- Aula 5 -

CAMADA DE REDE

1. INTRODUÇÃO

A camada de Rede está relacionada à transferência de pacotes da origem para o destino. No entanto, chegar ao destino pode envolver vários saltos em roteadores intermediários. Assim sendo, a camada de rede é a camada mais baixa que lida com a transmissão fim a fim. Para isso ela deve conhecer a topologia da sub-rede de comunicações, ou seja, os roteadores, escolhendo as melhores rotas, ou aquelas que evitem sobrecarregar algumas das linhas de comunicação.

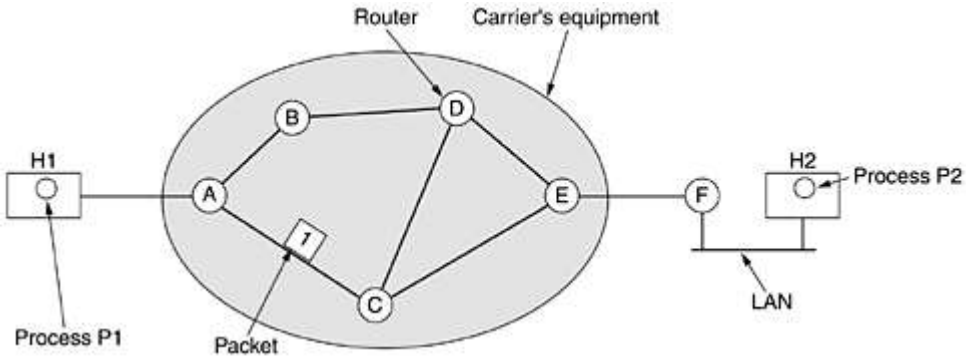


Figura 1 - Transferência de Pacotes

Quando alguns cientistas que fundaram a Cisco perceberam que poderiam utilizar filtragem da camada três do modelo de referência OSI para melhorar o desempenho da rede, eles desenvolveram o roteador.

Para facilitar o conceito imagine a situação a seguir. Quando você sai de São Paulo e vai para as praias da o Rio de Janeiro de carro e, como bom motorista, usa o mapa para chegar lá.

Figura 2 - Rota São Paulo - Rio de Janeiro

Note que existem dois caminhos: Por qual deles ir? Pelo caminho mais curto seria a resposta mais óbvia. No entanto, seria mais sensato responder que depende. Apesar de ser tentador ir pelo caminho mais curto, é necessário considerar alguns pontos:

1. Tráfego - Qual dos dois caminhos tem um tráfego menor?

2. Estado de conservação - Qual dos dois caminhos tem menos buracos.

3. Distância - Pode ser considera sim. Observe o próximo item.

4. Análise dos pontos anteriores - Apesar de buracos e do tráfego ou mesmo a distância maior, pode ser interessante ir naquele caminho do que o mais curto.

Assim trabalha o roteador. Ele, através de análise do link de comunicação, permite uma comunicação entre redes, pois trabalha na camada de rede, ou seja, lida diretamente com o *Internet Protocol*.

2. SERVIÇOS OFERECIDOS À CAMADA DE TRANSPORTE

A camada de rede oferece serviços à camada de transporte na interface entre a camada de rede e a camada de transporte. Tais serviços foram projetados visando os seguintes objetivos:

- Os serviços devem ser independentes da tecnologia de roteadores;
- A camada de transporte deve ser isolada do número, do tipo e da topologia dos roteadores presentes;
- Os endereços de rede que se tornaram disponíveis para a camada de transporte devem usar um plano de numeração uniforme, mesmo nas LAN's e WAN's.

Dentro desses objetivos entra uma questão polêmica, que é o fato da camada de rede fornecer serviço orientado a conexão ou sem conexão.

Por um lado a tarefa dos roteadores é tão somente movimentar pacotes, o que leva a crer que a sub-rede é inerentemente pouco confiável, independente de como tenha sito projetada. Sendo assim, os *hosts* devem realizar o controle de erros e o controle de fluxo. Além disso, cada pacote deve ter o endereço de destino completo, pois todos são transportados independentemente de seus predecessores.

Por outro lado, as provedoras de serviço de Internet alegam que a sub-rede deve fornecer um serviço orientado a conexões confiável, sob alegação a qualidade do serviço é o fator dominante, principalmente em se tratando de tráfego em tempo real, como voz e vídeo.

Estas duas opiniões são explicadas pela Internet e pelas redes ATM. A **Internet** oferece serviço da camada de rede sem conexões, enquanto as redes **ATM** oferecem serviço da camada de rede orientado a conexões. Contudo, à medida que as garantias de qualidade de serviço estão se tornando cada vez mais importantes, a Internet está evoluindo e está aderindo a propriedades associadas ao serviço orientado a conexões, como no caso das VLANS.

3. A IMPLEMENTAÇÃO DO SERVIÇO SEM CONEXÃO

Neste caso, os pacotes serão injetados individualmente na sub-rede e roteadores de modo independente uns dos outros. Não é necessária nenhuma configuração antecipada. Neste contexto, os pacotes freqüentemente são chamados de datagramas (analogia a telegramas) e a sub-rede denominada sub-rede de datagramas. Imagine que um determinado processo tenha uma longa mensagem para transmitir. Ele entrega a mensagem à camada de transporte, com instruções para que ela seja entregue no destino. Neste caso, é acrescentado um cabeçalho de transporte ao início da mensagem que entrega o resultado a camada de rede.

Se a mensagem for extremamente grande e houver a necessidade de dividi-la em quatro partes, por exemplo, um protocolo ponto a ponto (PPP) será utilizado. Estes pacotes serão entregues a um roteador que tem uma tabela interna que informa para onde devem ser enviados os pacotes a serem entregues a cada destino possível. Cada entrada da tabela é um par que consiste em um destino e na linha de saída a ser utilizada para este destino. À medida que os pacotes chegam ao roteador estes são armazenados e verificados de acordo com um algoritmo de verificação. Em seguida, cada um deles é enviado para o próximo roteador de acordo com a tabela criada. É possível que um dos pacotes seja enviado para um roteador diferente do que os demais foram sendo envidados. O algoritmo que gerencia as tabelas é chamado de **Algoritmo de Roteamento**.

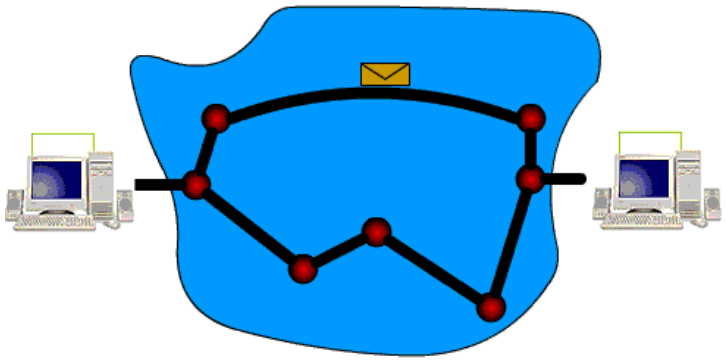


Figura 3 - Serviço sem conexão

4. A IMPLEMENTAÇÃO DO SERVIÇO ORIENTADO A CONEXÕES

No serviço orientado a conexões deve ser estabelecido um caminho desde o roteador de origem ao de destino, antes de iniciar o envio de quaisquer pacotes de dados, sendo assim chamada de **circuitos virtuais**. A idéia é evitar a necessidade de escolher uma nova rota para cada pacote enviado. Em vez disso, quando uma conexão é estabelecida, escolhe-se uma rota desde a origem até o destino, como parte da configuração da conexão, e essa rota é armazenada em tabelas internas dos roteadores. A rota é usada por todo o tráfego que flui pela conexão.

