endereço do *host*.

Classe	Byte 1	Byte 2	Byte 3	Byte 4
A	0 Net (1 byte)	Host (3 bytes)		

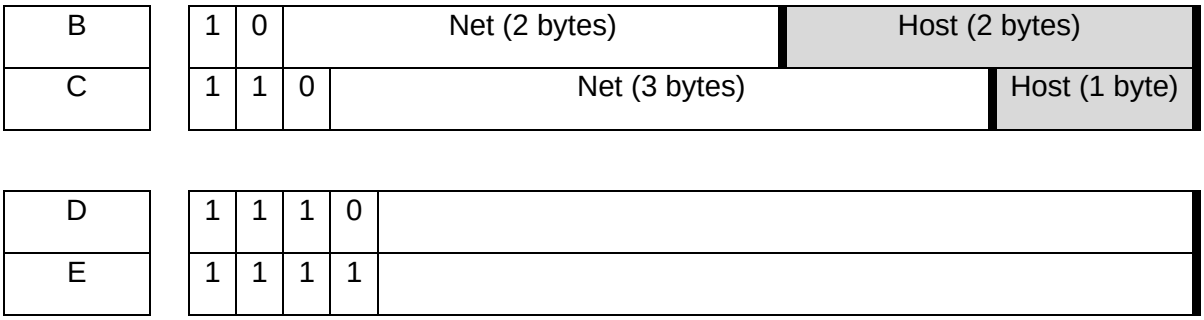


Fig. 2.4: Classes de endereços IP

Tabela 2.1: Capacidade de endereçamento IP por classe

Classe	Bits Net	Bits Host	Net Inicial	Net Final	Qtde Nets	Qtde Hosts
A	7	24	1.0.0.0	126.0.0.0	127	16.777.214
B	14	16	128.0.0.0	191.255.0.0	16.384	65.534
C	21	8	192.0.0.0	223.255.255.0	2.097.152	254
D	-	-	224.0.0.0	239.255.255.254	-	-
E	-	-	240.0.0.0	255.255.255.255	-	-

Exemplos:

Classe A 41.123.91.1 = 00101001.01111011.0101101.00000001

Classe B 129.12.12.12 = 10000001.00001100.00001100.00001100

Classe C 192.200.15.1 = 11000000.11001000.00001111.00000001

Quando se quer referir ao endereço de uma rede, escreve-se o número da rede seguido de zeros nas posições do endereço do *host*. Exemplos: redes 41.0.0.0, 129.12.0.0 e 192.200.15.0.

Há alguns endereços IP reservados para usos especiais e não podem ser utilizados como endereços comuns:

- 127.x.x.x é utilizado em testes locais de software
- Rede com tudo “1” ou tudo “0”
- Host número “0” significa o número da rede

- Host tudo “1” significa broadcast na rede específica e só pode ser usado como endereço destino.
- 0.0.0.0 significa rota defaut nas tabelas dos roteadores
- 255.255.255.255 significa broadcast a todos os host da minha rede.

Há outros endereços IP, segundo a RFC 1918, definidos para uso somente interno em redes privadas, não podem ser divulgados pela Internet. Esses endereços são inválidos na Internet:

- 10.0.0.0 até 10.255.255.255 classe A
- 172.16.0.0 até 172.31.255.255 classe B
- 192.168.0.0 até 192.168.255.255 classe C

Se uma empresa utilizar uma dessas faixas de endereços inválidos, internamente em sua rede, deve possuir um tradutor de endereços inválidos para endereços válidos a fim de se comunicar pela Internet. Um tradutor conhecido é o NAT (*Network Address Translation*), que será visto adiante.

2.7 TRANSLAÇÃO DE ENDEREÇOS - NAT

NAT, *Network Address Translation*, definida na RFC 1918, é uma operação que converte endereços inválidos, internos a uma rede, para endereços válidos, registrados, que circularão publicamente pela Internet. A operação de NAT é executada em um roteador de saída para a Internet. A grande vantagem do NAT é que a empresa precisa registrar somente a quantidade de endereços IP que vai utilizar na Internet, podendo estabelecer outro esquema para o endereçamento interno. Os provedores de acesso, por exemplo, se beneficiam bastante dessa operação. Uma consequência natural do NAT é que dificulta a identificação da fonte original do pacote.

O NAT pode ser estático ou dinâmico:

- Estático: Um para um, estabelece uma relação biunívoca entre pares de endereços internos e externos. O endereço privado corresponde a um endereço público. Essa modalidade deixa o dispositivo visível ao mundo externo.

- Dinâmico: Muitos privados para um público.

NAT dinâmico escolhe um endereço de uma lista de endereços válidos disponíveis e aloca para o endereço inválido que solicita a translação. Esse mapeamento é temporário e o mesmo IP interno pode receber outro IP válido na próxima requisição.

2.8 SUB-REDES IP

Chama-se de sub-rede, uma rede dentro de outra. Um subconjunto de estações com alguma característica comum que pertencem a um grupo de endereços IP. Essas estações podem estar em um mesmo domínio de colisão, ou não, se estiverem separadas por *switch*.

Para se formar uma sub-rede é preciso separar um determinado conjunto dos demais com um roteador.

A separação das sub-redes é física. Cada porta do roteador vai determinar uma sub-rede.

As classes A e B possuem um número muito grande para identificar *hosts* e isso fez surgir o conceito de sub-redes.

Com um determinado endereço de rede, o responsável divide o campo do endereço do *host* em duas partes: sub-rede e *host* propriamente.

Por exemplo, a figura 2.5 ilustra um endereço da classe B, com 16 bits para o endereço da rede, dividido em 62 sub-redes (6 bits, mas não pode usar tudo zero nem tudo um). Cada sub-rede pode ter até 1022 *hosts*.

