

# Unidade II

## 3 ELEMENTOS E ARQUITETURA DE REDES NGN

### 3.1 Arquitetura em camadas de NGN

Um diferencial da arquitetura NGN é a divisão em camadas. A arquitetura decompõe os elementos de rede em quatro camadas funcionais:

- camada de acesso;
- camada de núcleo ou central;
- camada de controle;
- camada de serviços.

Vejam a arquitetura das camadas da rede convergente NGN:

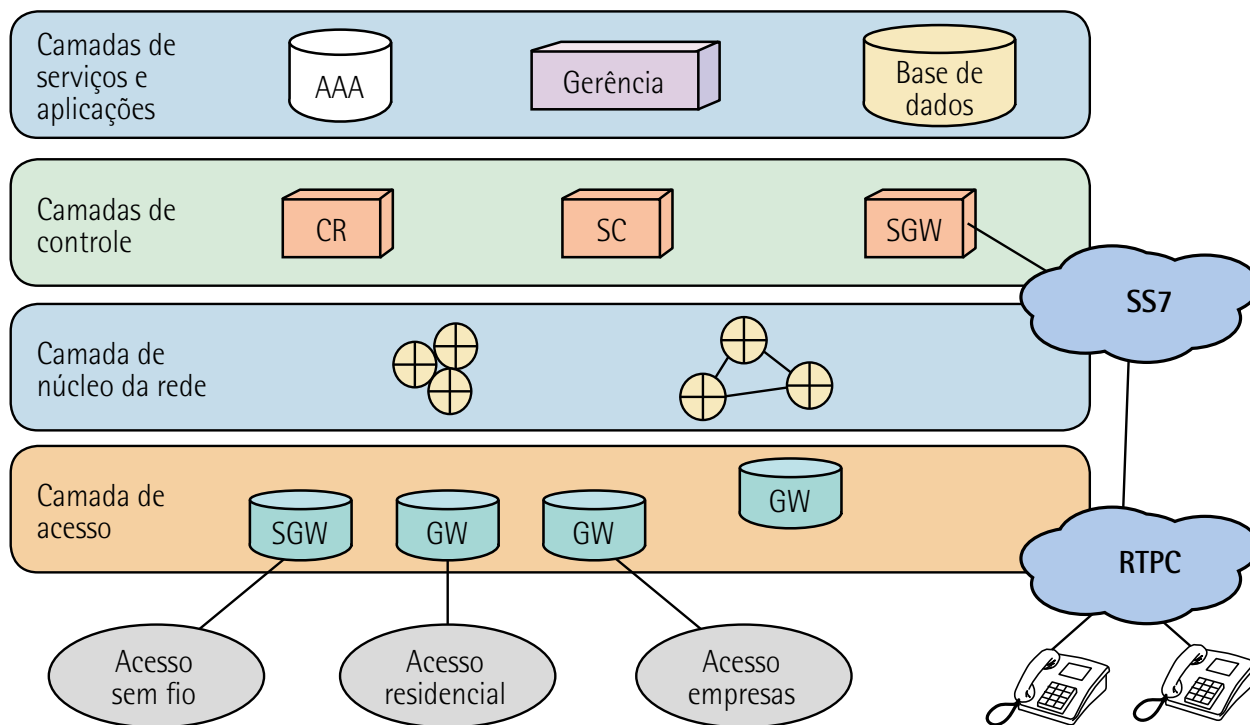


Figura 15 – Arquitetura de camadas NGN

- Camada de acesso (*edge layer*): responsável por prover interfaces para os dispositivos dos usuários ou para outras entidades de rede no plano de adaptação do fluxo de dados do usuário às características da rede. Também se encarrega de agregação de tráfego, controle de QoS, gerenciamento de *buffer*, armazenamento, escalonamento, filtragem de pacotes, classificação de tráfego, marcação, policiamento e formatação.
- Camada central (*core layer*): possui a função de comutação, estabelecendo rotas para os equipamentos de acesso e de núcleo para o encaminhamento do tráfego de dados.
- Camada de controle (*control layer*): responsável por suportar multimídia e outros serviços e funções de controle, além daquelas envolvidas no processo de chamada são divididas em duas funções:
  - controle de serviço – autenticação de usuários, identificação de usuários, controle de admissão de serviços e as funções do servidor de aplicativos.
  - controle de operadoras do sistema – controle da rede, controle da admissão de recurso, política de rede, fornecendo conectividade dinâmica ao sistema.