Quando a conexão é liberada, o circuito virtual também é encerrado. Neste serviço cada pacote transporta um identificador dizendo a qual circuito ele pertence.

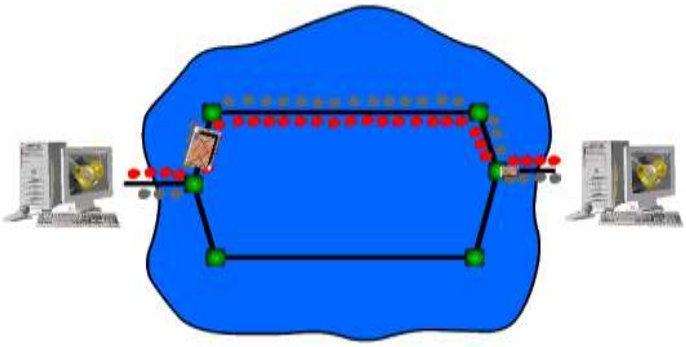


Figura 4 - Serviço com conexão

5. COMPARAÇÃO ENTRE SUB-REDES DE CIRCUITOS VIRTUAIS E DE DATAGRAMAS

Dentro da sub-rede, existem vários compromissos entre circuitos virtuais e datagramas, como o compromisso entre espaço de memória do roteador e largura de banda. Os circuitos virtuais permitem que os pacotes contenham números de circuitos em vez de endereços de destino completos. O preço pago pelo uso de circuitos virtuais é o espaço na tabela dentro dos roteadores.

Outro compromisso é o que se dá entre o tempo de configuração e o tempo de análise de endereço. O uso de circuitos virtuais requer uma fase de configuração que leva tempo e consome recursos. Entretanto, é fácil descobrir o que fazer com um pacote de dados em uma sub-rede de circuitos virtuais. O roteador só utiliza o número do circuito para criar um índice em uma tabela e descobrir para onde vai o pacote.

Em uma sub-rede de datagramas, é necessário um procedimento de pesquisas mais complicado para localizar a entrada correspondente ao destino.

Os circuitos virtuais têm vantagens na garantia da qualidade de serviço e ao evitar o congestionamento dentro de uma sub-rede, pois os recursos podem ser reservados antecipadamente, o que não ocorre na rede de datagramas.

Os circuitos virtuais têm um problema grande com a vulnerabilidade. Se um roteador apresentar uma falha e perder sua memória, mesmo que volte um segundo depois, todos os circuitos virtuais que estiverem passando por ele terão de ser interrompidos. No roteador de datagramas somente os usuários cujos pacotes estiverem enfileirados no roteador naquele momento serão afetados. A perda de uma linha de comunicação é fatal para os circuitos virtuais, mas podem ser compensadas se utilizados datagramas, pois estes permitem que os roteadores equilibrem o tráfego pela sub-rede uma vez que a rota pode ser parcialmente alterada.

QUESTÃO	SUB-REDE DE DATAGRAMAS	SUB-REDE DE CIRCUITOS VIRTUAIS
Configuração de circuitos	Desnecessária	Obrigatória
Endereçamento	Cada pacote contém os endereços de origem e de destino completos	Cada pacote contém um número de circuito virtual curto.
Informações sobre o estado	Os roteadores não armazenam informações sobre o estado das	Cada circuito virtual requer espaço em tabelas de roteadores

	conexões	por conexão
Roteamento	Cada pacote é roteado independentemente	A rota é escolhida quando o circuito virtual é estabelecido; todos os pacotes seguem essa rota.
Efeito de falhas no roteador	Nenhum, com exceção dos pacotes perdidos durante a falha	Todos os circuitos virtuais que tiverem passado pelo roteador que apresentou o defeito serão encerrados.
Qualidade de serviço	Difícil	Fácil, se for possível alocar recursos suficientes com antecedência para cada circuito virtual
Controle de congestionamento	Difícil	Fácil, se for possível alocar recursos suficientes com antecedência para cada circuito virtual

6. ALGORITMOS DE ROTEAMENTO

Na maioria das sub-redes os pacotes necessitarão de vários saltos para cumprir seu trajeto. Para que isto se consuma é necessário seguir alguns **algoritmos de roteamento**.

O algoritmo de roteamento é parte do software da camada de rede responsável pela decisão sobre a linha de saída a ser usada na transmissão do pacote de entrada. Se a sub-rede utilizar datagramas internamente, essa decisão deverá ser tomada mais uma vez para cada pacote de dados recebido, pois a melhor rota pode ter sido alterada desde a última vez. Se a sub-rede utilizar circuitos virtuais internamente, as decisões de roteamento serão tomadas somente quando um novo circuito virtual estiver sendo estabelecido. Por conseguinte, os pacotes de dados seguirão a rota previamente estabelecida.

Às vezes, essa última circunstância é chamada de roteamento por sessão, visto que uma rota permanece em vigor durante toda uma sessão do usuário (ex.: terminal remoto).

O que acontece é que há dois processos no interior do roteador, um que procura a linha de saída a ser utilizado em uma tabela de roteamento, denominado processo de **encaminhamento**. O outro processo é o responsável pelo preenchimento e atualização das tabelas de roteamento, entrando em cena o **algoritmo de roteamento**.

Propriedades desejáveis em um algoritmo de roteamento são:

- Correção;
- Simplicidade;
- Robustez;
- Estabilidade;
- eqüidade; e
- otimização.

O algoritmo de roteamento deve ser capaz de aceitar as alterações na topologia e no tráfego sem exigir que todas as tarefas de todos os hosts sejam interrompidas e que a rede seja reinicializada sempre que algum roteador apresentar falha.

Tais algoritmos podem ser agrupados em duas classes:

- Adaptativos; e
- Não-Adaptativos.

Os **não-adaptativos** não baseiam suas decisões de roteamento em medidas ou estimativas do tráfego e da topologia atuais. Este tipo de roteamento é denominado **roteamento estático,** uma vez que a escolha da rota é definida previamente off-line.

Os **algoritmos adaptativos** mudam suas decisões de roteamento para refletir mudanças na topologia e, normalmente, também no tráfego. Estes diferem em termos do lugar em que obtêm suas informações, seja no próprio local, em roteadores adjacentes ou todos os roteadores.

6.1. Roteamento pelo caminho mais curto

Esta é uma técnica muito utilizada, haja vista ser simples e fácil de entender. A idéia principal é criar um grafo de sub-rede, com cada nó do grafo representando um roteador e cada arco indicando uma linha de comunicação (enlace). Para escolher uma rota, o algoritmo simplesmente encontra o caminho mais curto expresso na rota.

A métrica usada para determinar o caminho mais curto entre fonte e destino pode se basear em diferentes métodos:

- Número de *hops* (saltos) entre fonte e destino;
- Distância Física (Geográfica);
- Fila média e atraso de transmissão associados a cada arco no caminho para algum pacote padrão de teste transmitido a intervalos regulares. O caminho mais curto é o mais rápido, ao invés daquele com menor número de arcos ou km.

Em geral os *labels* nos arcos podem ser computados como função de mais de um argumento, entre os quais:

- Distância;
- Custo de comunicação;
- Largura de banda;
- Tamanho médio da Fila;
- Tráfego Médio;
- *Delays* (atrasos).

O algoritmo pode calcular o caminho mais curto através de um dos critérios citados ou através de uma combinação ponderada dos diferentes critérios.