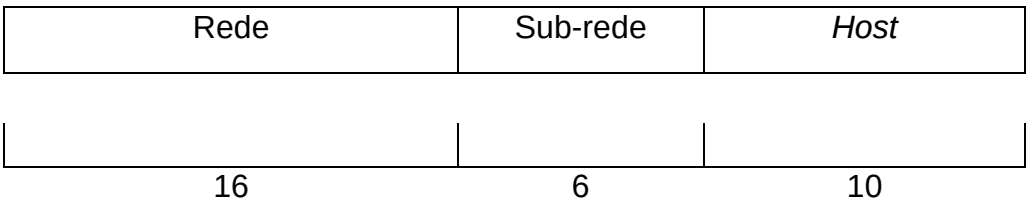


Fig. 2.5: Subdivisão do endereço da classe B

A divisão em sub-redes é extremamente útil em aplicações corporativas onde se deseja associar departamentos com um número de sub-rede. Com a aplicação de sub-redes as tabelas de roteamento nos roteadores ficarão mais reduzidas.

2.9 MÁSCARA DE SUB-REDE IP

A máscara de sub-rede é o recurso, utilizado no endereçamento IP, para que o roteador identifique uma sub-rede. A máscara é uma sequência de bits, do mesmo comprimento do endereço IP, com os bits de endereço de rede todos em “1” e os bits de identificação do *host* todos em “0”. O roteador faz uma operação lógica AND para determinar a sub-rede.

Por exemplo, uma sub-rede 200.14.20.32 com máscara 255.255.255.224:

11001000	00001110	00010100	001 00000
11111111	11111111	11111111	111 00000
255	255	255	224

rede

sub

host

Fig. 2.6: Exemplo de endereçamento com sub-rede

Pelo primeiro byte do endereço sabe-se que a rede é classe C (192 a 223). Então, o último byte deve designar o host. Como a máscara avança três bits no campo do host, sobram só 5 bits para o endereço do host e três bits para designar a sub-rede, permitindo um total de 7 sub-redes.

Utiliza-se a nomenclatura 200.14.20.32/27 para designar a subrede, onde "27" significa quantos bits "1" possui a máscara.

Tabela 2.2: Máscaras de subrede

		/	sub	Quantidade		
	máscara	bits =1	bits b	sub-redes 2^b	hosts B $2^{16-b}-2$	hosts C $2^{8-b}-2$
B	255.255.128.0	/17	1	2	32.766	-
	255.255.192.0	/18	2	4	16.382	-
	255.255.224.0	/19	3	8	8.190	-
	255.255.240.0	/20	4	16	4.094	-
	255.255.248.0	/21	5	32	2.046	-
	255.255.252.0	/22	6	64	1.022	-
	255.255.254.0	/23	7	128	510	-
	255.255.255.0	/24	8	256	254	-
	255.255.255.128	/25	9	512	126	-
	255.255.255.192	/26	10	1.024	62	-

	255.255.255.224	/27	11	2.048	30	-
	255.255.255.240	/28	12	4.096	14	-
	255.255.255.248	/29	13	8.192	6	-
	255.255.255.252	/30	14	16.384	2	-
C	255.255.255.128	/25	1	2	-	126
	255.255.255.192	/26	2	4	-	62
	255.255.255.224	/27	3	8	-	30
	255.255.255.240	/28	4	16	-	14
	255.255.255.248	/29	5	32	-	6
	255.255.255.252	/30	6	64	-	2

2.10 BROADCAST

Há três tipos de endereços IP: *Unicast*, destinado a um único *host*; *Multicast*, destinado a um grupo de *hosts* e *Broadcast*, destinado a todos os *hosts*.

Há dois tipos principais de *broadcast*:

- Limitado
- Direcionado (a rede ou a sub-rede)

O endereço destinatário utilizado quando se deseja emitir um *broadcast* limitado é “255.255.255.255”. Um pacote de *broadcast* limitado fica confinado a uma região sem sub-redes e não deve ser repassado por qualquer roteador.

O endereço destinatário utilizado no *broadcast* direcionado a uma rede possui todos os bits da identificação do *host* iguais a “1” e fica do tipo “rede.255.255.255” no caso de um endereço classe A, por exemplo.

O *broadcast* destinado a uma sub-rede é semelhante.

2.11 MULTICAST

IP multicast é uma técnica que permite que uma única fonte transmita mensagens a um determinado grupo de destinatários. Esse recurso é espcialmente importante para algumas aplicações, como distribuição de vídeo ou notícias, videoconferência e levantamento de recursos de rede. Uma estação inicia a transmissão em multicast quando, em sua rede, pelo menos uma estação, nessa mesma rede, se manifesta como interessado na informação dessa estação

transmissora. A mensagem multicast utiliza a faixa de endereços de 224.0.0.0 a 239.255.255, onde os primeiros 4 bits do endereço são “1110” e os demais 28 bits indicam o ID do grupo. Alguns endereços de multicast são registrados e possuem signifaicaod específico:

224.0.0.2 = todos os roteadores nesta sub-rede

224.0.0.9 = roteadores RIPv2

224.0.0.10 = roteadores IGRP

224.0.0.12 = servidor DHCP

Alguns protocolos de multicast estabelecidos são:

- IGMP
- PIM-SM
- PIM-DM

2.11.1 IGMP

As estações da rede utilizam o protocolo IGMP *(Internet Group Management Protocol*) para se incluírem em um determinado grupo de multicast. Um roteador configurado para multicast IGMP fica em estado de espera de requisições de eventuais participantes e envia periodicamente mensagens para descobrir que grupos de transmissão estão ativos. A especificação atual é o IGMPv3 publicada pela RFC-3376, no entanto muitos equipamentos ainda operam com as veresões anteriores: IGMPv2 (RFC-2236) ou IGMPv1 (RFC-1112).