### 3.2 Estrato de serviços e estrato de transporte

Nas redes NGN, a separação entre serviços e transporte é representada por dois blocos distintos, conhecido como estrato de funcionalidade. As funções de transporte residem no estrato de transporte e as funções de aplicações, no estrato serviço. A figura seguinte representa a separação entre transporte e serviço.

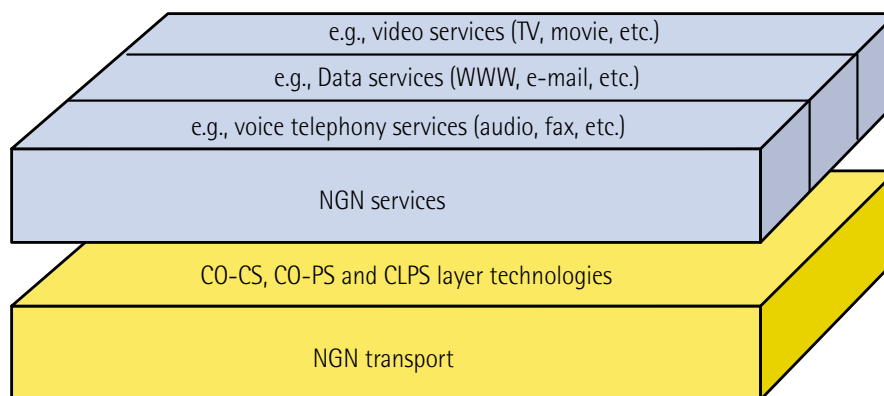


Figura 16 – Separação entre serviço e transporte

A figura a seguir mostra uma visão mais geral da arquitetura de uma rede NGN, e não somente da fronteira entre os estratos de serviços e transporte. Nelas, a separação entre serviços e transporte é apresentada por dois blocos distintos, conhecido como estrato de funcionalidade. As funções de transporte residem no Estrato de Transporte (Transport stratum) e as funções relacionadas a aplicações residem no Estrato Serviço (Service stratum).