Exemplo:

Algoritmo de Dijkstra

6.2. *Flooding* (Inundação)

O algoritmo de inundação é um algoritmo estático no qual cada pacote de entrada é enviado para todas as linhas de saída, exceto para aquela em que chegou. É gerada uma vasta quantidade de pacotes duplicados, a menos que algumas medidas sejam tomadas para tornar mais lento o processo. Uma dessas medidas é ter um contador de *hops* contido no cabeçalho de cada pacote. O contador é decrementado até atingir zero. Normalmente ele tem o número que saltos necessários para percorrer todo o caminho. Outro meio é contar quais pacotes foram transmitidos para que eles não sejam enviados novamente.

É usado para distribuir informação para todos os nós que age como um receptor e transmissor de mensagem.

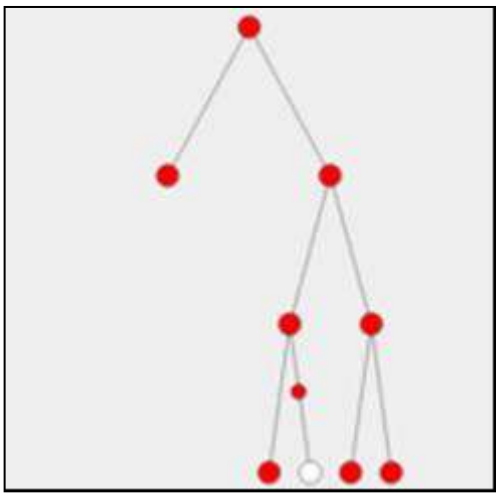


Figura 5 – Inundação

6.3. Roteamento por difusão

Em algumas aplicações, os hosts precisam enviar mensagem a muitos outros *hosts*. Neste caso o envio de um pacote a todos os destinos simultaneamente é chamado de difusão (*broadcasting*). O método exige que a origem tenha uma lista completa de todos os destinos. Na prática, essa pode ser a única possibilidade completa de todos os destino receberem o pacote transmitido.

6.4. Roteamento para hosts móveis

Como visto, a principal função da camada de rede é rotear pacotes. Na maioria das sub-redes os pacotes necessitarão de vários saltos para cumprir seu trajeto. Para isso são implementados diversos tipos de algoritmos de roteamento, dentre eles o **Roteamento para Hosts Móveis.**

É comum hoje em dia pessoas utilizarem computadores pessoais para ler mensagens de e-mail, acessar internet, etc. Esses hosts móveis criam uma nova complicação: **antes de rotear um pacote para um host móvel, primeiro a rede precisa localizá-lo**.

Para resolver essa problemática definiu-se para cada área um ou mais agentes externos, que controlam todos os usuários móveis que visitam a área. Além disso, cada área possui um agente interno, que controla os usuários cujas bases estejam na área, mas que estejam no momento visitando outra área. Quando um novo usuário entra em uma área, conectando-se a ela (por exemplo, ligando seu computador na LAN), ou simplesmente percorrendo a célula, seu computador deve-se registrar com o agente externo dessa área. Periodicamente, cada agente externo transmite um pacote anunciando sua existência e endereço.

Um host móvel recém-chegado pode aguardar uma dessas mensagens; no entanto, se nenhuma chegar rápido o suficiente, o host móvel poderá transmitir um pacote dizendo: "Existe algum agente externo?"

- O host móvel é registrado com o agente externo, fornecendo seu endereço fixo, o endereço atual de camada de enlace de dados e algumas informações de segurança.
- O agente externo contacta o agente interno do host móvel e diz: "Um de seus hosts está aqui".
- A mensagem do agente externo para o agente interno contém o endereço de rede do agente externo.
- A mensagem contém ainda as informações de segurança, para convencer o agente interno de que o host móvel está realmente lá.
- O agente interno examina as informações de segurança, que contêm um timbre de hora, para provar que foi gerando há alguns segundos. Se estiver tudo de acordo, o agente interno diz ao externo para prosseguir.
- Quando o agente externo obtém a confirmação do agente interno, ele cria uma entrada em sua tabela e informa ao host móvel que agora ele está registrado.
- O ideal é que quando o usuário sair de uma área, isso também seja divulgado para permitir o cancelamento do registro, mas muitos usuários desligam seus computadores abruptamente quando terminam de usá-los.

Quando é enviado a um usuário móvel, o pacote é roteado para a LAN básica do usuário, pois é isso que o endereço diz que deve ser feito. Os pacotes enviados para o usuário móvel através de sua LAN básica são interceptados pelo agente interno. Em seguida, o agente interno consulta a nova localização (temporária) do usuário móvel e encontra o endereço do agente externo que está tratando do usuário móvel.

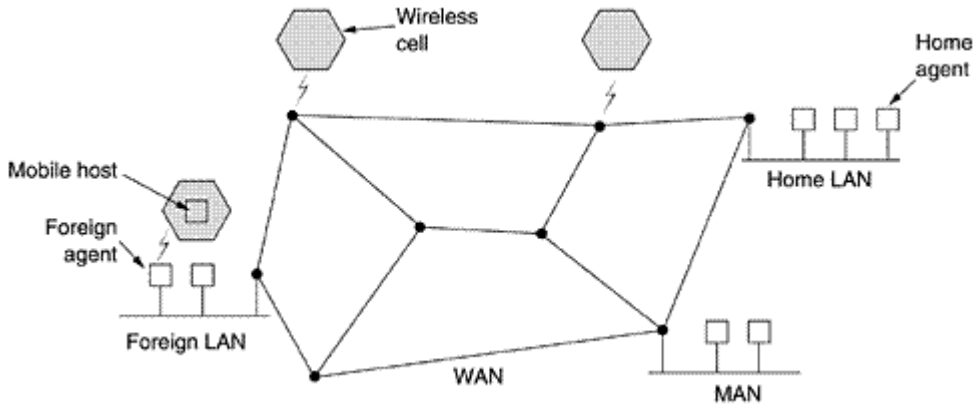


Figura 6 - Roteamento para hosts móveis

7. ALGORITMOS DE CONTROLE DE CONGESTIONAMENTO

Congestionamento ocorre quando a quantidade de pacotes na rede é muito grande (normalmente isso ocorre quando se atinge um patamar da capacidade de carga dos canais de comunicação).

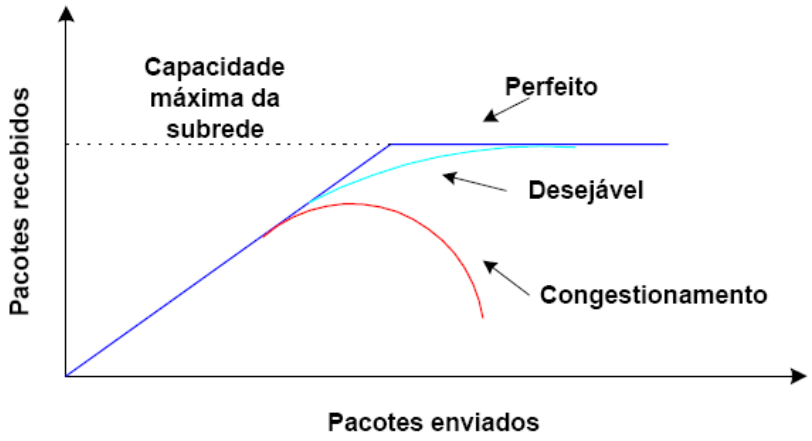


Figura 7 - Janela de congestionamento

As causas do congestionamento podem ser as seguintes:

- Pacotes chegando por canais de comunicação rápidos, tendo de sair por canais mais lentos;
- Roteadores lentos;
- Roteadores com pouca memória para armazenar pacotes temporariamente;

Contudo, existem dois métodos que podem ser usados para controlar o fluxo, a saber:

- Modelo circuito aberto; e
- Modelo circuito fechado.

O primeiro propõe resolver os problemas na fase de projeto/configuração dos roteadores de modo a (tentar) garantir que não ocorra congestionamento. Para ajustar alguma coisa, é necessário de reinicializar tudo.