2.11.2 PIM

O protocolo PIM (*Protocol Independent Multicast*) possui dois modos de operação:

- PIM-DM (modo denso)
- PIM-SM (modo disperso)

O modo PIM-DM leva em consideração que a muitas estações (densamente distribuídas) vão participar do grupo. Esse modo é especialmente interessante quando há tráfego *multicast* intenso para muitos receptores. No modo PIM-SM o roteador deve fazer uma requisição específica para receber o fluxo de muitcast, reduzindo o uso da banda disponível e tornando esse modo mais interessante quando há poucos receptores em cada grupo e o tráfego de *multicast* não é tão constante

3 PROTOCOLOS DE ROTEAMENTO IP

Vimos que o roteador se baseia em sua tabela de roteamento para tomar suas decisões sobre encaminhamento dos pacotes. Há duas formas básicas para adicionar rotas na tabela de roteamento:

- estática
- dinâmica

Na forma estática as rotas são configuradas diretamente no roteador pelo administrador da rede. Nesse caso dizemos que o roteador foi programado com rotas estáticas. Essa tarefa será mais trabalhosa na medida em que cresce a rede. A configuração estática é utilizada principalmente nas seguintes situações:

- redes pequenas
- rotas para redes isoladas
- para garantir maior segurança

Em redes maiores e mais complexas dois fatores dificultam o uso de rotas estáticas: a existência de várias rotas possíveis entre dois pontos e as mudanças na topologia, seja por falhas (canal de comunicação ou roteador), seja por alterações naturais decorrentes de remodelagem ou crescimento da rede. Nesse caso é desejável que a escolha das rotas seja dinâmica, em outras palavras, que os roteadores se comuniquem, utilizando um protocolo apropriado e estabeleçam as rotas (de preferência, a melhor) e as alterem em caso de falha da rota em uso.

Há dois tipos básicos de protocolo para roteamento IP:

- "distância vetorial", (*distance vector*) que utiliza o algorítmo Bellman/Ford, e
- "estado de enlace" (*link-state*), que utiliza o algorítmo de Dijkstra (também conhecido como *Open Shortest Path First*).

No protocolo do tipo "distância vetorial" cada roteador transmite toda a sua tabela de roteamento aos roteadores vizinhos (somente aos vizinhos). Cada roteador da rede vai montando sua própria tabela sempre com base nas informações dos vizinhos. O protocolo "distância vetorial" é mais fácil de ser implementado mas, como as tabelas são transmitidas de vizinho para vizinho, possui a desvantagem de uma convergência lenta.

No protocolo do tipo “estado de enlace” o roteador, ao invés de enviar sua tabela aos vizinhos, envia apenas o estado de seus enlaces, mas para toda a rede. Cada roteador monta sua tabela com base em informações recebidas de toda a rede.

Os protocolos são divididos em dois grandes grupos:

- Protocolo de roteamento interior
- Protocolo de roteamento exterior

Quando o protocolo roda no interior de um sistema autônomo (AS – *Autonomous System*), ou domínio, é chamado de IGP*, Interior Gateway Protocol* ou protocolo de roteamento interior. Um AS pode ser, por exemplo, a rede de uma empresa. Em um AS todos os roteadores entendem o mesmo protocolo e pertencem a uma rede administrada por uma mesma entidade. No entanto, quando esse AS tem que se ligar a outro AS, deve utilizar outro tipo de protocolo, especial para interligar AS, chamado de EGP, *Exterior Gateway Protocol*. O roteador que fica na borda do AS deve ser capaz de trabalhar tanto com o protocolo EGP, que roda entre as AS, quanto com o protocolo IGP que roda no interior da AS e, portanto, é um roteador com características adicionais.

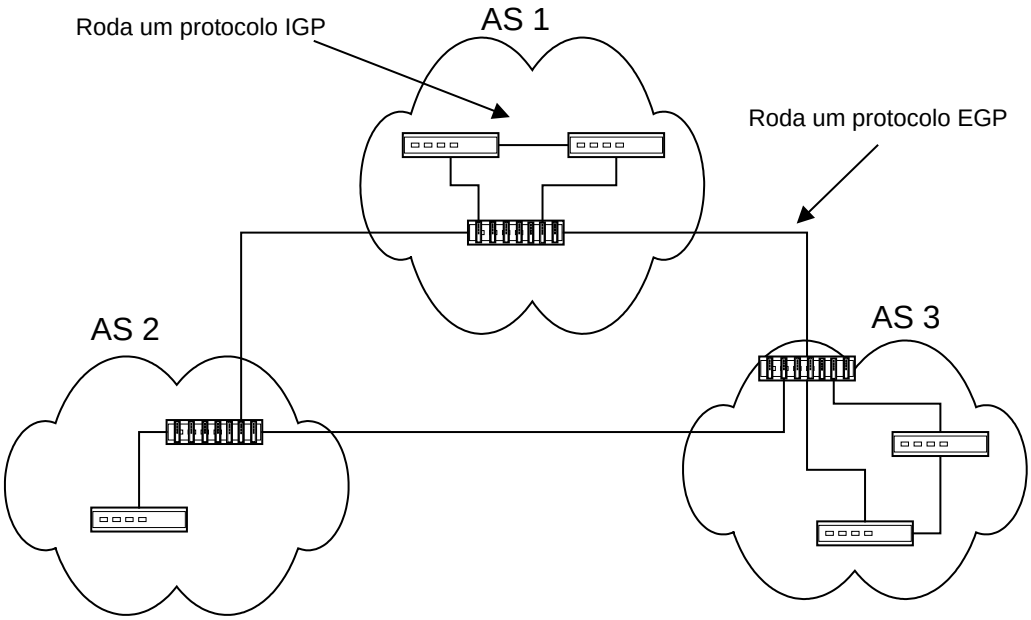


Fig. 3-1: Sistemas Autônomos

BGP é o principal protocolo do tipo *Exterior Gateway Protocol*. Como sua especificação está na revisão 4, é conhecido como BGP-4.