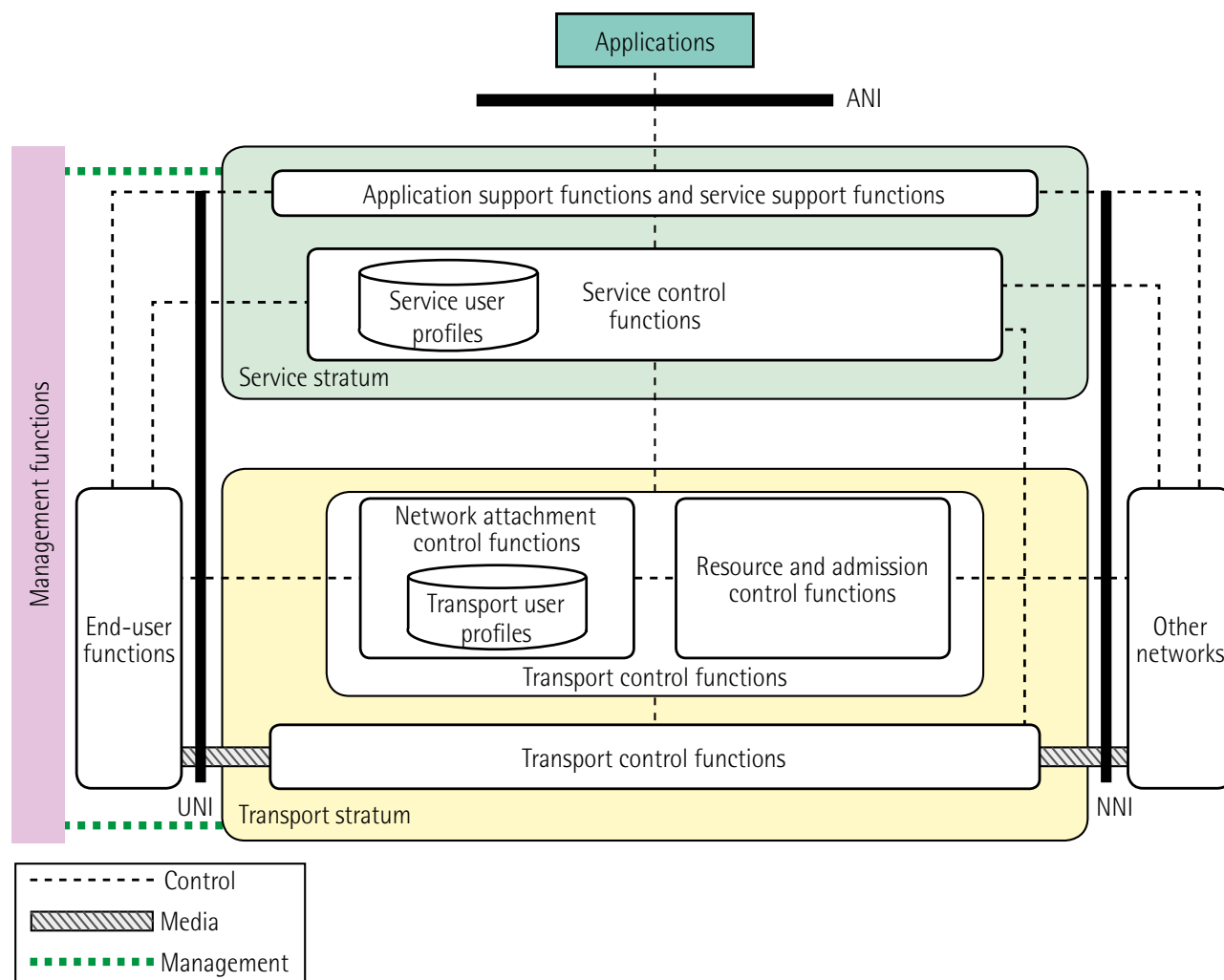


Figura 17 – Visão geral da arquitetura NGN

O estrato de transporte provê funções de usuário que transferem dados e as funções de controle e gerência dos recursos de transporte para carregar estes dados entre as entidades terminais. O dado carregado pode ser a própria informação de usuário, controle ou gerenciamento. Para tal, são fixadas associações dinâmicas e estáticas a fim de acompanhar a transferência de informação entre as entidades. Um estrato de transporte NGN é implementado por múltiplas redes em camada. Analisando do ponto de vista de arquitetura, cada camada no estrato de transporte é considerada por seu próprio plano de usuário, controle e gerência.

Essa camada provê IP baseado na conectividade e pode suportar a qualidade de serviço. Talvez seja dividido em rede de acesso e redes centrais.

As funções de acesso gerenciam o ingresso à rede. Uma variedade de acessos tanto com fio e sem fio devem ser suportados pela NGN. As funções de transporte de acesso gerenciam o tráfego da informação através da rede de acesso. As funções de borda processam a sinalização, mídia e gerenciamento de tráfego para agregação futura, se necessária, e a entrega para a rede central.



### Observação

Em relação às funções centrais de transporte, estas são responsáveis por carregar o tráfego nas redes centrais. Pode-se entender o transporte central como uma rodovia com diversas pistas, não exigindo sinais de controle de tráfego.

As funções de *gateway* proveem e suportam recursos para interagir com outras redes, já as de controle de transporte incluem as entidades funcionais descritas a seguir:

- Funções de controle de recursos e admissão estão envolvidas sem controle de admissão e atividades de controle de portas para voz, vídeo, dados e sessões móveis. O controle de admissão em geral envolve autenticação e autorização.
- Funções de controle de anexos de rede fornecem inicialização de funções do usuário final para acessar serviços NGN.
- Perfis de usuário de transporte são usualmente especificados e executados usando um conjunto de bancos de dados cooperativos. Eles são utilizados durante o controle de transporte de informações do usuário.

Por sua vez, o estrato de serviço fornece funções do usuário que transferem dados relativos a serviço para habilitar serviços e aplicações de usuário e armazena perfis de serviço para usuários. Esses serviços de usuário são fixados por múltiplas camadas dentro do estrato de serviço. O estrato de serviço NGN é associado à aplicação e sua operação a ser executada entre as entidades pares. Por exemplo, serviços podem ser relacionados a aplicações de voz, dados ou vídeo, arranjados separadamente ou em alguma combinação no caso de aplicações multimídia. De uma perspectiva de arquitetura, considera-se que cada camada no estrato de serviço tem seus próprios planos de usuário, controle e gerenciamento.