O segundo realiza a monitoração do sistema para detectar quando e onde o congestionamento ocorre. Realiza a passagem dessas informações para pontos de controle onde alguma ação pode ser tomada e realiza o ajuste da operação do sistema para corrigir o problema.

Neste modelo de circuito fechado, o controle pode ser **explícito**, quando o ponto de congestionamento avisa (de alguma forma) a origem dos pacotes (exemplo: ATM); ou **implícito**, quando a origem dos pacotes deduz que há congestionamento fazendo observações localmente (exemplo: pela demora no recebimento de confirmação de entrega de pacotes - TCP/IP).

7.1. Políticas de prevenção de congestionamento

As políticas adotadas em diversas camadas de uma pilha de protocolos que afetam o congestionamento são expressas na tabela abaixo:

Tabela 1 - Políticas de controle de congestionamento

CAMADA	POLÍTICAS
Transporte	- Política de retransmissão; - Política de armazenamento para segmentos fora de ordem; - Política de reconhecimento (Ack) de segmento; - Política de controle de fluxo; - Determinação do temporizador (*timeout*);
Rede	- Modo circuito virtual versus modo datagrama; - Enfileiramento de pacote e política de serviço; - Política de descarte de pacote; - Algoritmo de roteamento; - Gerência de tempo de vida de pacote;
Enlace de dados	- Política de retransmissão; - Política de armazenamento para quadro fora de ordem (*go back* N, *seletive repeat*); - Política de reconhecimento (Ack) de quadro (com/sem *pigybacking*); - Política de controle de fluxo (com/sem *slide window*).

7.2. Controle de congestionamento em sub-redes de circuitos virtuais

A maioria dos algoritmos de congestionamento tenta impedir que o congestionamento ocorra, em vez de lidar com ele após seu surgimento. Uma técnica muito utilizada para impedir que um congestionamento iniciado se torne pior é o **Controle de Admissão**. Uma vez que o congestionamento tenha dado alguma indicação de sua existência, nenhum outro circuito virtual será estabelecido até que o problema tenha passado. Portanto, todas as tentativas de estabelecer novas conexões da camada de transporte falharão. Alternativa é permitir novos circuitos, mas rotear com cuidado todos os novos circuitos virtuais em áreas problemáticas.

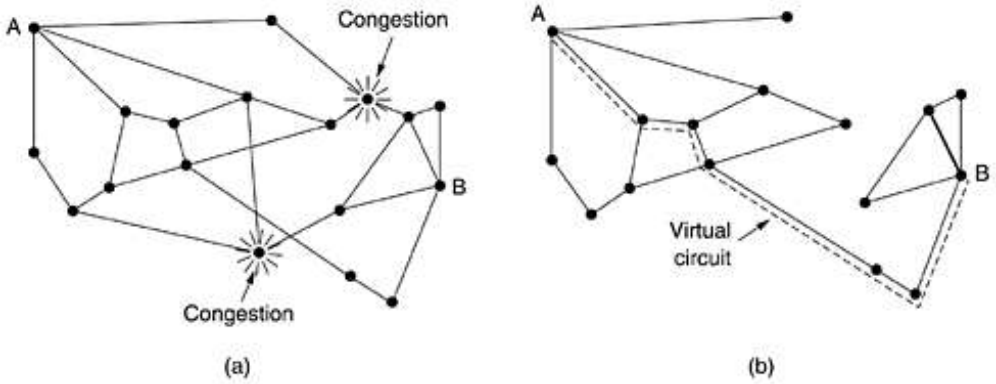


Figura 8 - Sub-rede congestionada

A idéia neste caso, como se vê na figura acima é **redesenhar a sub-rede** (b), omitindo os roteadores congestionados e todas as suas linhas.

Existe ainda outra situação que é um **acordo entre o host e a sub-rede**, na qual fica acordado, no momento da configuração do circuito virtual, o volume, a formatação do tráfego, a qualidade de serviço exigida e outros parâmetros. Para isso a sub-rede reservará recursos ao longo do caminho. Assim, é improvável que ocorra congestionamento nos novos circuitos virtuais. A desvantagem desse método é o desperdício de recursos.

7.3. Controle de congestionamento em sub-redes de datagramas

No caso das sub-redes de datagramas, cada roteador pode monitorar facilmente a utilização de suas linhas de saída e de outros recursos. O roteador pode associar a cada linha uma variável o qual reflete a utilização da linha. Assim, cada pacote recém-chegado é conferido para saber se sua linha de saída encontra-se em estado de advertência. Havendo algum estado de advertência, uma ação será tomada, dentre elas:

7.3.1. BIT DE ADVERTÊNCIA

Na antiga arquitetura DECNET assinalava o estado de advertência ativando um bit especial no cabeçalho do pacote, o que é feito no *frame relay.* Quando o pacote chega ao destino, a entidade de transporte copiava o bit na próxima confirmação a ser enviada de volta à origem. Em seguida, a origem interrompia o tráfego.

Enquanto estivesse no estado de advertência, o roteador continuava a definir o bit de advertência, e isso significava que a origem continuava a receber informações com o bit ativado. Assim, a origem monitora a fração de confirmações com o bit ativado e ajusta sua velocidade de transmissão. Enquanto os bits de advertência continuar a fluir, a origem continuava a diminuir sua taxa de transmissão. Quando diminui a velocidade de chegada das confirmações, a origem aumenta a taxa de transmissão.

7.3.2. PACOTES REGULADORES

Neste modelo o roteador enviará um pacote regulador ao host de origem, informando que deve interromper ou enviar mais lentamente os pacotes. O pacote original é marcado (um bit no cabeçalho é ativado) para que ele não venha a gerar mais pacotes reguladores ao longo do caminho e depois é encaminhado de forma habitual. Ao receber o pacote regulador, o host de origem é obrigado a reduzir o tráfego enviado ao destino especificado.

Este método ignora novos pacotes do mesmo destino por um tempo. Isso evita o excesso de *feedback.* Contudo, não funciona bem com longas distâncias ou grande largura de banda e há certa demora para avisar a origem.

7.3.3. PACOTES REGULADORES HOP A HOP

Em altas velocidades ou em longas distâncias, o envio de um pacote regulador para os hosts de origem não funciona bem devido à reação ser muito lenta. A solução é fazer com que o pacote regular tenha efeito em cada *hop* pelo qual passar. O efeito desse esquema é oferecer alívio rápido no ponto de congestionamento, ao preço de aumentar o consumo de buffers do fluxo ascendente. Assim o congestionamento pode ser cortado pela raiz sem perda de pacotes.

8. PROTOCOLO IP

O protocolo IP integra um sistema de entrega fim-a-fim. Dessa forma é um tipo de protocolo não orientados à conexão, sem controle de erros e sem reconhecimento. Isso significa que o protocolo IP não executa controle de erros sobre os dados da aplicação, controle de fluxo, seqüenciamento de dados e entrega ordenada.

O protocolo IP apresenta algumas características como às listadas abaixo:

- Utiliza um serviço de entrega denominado ***Best-Effort*** (Melhor esforço): Os pacotes não são descartados sumariamente, o protocolo torna-se não confiável somente quando há exaustão de recursos; Oferece ainda serviço não baseado em conexão.

- Apresenta um tamanho de datagrama variável. No caso do IPV4 seu tamanho máximo pode atingir 64 Kb;

- Realiza a fragmentação de datagramas com recombinação no destino. Isto garante suporte a redes intermediárias com MTU (*Maximum Transmission Unit*) diferentes;

- É responsável pelo roteamento de datagramas ou fragmentos;

- Provê envio e recebimento de erros através de um protocolo chamado ICMP.