Os principais protocolos do tipo IGP são: RIP, OSPF e EIGRP.

RIP ou *Routing Information Protocol*, foi o primeiro protocolo do tipo IGP a ser desenvolvido e possui algumas limitações para uso em redes mais complexas. As duas

principais vantagens do protocolo RIP são sua simplicidade e o fato de estar incorporado na maioria das versões UNIX.

OSPF ou *Open Shortest Path First*, foi criado posteriormente, especificamente para ambientes IP, para substituir o RIP, suprindo suas deficiências. Cada um desses protocolos utiliza um algoritmo específico para determinar rotas.

Alguns fabricantes desenvolvem seus próprios protocolos de roteamento, que, por serem proprietários, somente podem ser utilizados em redes cujos roteadores são da mesma marca, ou utilizam roteadores licenciados para esse protocolo. Dois exemplos conhecidos são os protocolos IGRP (*Interior Gateway Routing Protocol*) e EIGRP (*Enhanced IGRP*), desenvolvidos pela Cisco Systems, cujas características foram incluídas na tabela 3.1 com base em literatura oficial do fabricante[8].

Tabela 3.1: Protocolos de roteamento

Protocolo	RIP	RIPv2	OSPF	IGRP	EIGRP
Distância vetorial	*	*	-	*	*
Estado de enlace	-	-	*	-	*
VLSM	-	*	*	-	*
Padrão aberto	*	*	*	-	-
Convergência média/rápida	-	*	**	-	**
Métrica por banda	-	-	*	*	*
Rede grande/muito grande	-	-	*	-	**

O estudo detalhado dos protocolos de roteamento citados anteriormente foge ao objetivo deste livro. Veremos o protocolo RIP, por ser uma forma quase que intuitiva de se estabelecer rotas automaticamente em uma rede de roteadores.

3.1 PROTOCOLO RIP

Os pacotes de controle do protocolo RIP são encapsulados em UDP, utilizando a porta “520”.

O protocolo RIP decide qual caminho o pacote IP deve tomar somente com base na quantidade de roteadores (saltos ou *hops*) que há nas possíveis rotas. O caminho com menos roteadores é o escolhido. Esse processo é simples mas não garante a

[8] CCDA Self-Study: Designing for Cisco Internetwork Solutions (DESGN), Cisco Press, 2004

melhor alternativa pois o pacote pode ser encaminhado por uma rota mais curta porém mais congestionada (menos banda disponível). O RIP em sua versão original (RIPv1) possui mais duas limitações: somente permite operar com máscaras de comprimentos fixos, casadas com as classes A, B ou C, e somente consegue alcançar 15 roteadores em uma rota. A especificação RIPv2 eliminou a restrição da máscara fixa e passou a operar com máscaras de comprimento variável (VLSM *ou Variable Lenght Sub-net Mask*), mas manteve a restrição dos 15 roteadores.

Vamos analisar sua operação, nos referindo ao roteador "R2", da próxima figura, para descrever como funciona o protocolo.

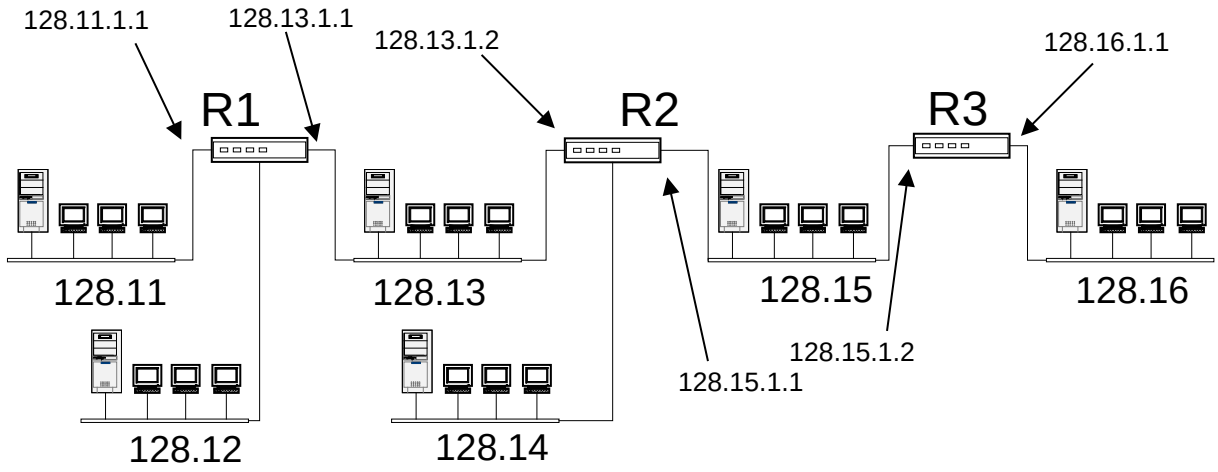


Fig. 3.2: Redes interconectadas com roteadores

Antes do roteador iniciar sua operação, o administrador da rede deve configurá-lo, entrando com as informações que definem as redes diretamente ligadas a ele, surgindo a tabela de roteamento mostrada na tabela 3.2, onde as redes diretamente conectadas (próximo hop igual 0.0.0.0) constam com métrica igual a 1.

Tabela 3.2: Tabela de roteamento de R2 (inicial)

Destino	Próximo hop	Porta	Métrica	Direto/ Remoto	Aprendido Local/RIP

128.13.0.0	0.0.0.0	1	1	D	L
128.14.0.0	0.0.0.0	2	1	D	L
128.15.0.0	0.0.0.0	3	1	D	L

A cada 30 segundos, cada roteador da rede emite pacotes IP do tipo *broadcast*, divulgando sua tabela de roteamento (mensagem RIP), em todas as suas portas. A mensagem RIP é montada em um pacote do protocolo UDP, da camada de transporte, que, por sua vez, é montado em pacote IP. A mensagem RIPv2 possui a forma apresentada na figura 3.3, que mostra os diversos campos e seus respectivos comprimentos em bytes.

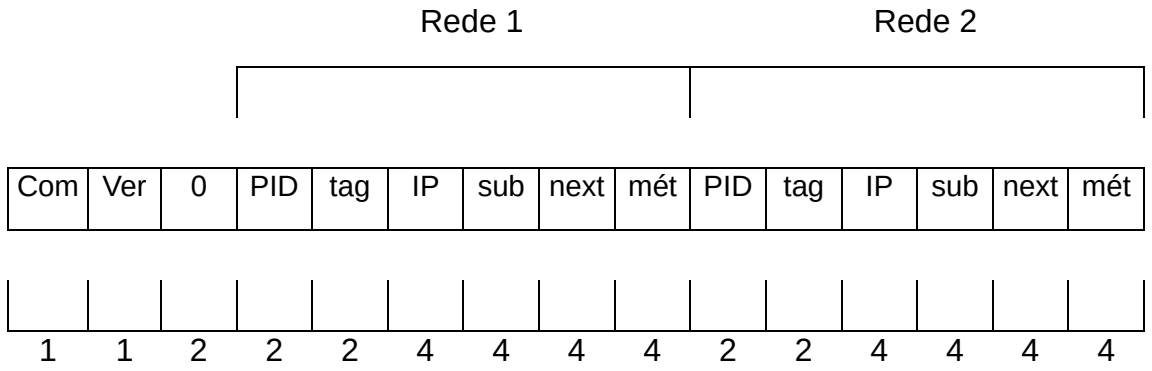


Fig. 3.3: Mensagem RIPv2

Os dois primeiros campos identificam o tipo de mensagem (comando e versão). O próximo campo contém zeros (“0”). Para cada rede cadastrada no roteador ele envia a informação “PID” (que protocolo está utilizando o RIP – normalmente é o IP), “tag” que indica como o protocolo está aprendendo as rotas (normalmente é do RIP),), “IP” (endereço IP da rede em questão), “sub” que indica a máscaea de sub-rede, “next” que indica o próximo roteador (next hop) e “mét” (métrica da rede em questão) cujo valor máximo é 15.

O RIP pode enviar informações de até 25 redes em uma única mensagem. Fica claro que, eventualmente, o roteador vai ter que enviar diversas mensagens desse tipo para divulgar toda a sua tabela. Voltemos à descrição do protocolo RIP.

Logo após ser ligado, o roteador “R2” vai receber as tabelas de “R3” e “R1”.

O roteador “R2” vai receber tabelas com redes que já constam em sua própria tabela, como por exemplo, a rede 128.13.0.0 que também constará na tabela divulgada por “R1”.

Ao receber uma tabela, “R2” vai atualizar a informação de uma determinada rede, em sua própria tabela, se a métrica da informação recebida for menor que a atual. Se, na tabela recebida, constar uma rede que “R2” não possui em sua tabela, ele soma um à métrica recebida e acrescenta essa informação em sua tabela.

A métrica pode assumir valores de 1 a 15. Uma métrica de valor 16 indica que a rede não pode ser alcançada. O protocolo RIP só pode ser utilizado em redes cujas rotas possuam, no máximo, 15 roteadores.

Tabela 3.3: Tabela de roteamento de R2 (final)

Destino	Próximo	Porta	Métrica	Direto/ Remoto	Aprendido Local/RIP
128.13.0.0	0.0.0.0	1	1	D	L
128.14.0.0	0.0.0.0	2	1	D	L
128.15.0.0	0.0.0.0	3	1	D	L
128.11.0.0	128.13.1.1	1	2	R	R
128.12.0.0	128.13.1.1	1	2	R	R
128.16.0.0	128.15.1.1	3	2	R	R

Se o protocolo RIP suporta até 15 roteadores em seqüência, e , supondo que cada leva 30 segundos para transmitir sua tabela, vamos concluir que uma modificação de tabela pode levar até 7 minutos para chegar a todos os roteadores. Esse tempo de convergência longo do protocolo RIP é um de seus problemas.

3.2 PROTOCOLO OSPF

O protocolo de roteamento OSPF, atualmente na versão 2, também citado como OSPFv2, foi definido pela RFC-2328 de abril de 1998. É mais complexo que o RIP e exige mais capacidade de processamento do roteador. Em contrapartida é superior ao RIP tanto na forma como distribui as informações aos demais roteadores quanto na flexibilidade de métricas.

O pacote OSPF é encapsulado diretamente em um pacote IP com identificação de protocolo igual a “89”. A figura 3.4 mostra o pacote OSPF.