É ao IP que compete levar a informação de um extremo ao outro na Internet, atravessando várias redes, potencialmente muito diferentes.

8.1. Datagrama IP

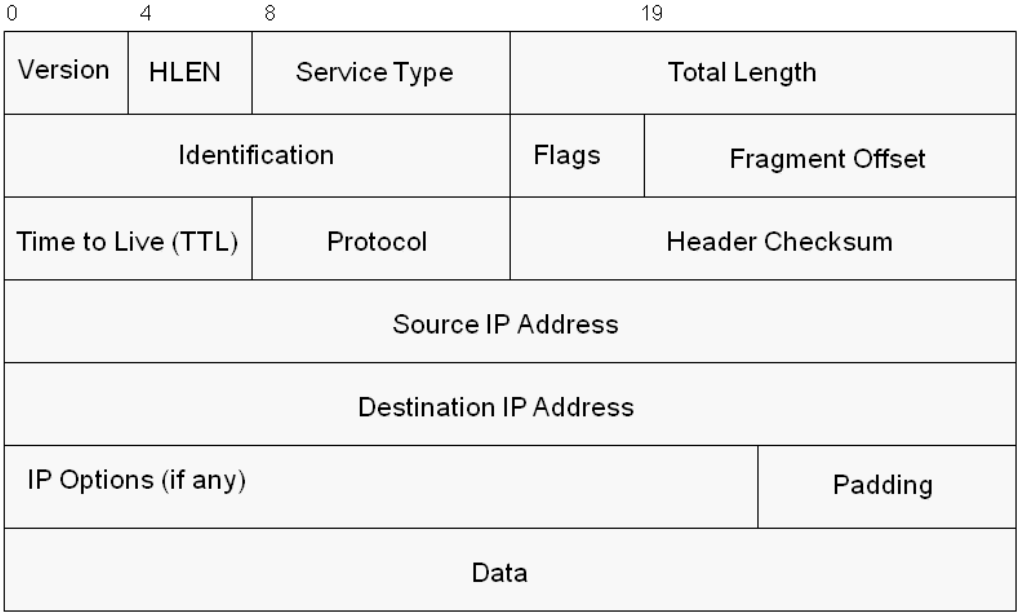


Figura 9 – Frame IP

Version: A Versão do protocolo hoje é ipv4, no entanto para o futuro será trabalhado a versão ipv6.
Hlen: tamanho do cabeçalho, devido a opções variáveis.
Service type: Atualmente ignorado.
Fragmentação controlada por:
Identification (campo tem o mesmo valor para cada fragmento de um datagrama)
Flags: "*don't fragment*" (o destino não sabe recombinar) e "*more fragments*";
Offset: offset do fragmento em múltiplos de 8 bytes;
Time to live: Decrementado durante a vida do datagrama para ter certeza que tabelas de roteamento corrompidas não manterão pacotes na rede para sempre; Datagrama descartado quando ttl chega a 0. Deveriam ser segundos, mas todo mundo decrementa a cada *hope*.
Protocol: icmp, udp, tcp, dentre outros;
Checksum: controle de erro. Deve ser recalculado a cada *hope* devido a mudanças de ttl;
Source/Destination: endereços discutidos mais à frente;
Padding: Para ter cabeçalho múltiplo de 32 bits;

8.2. Endereçamento IP

O endereço IP (*Internet Protocol*), de forma genérica, é um endereço que indica o local de um determinado equipamento (normalmente computadores) em uma rede privada ou pública.

O endereço IP, na versão 4 (IPv4), é um número de 32 bits escrito com quatro octetos representados no formato decimal (exemplo: 128.6.4.7). **A primeira parte do endereço identifica uma rede específica na inter-rede, a segunda parte identifica um host dentro dessa rede**. Dessa forma, os endereços IP podem ser usados tanto para nos referir a redes quanto a um host individual. Podemos também nos referir a todos os hosts de uma rede através de um endereço por difusão, quando, por convenção, o campo identificador de host deve ter todos os bits iguais a 1 (um). Um endereço com todos os 32 bits iguais a 1 é considerado um endereço por difusão para a rede do host origem do datagrama.

8.2.1. CLASSES IP

O IP utiliza cinco classes diferentes de endereços, contudo, efetivamente somente três:

CLASSE	FAIXA DE IP	Nº DE HOSTS POR REDE
A	1.0.0.0 até 126.0.0.0	16 777 216
B	128.0.0.0 até 191.255.0.0	65 536
C	192.0.0.0 até 223.255.255.254	256
D	224.0.0.0 até 239.255.255.255	*Multicast*
E	240.0.0.0 até 247.255.255.255	*Uso futuro; atualmente reservada a testes pela IETF*

A definição de tipo de endereço classes de endereços deve-se ao fato do tamanho das redes que compõem a inter-rede variar muito, indo desde redes locais de computadores de pequeno porte, até redes públicas interligando milhares de hosts.

8.2.2. CLASSES ESPECIAIS

Existem classes especiais na Internet que não são consideradas públicas, não são consideradas como endereçáveis, ou seja, **são reservadas**, por exemplo: para a comunicação com uma rede privada ou com o computador local (*localhost*).

Blocos de Endereços Reservados:

BLOCO DE ENDEREÇOS	DESCRIÇÃO	REFERÊNCIA
0.0.0.0/8	Rede corrente (só funciona como endereço de origem)	RFC 1700
10.0.0.0/8	Rede Privada	RFC 1918
14.0.0.0/8	Rede Pública	RFC 1700
39.0.0.0/8	Reservado	RFC 1797
127.0.0.0/8	Localhost	RFC 3330
128.0.0.0/16	Reservado (IANA)	RFC 3330
169.254.0.0/16	Zeroconf	RFC 3927
172.16.0.0/12	Rede Privada	RFC 1918
191.255.0.0/16	Reservado (IANA)	RFC 3330
192.0.0.0/24		
192.0.2.0/24	Documentação	RFC 3330
192.88.99.0/24	IPv6 para IPv4	RFC 3068
192.168.0.0/16	Rede Privada	RFC 1918
198.18.0.0/15	Teste de benchmark de redes	RFC 2544
223.255.255.0/24	Reservado	RFC 3330
224.0.0.0/4	Multicasts (antiga rede Classe D)	RFC 3171
240.0.0.0/4	Reservado (antiga rede Classe E)	RFC 1700

8.2.3. LOCALHOST

A faixa de IP 127.0.0.0 – 127.255.255.255 (ou 127.0.0.0/8) é reservada para a comunicação com o computador local (*localhost*). Qualquer pacote enviado para estes endereços ficarão no computador que os gerou e serão tratados como se fossem pacotes recebidos pela rede (*Loopback*).

O endereço de *loopback* local (127.0.0.0/8) permite à aplicação-cliente endereçar ao servidor na mesma máquina sem saber o endereço do host, chamado de *localhost*.

Na pilha do protocolo TCP/IP, a informação flui para a camada de rede, onde a camada do protocolo IP reencaminha de volta através da pilha.

8.2.4. REDES PRIVADAS

Dos mais de 4 bilhões de endereços disponíveis, três faixas são reservadas para redes privadas. Estas faixas não podem ser roteadas para fora da rede privada - não podem se comunicar diretamente com redes públicas. Dentro das classes A, B e C foram reservadas redes (normalizados pela RFC 1918) que são conhecidas como endereços de rede privados.

8.2.5. SUB-REDES

Uma sub-rede é uma divisão de uma rede de computadores. A divisão de uma rede grande em redes menores resulta num **tráfego de rede reduzido, administração simplificada e melhor performance de rede**.

Para criar sub-redes, qualquer máquina tem que ter uma máscara de sub-rede que define que parte do seu endereço IP será usado como identificador da sub-rede e como identificador do host.

As sub-redes servem para:

- Simplificar a administração de redes. As sub-redes podem ser usadas para delegar gestão de endereços, problemas e outras responsabilidades.

- Reconhecer a estrutura organizacional. A estrutura de uma organização (empresas, organismos públicos, etc.) pode requerer gestão de rede independente para algumas divisões da organização.

- Isolar tráfego por organização. Acessível apenas por membros da organização, relevante quando questões de segurança são levantadas.

- Isolar potenciais problemas. Se um segmento é pouco viável, podemos fazer dele uma sub-rede.

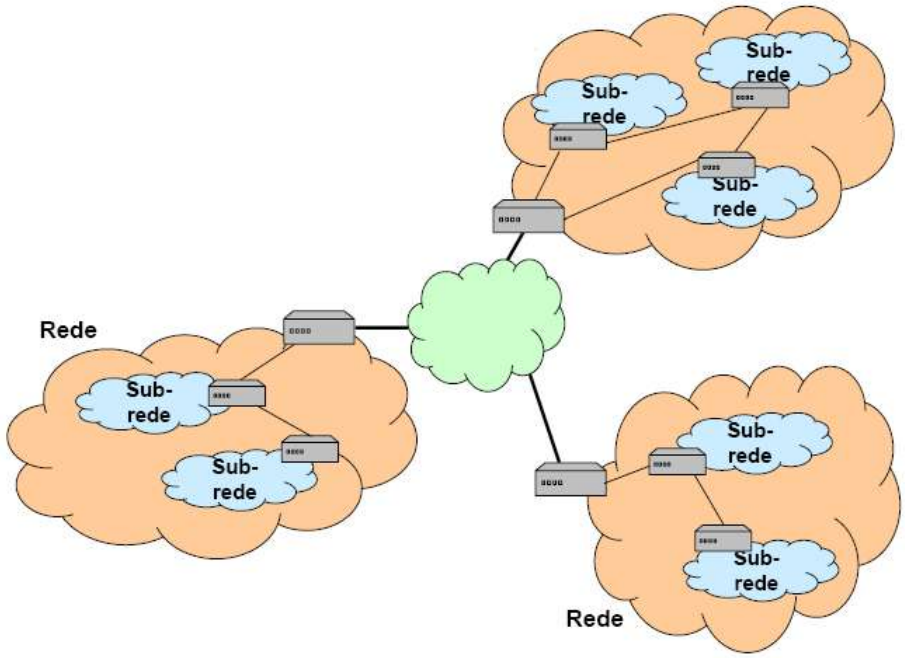


Figura 10 - Sub-redes

8.2.6. MÁSCARA DE SUB-REDE

A máscara de sub-rede é um endereço de 32 bits usado para bloquear (mascarar) uma parte do endereço IP para se distinguir a parte de identificador de rede e a parte de identificador de computador (*Host*).

Cada computador numa rede TCP/IP precisa ter uma mascara de sub-rede (é obrigatório). Isto pode ser conseguido a partir de uma máscara padrão de classe A, B ou C (usada quando a

rede não necessita de ser dividida em sub-redes) ou através de uma máscara personalizada (usada quando a rede precisa de ser dividida em sub-redes). Na mascara padrão todos os bits que correspondem à parte do identificador da rede são colocados "1", que convertido para decimal obtêm-se o valor 255 (11111111 = 255). Todos os bits que correspondem à parte do Host são colocados a "0", que convertido para decimal obtêm-se o valor 0 (00000000 = 0).

255	255	255	0
11111111	11111111	11111111	00000000
Rede	Rede	Rede	Host

As classes dão certa flexibilidade na distribuição dos endereços. Uma vez que o endereço IP tem tamanho fixo, uma das opções dos projetistas seria dividir o endereço IP em duas metades, dois bytes para identificar a rede e dois bytes para a estação. Entretanto isto traria inflexibilidade, pois só poderiam ser endereçados 65.536 redes, cada uma com 65.536 estações. Uma rede que possuísse apenas 100 estações estaria utilizando um endereçamento de rede com capacidade de 65536 estações, o que também seria um desperdício.

É importante conceber que dentro de uma faixa de IP há dois endereços especiais denominados endereço de rede e endereço de broadcast. O primeiro com todos os bits iguais a zero e o segundo com todos os bits iguais a um.

Para estabelecer uma comunicação direta, servidores têm que ter os mesmos endereços de rede. Se os servidores tiverem endereços de rede diferentes, então há necessidade de usar um roteador para conectar dois segmentos de rede. **Um roteador pode conectar seguimentos de rede somente se eles tiverem endereços de rede diferentes.**

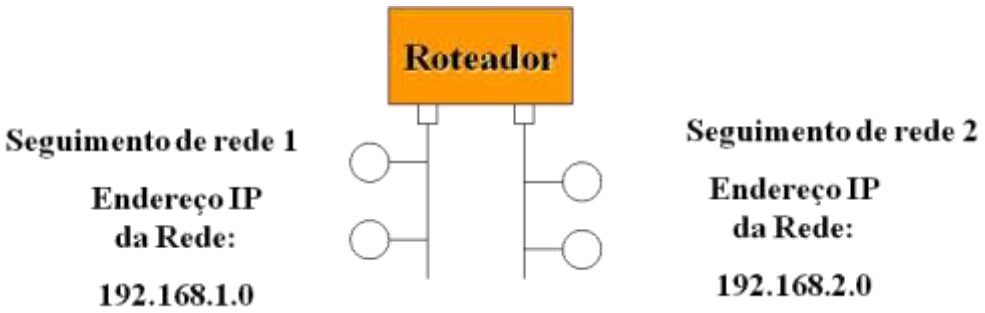


Figura 11 – Segmentos de rede

Exemplos de endereçamento

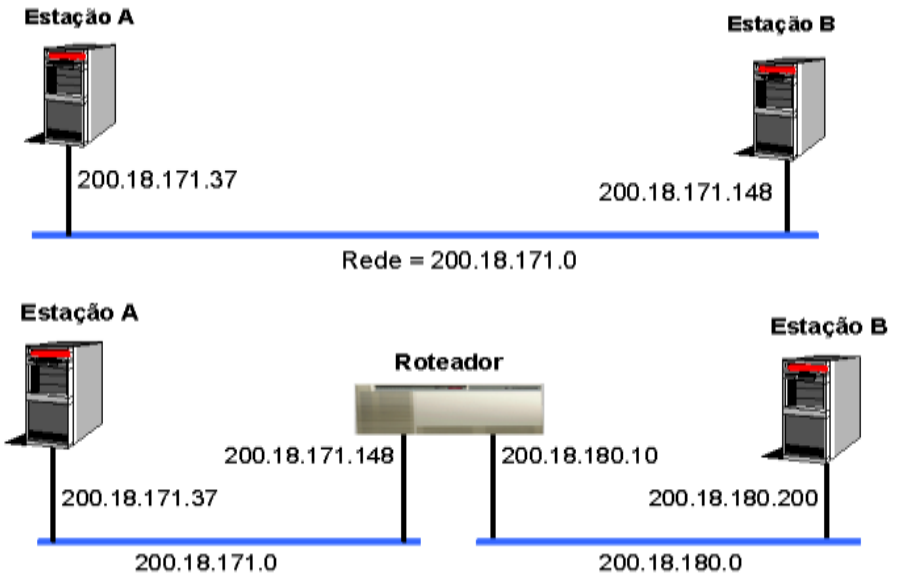


Figura 12 - Exemplos de endereçamento

A divisão de endereçamento tradicional da Internet em classes causou sérios problemas de eficiência na distribuição de endereços. Cada rede na Internet, tenha ela 5, 200, 2000 ou 30.000 máquinas deveria ser compatível com uma das classes de endereços. Desta forma, uma rede com 10 estações receberia um endereço do tipo classe C, com capacidade de endereçar 254 estações. Isto significa um desperdício de 244 endereços. Da mesma forma, uma rede com 2.000 estações receberia uma rede do tipo classe B, e desta forma causaria um desperdício de 63.534 endereços.