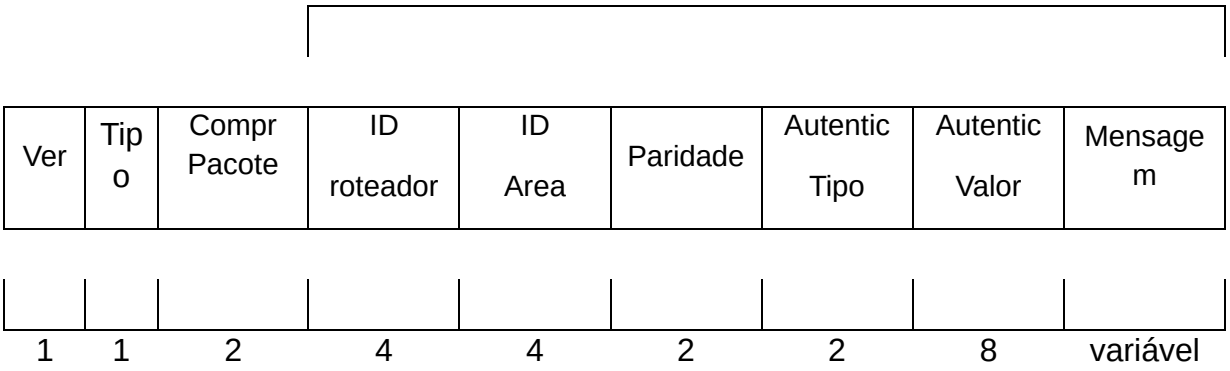


Fig. 3.4: Mensagem OSPF

O primeiro campo, de um byte, identifica a versão do protocolo. O próximo campo indica o tipo de mensagem (Hello, ou uma descrição de base de dados: solicitação de estados, atualização de estados, aceitação de estados). O próximo campo indica o comprimento do pacote em bytes. Os próximos campos indicam: as identificações do roteador remetente e de sua área, um código de paridade, o tipo e o valor da autenticação. Há um formato específico para cada tipo de mensagem, cuja abordagem foge ao escopo deste curso.

Ao contrário do RIP, o protocolo OSPF monta uma tabela com todos os destinos possíveis, com os respectivos indicadores “próximo roteador” e “custo”, conforme ilustra a tabela 2.www. O próximo roteador indica que caminho o pacote deve tomar para chegar ao destino com o menor custo.

Tabela 3.4: Tabela de roteamento OSPF

Destino	Próximo	Custo
128.13.0.0	128.13.1.1	1
128.14.0.0	128.13.1.1	2
128.15.0.0	128.15.1.1	3
128.11.0.0	128.13.1.1	1
128.12.0.0	128.13.1.1	1
128.16.0.0	128.15.1.1	3

Há duas alternativas para o roteador disparar o processo de recalcular sua tabela de roteamento, para descobrir os caminhos de menor custo: a cada mudança de topologia, o que vai demandar muito recurso de processamento e memória interna do roteador, ou após um tempo fixo pré-determinado.

A primeira providência que um roteador, rodando OSPF, toma ao ser ligado, é enviar mensagens de “Hello” aos seus vizinhos. Dessa forma todos os roteadores podem iniciar a montagem de suas tabelas pelas redes que estão mais próximas.

4 CONFIGURAÇÃO DO ROTEADOR

4.1 DEFINIÇÃO DOS ENDEREÇOS IP

A figura 4.1 mostra uma rede WAN com três nós (três roteadores) unindo três redes locais em localidades distintas. A seguir vamos ver, como exemplo, um procedimento para estabelecer os endereços IP.

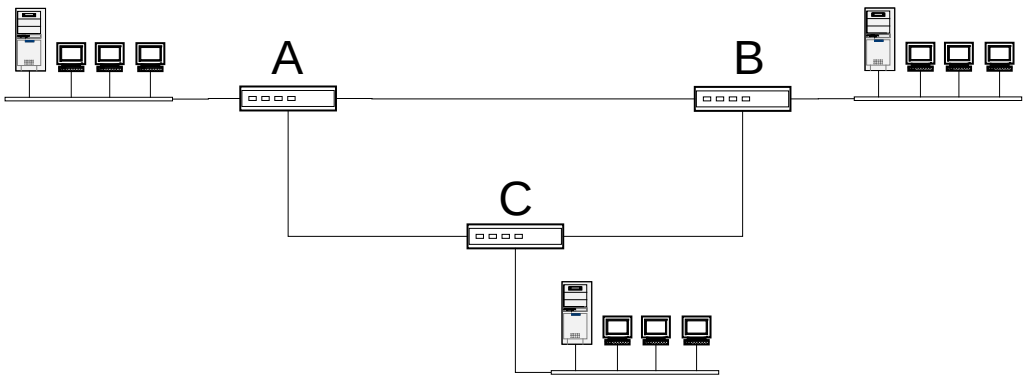


Fig. 4.1: rede WAN com 3 nós

Metodologia

1 - Providenciar o endereço da rede junto à organização responsável, ou escolher um endereço inválido, se for o caso. Digamos que o endereço da rede seja 200.14.20/24.

2 - Listar as sub-redes. Cada enlace serial é considerado uma sub-rede. No exemplo, então, temos 6 sub-redes: as 3 localidades e os 3 enlaces.

3 - Definir a máscara de sub-rede. Levantar a quantidade de hosts em cada sub-rede para determinar os comprimentos necessários dos endereços de host e sub-redes. Analisar a perspectiva de crescimento da empresa e projetar para essa situação futura prevista.

Como neste exemplo temos 8 bits para repartir e sabemos que a empresa não terá mais que 5 ou 6 escritórios, definimos:

3 bits para sub-rede (serão 7 possíveis)
5 bits para host (serão 30 possíveis)

Então, a máscara fica 255.255.255.224/27

4 - Definir o IP das sub-redes.