O número de redes interligando-se à Internet a partir de 1988 aumentou, causando o agravamento do problema de disponibilidade de endereços na Internet, especialmente o desperdício de endereços em classes C e B. Desta forma, buscou-se alternativas para aumentar o número de endereços de rede disponíveis sem afetar o funcionamento dos sistemas existentes. A melhor alternativa encontrada foi flexibilizar o conceito de classes - onde a divisão entre rede e host ocorre somente a cada 8 bits.

A solução encontrada foi utilizar a divisão da identificação de rede e host no endereçamento IP de forma variável, podendo utilizar qualquer quantidade de bits e não mais múltiplos de 8 bits conforme ocorria anteriormente. Um identificador adicional, a **máscara**, identifica em um endereço IP - qual porção dos bits é utilizada para identificar a rede e qual porção dos bits para host.

A máscara pode ser compreendida também como um número inteiro que diz a quantidade de bits 1(um) utilizados. Por exemplo, uma máscara com valor 255.255.255.192, poderia ser representada como /26. Este tipo de notação é empregada em protocolos de roteamento mais recentes.

8.2.7. CONSTRUINDO SUB-REDES

Antes de tudo, é importante memorizar a tabela abaixo:

128	128	10000000
192	128 + 64	11000000
224	128 + 64 + 32	11100000
240	128 + 64 + 32 + 16	11110000
248	128 + 64 + 32 + 16 + 8	11111000
252	128 + 64 + 32 + 16 + 8 + 4	11111100
254	128 + 64 + 32 + 16 + 8 + 4 + 2	11111110
255	128 + 64 + 32 + 16 + 8 + 4 + 2 + 1	11111111

Quando se depara com uma máscara de rede e se precisa determinar o número de sub-redes, hosts válidos e endereços de *broadcast* que a máscara define tudo o que você tem a fazer é responder a cinco perguntas:

1. Quantas sub-redes tal máscara produz?
2. Quantos endereços de hosts válidos são obtidos por sub-rede?
3. Quais são as sub-redes válidas?
4. Quais os hosts válidos em cada sub-rede?
5. Qual o endereço de broadcast de cada sub-rede?

1) Quantas sub-redes? 2^x = quantidade de sub-redes, onde "x" representa o número de bits "mascarados" ou número de "1s".
Por exemplo: 11000000(corresponde a 192 na base 10) seriam $2^2 = 4$. Nesse caso, haveria quatro sub-redes possíveis com tal máscara.

2) Quantos hosts válidos por sub-rede? $2^y - 2$ = quantidade de hosts válidos, onde "y" representa o número de bits disponíveis para manipulação dos endereços de host, ou o número de "0s".
Por exemplo: 11000000 seria $2^6 - 2 = 62$. Neste caso, existem 62 endereços válidos para hosts por sub-rede.

3) Quais são as sub-redes válidas? 256 – máscara de rede = valor da sub-rede base. A esse resultado, soma-se o valor obtido até que se atinja o número da máscara (que seria inválido).
Seguindo nosso exemplo: 256 – 192 = 64 (número base e primeira sub-rede válida). 64 + 64 = 128 (segunda sub-rede válida). 128 + 64 = 192 (valor da máscara = sub-rede inválida). Portanto, as sub-redes válidas seriam 64 e 128.

4) Qual o endereço de broadcast para cada sub-rede? O endereço de *broadcast* seria o valor imediatamente anterior ao valor da próxima sub-rede (ou da máscara, se estivéssemos falando da última sub-rede na seqüência).
Em nosso exemplo, temos as sub-redes 64 e 128. O endereço de *broadcast* da primeira seria 128 – 1 =127. Já o da segunda 192 (valor da máscara) – 1 = 191.

5) Quais os hosts válidos? Os valores válidos seriam os compreendidos entre as sub-redes, menos todos os bits ligados e desligados. A melhor maneira de se identificar esses valores é se descobrindo as sub-redes válidas e os endereços de *broadcast* de cada uma. Em nosso exemplo,

os hosts válidos estariam compreendidos nos intervalos entre 65-126 para a primeira sub-rede e 129-190 para a segunda (pois 64 e 127 são os valores que definem as respectivas.

2.2.7.1 Emprestando bits

Vamos imaginar que eu precise de uma rede para pelo menos 1.000 hosts.

Como tem que ser múltiplo binário, ou seja $X^{2,}$ o mais próximo que temos a isso é 1024 (2^{10}). Logo, além do último octeto (8 bits) precisamos "pegar emprestado" mais 2 bits.

Máscara classe C padrão 255.255.255.0 ou 11111111.11111111.11111111.00000000;
Pegando 2 bits emprestados do terceiro octeto ficaria:
11111111 11111111 11111100 00000000 ou 255.255.252.0

Sendo os 2 primeiros octetos "fixos" da rede teríamos para sub-rede 64 para rede (2^6) e 1024 para host (2^{10}) o que nos daria 1024 endereços de host disponíveis para cada uma da 64 sub-redes como 1 endereço é de rede e 1 de *broadcast* teríamos que diminuir 2 que daria 1022 endereços validos por sub-rede.

2.2.7.2. Exemplos

Quando se deseja quer obter 2 redes lógicas de um endereço classe C , é preciso modificar a máscara de sub-rede para 255.255.255.128. Observe a figura e aplique as 5 perguntas conforme ensinado acima.

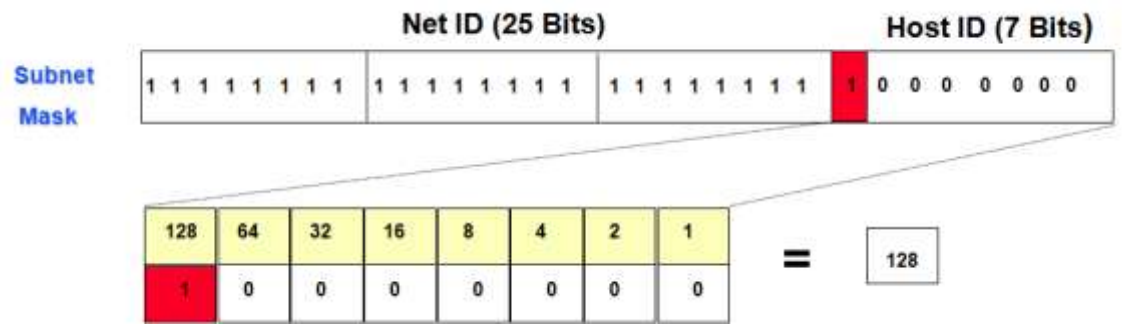


Figura 13 - Cálculo de sub-rede

Faixa total: 192.168.1.0 a 192.168.1.127
Endereço de rede: 192.168.1.0
End. Broadcast: 192.168.1.127
End. Dos hosts: 192.168.1.1 a 192.168.1.126

} Rede 0

Faixa total: 192.168.1.128 a 192.168.1.255
Endereço de rede: 192.168.1.128
End. Broadcast: 192.168.1.255
End. Dos hosts: 192.168.1.129 a 192.168.1.256

} Rede 1

Quando se deseja quer obter 4 redes lógicas de um endereço classe C , é preciso modificar a máscara de sub-rede para 255.255.255.192. Observe a figura e aplique as 5 perguntas conforme ensinado acima.

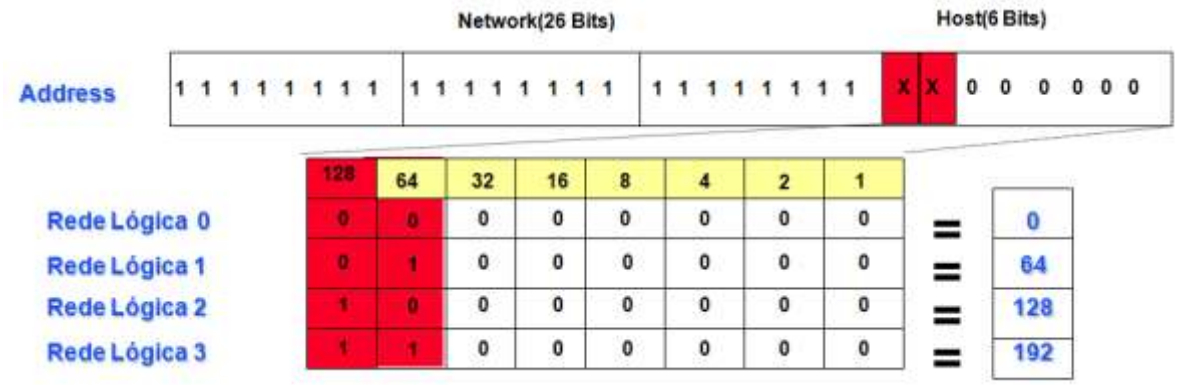


Figura 14 - Cálculo de sub-rede

Note que, para que exista comunicação entre as sub-redes é necessário um roteador, uma vez que as sub-redes não se comunicam.

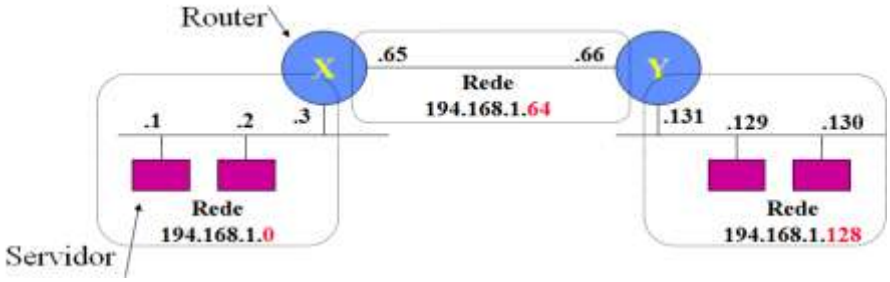


Figura 15 - Divisão da rede

Como calculado é possível usar a máscara de sub-rede 255.255.255.192 e obter 4 redes com os seguintes endereços IP:

- 192.168.1.0
- 192.168.1.64
- 192.168.1.128
- 192.168.1.192

8.2.8. CALCULANDO A REDE QUE DETERMINADO IP PERTENCE

Este cálculo é feito pelo roteador para determinar a rede ou sub-rede para a qual um pacote deve ser enviado.

Para determinar qual rede ou sub-rede host pertence é necessário realizar uma operação AND.

Exemplos:

Endereço Completo	192.168.5.10	11000000.10101000.00000101.00001010	AND
Máscara da Sub-Rede	255.255.255.0	11111111.11111111.11111111.00000000	
Rede/Sub-Rede	192.168.5.0	11000000.10101000.00000101.00000000	

Endereço Completo	192.168.5.130	11000000.10101000.00000101.10000010	AND
Máscara da Sub-Rede	255.255.255.192	11111111.11111111.11111111.11000000	
Rede/Sub-Rede	192.168.5.128	11000000.10101000.00000101.10000000	

9. EXERCÍCIOS

1.a) Dos seguintes endereços de rede IP, escolher um endereço IP classe B: 192.168.1.0 - 198.124.144.0 - 146.44.63.0 - 10.10.1.0

1.b) Qual é a máscara de sub-rede default para endereço IP classe B?

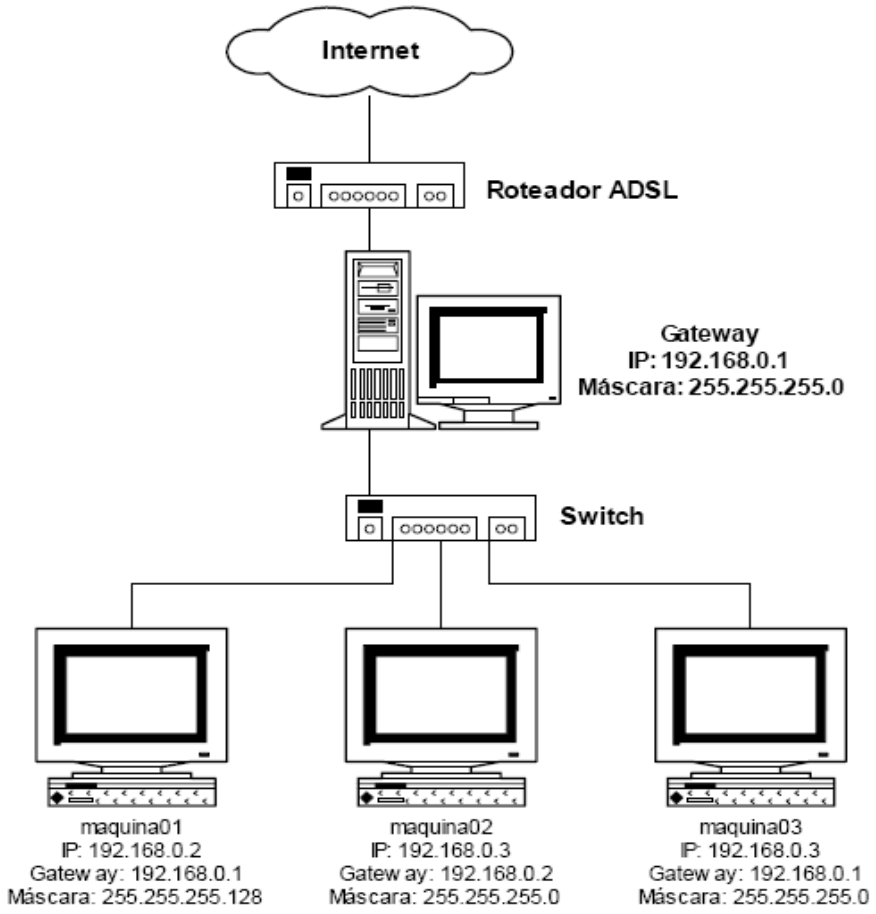
1.c) Agora modifique o número da mascara de sub-rede para obter sub-redes com no máximo 6 (seis) servidores cada uma.

2) A qual rede/Sub-rede pertence o endereço IP 200.110.10.20 com máscara 255.255.255.0.

3) Dada a figura abaixo:

a) A maquina03 está com o endereço IP 192.168.0.3. Esta configuração gerou um erro no sistema, sendo mostrada uma mensagem de conflito de endereçamento IP. Como este problema pode ser resolvido?

b) Suponha o problema acima resolvido. A situação agora é a seguinte: uma das máquinas não consegue se comunicar com as outras da sub-rede. Que máquina é essa e que configuração deve ser feita para resolver esse problema?



4.a) Admita que você tenha recebido o bloco de rede 200.35.1.0/24. Defina um prefixo de rede que permita a criação de 20 hosts em cada sub-rede.

4.b) Qual o número máximo de hosts que podem ser designados em cada sub-rede?

4.c) Qual o número máximo de sub-redes que podem ser definidas?

4.d) Especifique as sub-redes de 200.35.1.0/24 no formato.