Tabela 4.1: definição de IP

Sub-rede	binário	decimal
Enlace A-B	0 0 1 x x x x x	32
Enlace A-C	0 1 0 x x x x x	64
Enlace B-C	0 1 1 x x x x x	96
Rede B	1 0 0 x x x x x	128
Rede C	1 0 1 x x x x x	160
Rede A	1 1 0 x x x x x	192

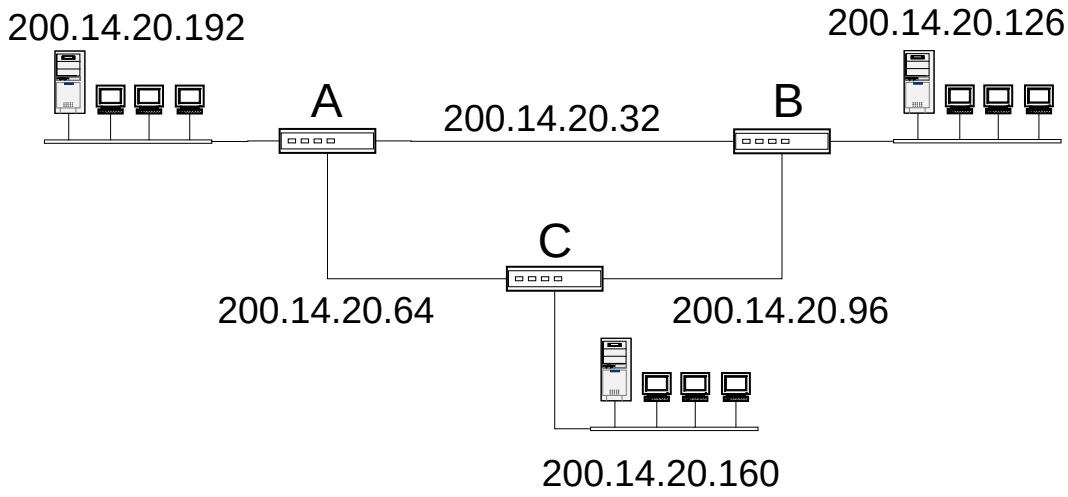


Fig. 4.2: escolha dos endereços IP

5 - Definir as faixas de IP para os hosts:

Interfaces/roteadores: 1,2,3

Servidores: 4,5,6

Estações: 7 até 30

6 - Definir os IPs das interfaces dos roteadores:

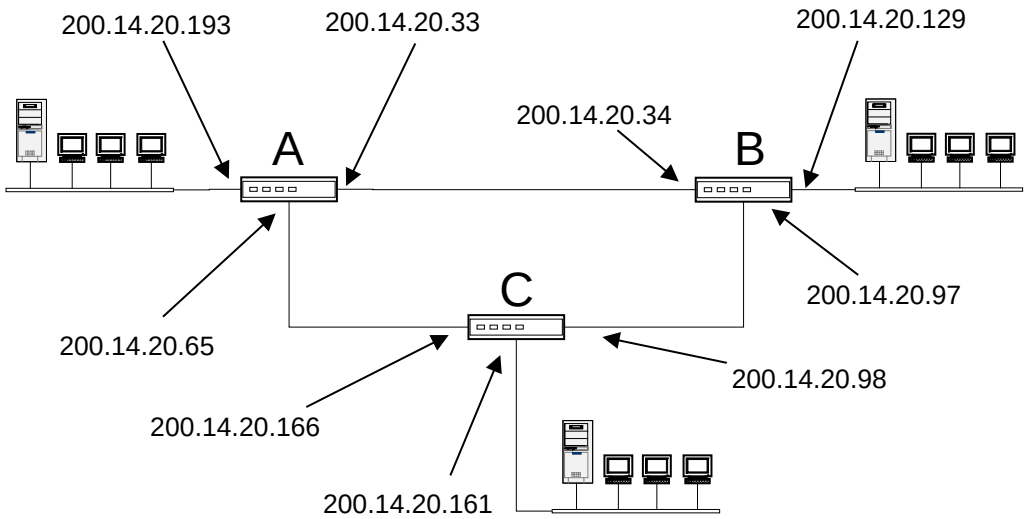


Fig. 4.3: endereços IP das interfaces dos roteadores

4.2 CONFIGURAÇÃO DOS ENDEREÇOS NO ROTEADOR

Com um terminal conectado na porta console do roteador, ou remotamente utilizando o programa Telnet, o administrador deve entrar os comandos de configuração. Esses comandos são específicos para cada roteador ou família de roteadores, definidos pelo fabricante, podendo ainda sofrer alterações conforme a versão de firmware do equipamento. Como exemplo, utilizaremos o padrão intuitivo utilizado pela **Cisco** daqui por diante. Então, teremos os seguintes comandos para configurar o roteador A:

interface serial 0	(escolhe a interface 0)
ip address 200.14.20.33 255.255.255.224	(define IP e máscara)
interface serial 1	(escolhe a interface 1)
ip address 200.14.20.65 255.255.255.224	(define IP e máscara)
interface ethernet 0	(escolhe a interface 0)

ip address 200.14.20.193 255.255.255.224 (define IP e máscara)

exit

4.3 DEFINIÇÃO DE ROTAS NO ROTEADOR

O roteador tem duas formas de saber por onde mandar um pacote: por rotas pré-definidas no roteador (rotas estáticas) ou através de um protocolo de roteamento rodando em seu sistema operacional (RIP, OSPF, etc). As rotas estáticas devem ser utilizadas em redes pequenas ou redes com uma única saída, pois evitam o tráfego de mensagens do protocolo de roteamento e conferem maior segurança. Para redes maiores ou situações dinâmicas, devemos ativar um protocolo de roteamento no roteador. A configuração do roteador "A" para operar o protocolo RIP é:

```
router rip                          (ativa o protocolo de roteamento)
network 200.14.20.0                 (define IP da rede)
ip route  200.14.20.128   255.255.255.224   200.14.20.34
```

A configuração de uma rota estática é feita pelo comando "ip route", seguido dos endereços: da sub-rede destino, máscara da sub-rede e endereço do próximo roteador (no caso é a interface serial do roteador remoto da sub-rede desejada):

Se o roteador for o responsável pela saída dos dados para um ambiente onde roda outro protocolo, digamos o protocolo OSPF, e a rede da empresa opera RIP, ele deve passar as informações de roteamento entre os ambientes RIP e OSPF.

No caso dos roteadores Cisco, o que se faz é suprimir o RIP nas interfaces que vão se conectar ao ambiente OSPF. Digamos que a interface serial "0" do roteador "A" vai se ligar a um ambiente OSPF:

```
router rip                          (ativa o protocolo de roteamento)
network 200.14.20.0                 (define IP da rede)
passive-interface serial 0          (suprime o RIP da interface)
```

Outros comandos serão necessários para redistribuir as rotas OSPF no ambiente RIP, ativar o protocolo OSPF, etc.

4.4 SUMARIZAÇÃO DE ROTAS

A definição do endereçamento IP em um projeto deve seguir um modelo hierárquico, onde redes com bits mais significativos iguais estão do mesmo lado de uma interface de roteador. Essa medida é fundamental para que o roteador possa reunir várias rotas de hierarquia menor em uma única de hierarquia maior, reduzindo sua tabela de roteamento e, consequentemente, melhorando sua performance e reduzindo o tráfego de pacotes de controle nos enlaces adjacentes.

Por exemplo, o roteador R1 da figura www pode anunciar somente a rota 200.14.168/23 para o roteador R2, ou seja, as redes com esses 23 primeiros bits, que estão ligadas a ele. Da mesma forma o roteador R2 pode anunciar somente a rota 200.14.168/22.

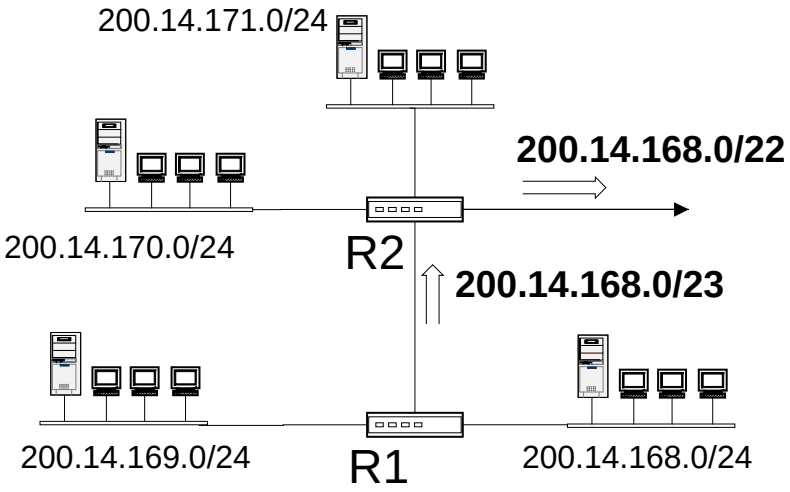


Fig. 4.4: Sumarização de rotas

Se não houvesse sumarização de rotas, o roteador R2 teria que divulgar quatro redes, ao invés de uma só. A tabela 4.2 mostra que os primeiros 22 bits dos endereços das redes sumarizadas por R2 são os mesmos.

Tabela 4.2: sumarização de rotas

IP	200	14	1 0 1 0 1 0 *0 0*	00000000	168
		14	1 0 1 0 1 0 *0 1*	00000000	169
		14	1 0 1 0 1 0 *1 0*	00000000	170
		14	1 0 1 0 1 0 *1 1*	00000000	171

máscara	255	255	1 1 1 1 1 0 0 0	00000000

4.5 MÁSCARA DE COMPRIMENTO VARIÁVEL

O protocolo RIP não aceita um ambiente com máscara de comprimento variável, mas os protocolos RIPv2, OSPF e EIGRP (proprietário da Cisco) aceitam.

Suponha uma situação em que se deseja criar sub-redes em uma rede classe "C" com IP 20.14.20.0/24. Suponha, ainda, que são três localidades, conforme a figura 4.3 do exemplo descrito em 4.1, com:

local A: 110 estações

local B: 50 estações

local C: 12 estações

O endereçamento estabelecido em 4.1 não mais atende. Com o oitavo bit de host em "0", definimos a primeira sub-rede; com o sétimo e oitavo bit em "10" definimos a segunda; e assim por diante:

sub-rede 1: 200.14.20.00000000 $\rightarrow 2^7-2 = 126$ hosts

sub-rede 2: 200.14.20.10000000 $\rightarrow 2^6-2 = 62$ hosts

sub-rede 3: 200.14.20.11000000 $\rightarrow 2^5-2 = 30$ hosts

sub-rede 4: 200.14.20.11100000 $\rightarrow 2^2-2 = 2$ hosts

sub-rede 5: 200.14.20.11100000 $\rightarrow 2^2-2 = 2$ hosts

sub-rede 6: 200.14.20.11100000 $\rightarrow 2^2-2 = 2$ hosts

sub-rede 7: 200.14.20.11100000 $\rightarrow 2^2-2 = 2$ hosts

.....

sub-rede 11: 200.14.20.11100000 $\rightarrow 2^2-2 = 2$ hosts

As sub-redes, de "4" a "11" podem ser utilizadas para os enlaces seriais.

- o – o – o -