- Perfis de serviço de usuário (*service user profiles*): tais funções são normalmente especificadas e implementadas usando um conjunto de bancos de dados cooperativos. Esses dados são utilizados para permitir e gerenciar o acesso aos serviços NGN pelo usuário.
- Funções de controle de serviço: envolvem registro de nível de serviço, autenticação e autorização, podendo incluir NGN, dados de controle e de sessão.



### Saiba mais

O livro a seguir é uma fonte de informação a respeito das redes NGN.

PLEVYAK, T.; SAHIN, V. *Next generation telecommunications networks, services, and management*. EUA: IEEE Press, 2010.

### 3.3 Gerenciamento

As funções de gerenciamento incluem as funções de controle de rede e serviço, base de informações de gerenciamento (MIB) e interfaces dentro da rede. O objetivo é garantir o nível esperado de segurança, confiabilidade, disponibilidade e QoS para os serviços NGN faturáveis. Isso fornece os seguintes serviços na rede: gerenciamento de falhas, de configuração, de contabilização, de desempenho e de segurança.

#### 3.3.1 Gerenciamento de falhas

Aborda o gerenciamento de serviços e sessões nos níveis acordados, mesmo quando existem falhas, incluindo sobrecargas e desastres, nos estratos de serviço, aplicação e transporte. As funções podem incluir monitoramento e controle da utilização de recursos durante a instalação, manutenção e lançamento de sessões para serviços NGN.

Desde NGN, suporta uma multidão de serviços. Recomenda-se que a filtragem e a correlação apropriada sejam usadas para gerenciar falhas específicas do serviço. Quando os serviços abrangem várias tecnologias e recursos administrativos e domínios, como seria a exemplo da interoperabilidade de redes e serviços, um ou mais mecanismos de gerenciamento de falhas são necessários por acordo bilateral. Isso ajudará a manter a transparência do serviço no NNI.

#### 3.3.2 Gerenciamento de configuração

Refere-se ao desenvolvimento, monitoramento e gerenciamento das configurações de *hardware* e *software* de dispositivos, elementos e sistemas com o objetivo de manter as operações de rede sem afetar negativamente os serviços e as receitas. Por exemplo, muitas vezes é desejável armazenar o teste e configurações aprovadas dos terminais do usuário final em um servidor de rede para que os usuários possam baixá-los quando eles acessarem novos recursos e serviços.

Embora essa prática seja muito comum na indústria de telefonia celular, internet e televisão baseada em IP (IPTV), prestadores de serviços também estão achando cada vez mais útil. Da mesma forma, para gerenciamento de configuração de elementos especializados de rede (*on-line* e *off-line*), servidores são comumente usados.

#### 3.3.3 Gerenciamento de contabilização

No contexto das redes NGN, o gerenciamento de contabilização envolve o registro da utilização de serviços e recursos de rede com o objetivo de criar um registro de faturamento. A gravação pode ser feita em vários formatos, incluindo os valores brutos separados por vírgulas, que podem ser alimentados para formatar dados em outros formatos aceitáveis a fim de que o cliente crie contas legíveis.

A medição do uso de serviços e recursos pode ser feita de várias maneiras. Por exemplo, o paradigma *per-service per-user* é rotineiramente utilizado para usuários de dados de voz e mensagens de texto, *download* de vídeo e jogos, a menos que o faturamento de taxa fixa seja assumido. Para clientes corporativos, gravação de rede e uso de serviços e eventos como

interrupção de serviço e tempo de reparo para gerenciar o contrato de nível de serviço (SLA) são mais importantes do que documentar o uso do serviço.

### 3.3.4 Gerenciamento de desempenho

A gestão de desempenho está preocupada com o monitoramento da *performance* dos elementos de redes, tanto os *links* de transmissão como os dispositivos nodais, com o objetivo de manter o nível desejado de qualidade de serviço ou SLA. Ambos os dispositivos e técnicas de monitoramento ativo e passivo são comumente usados em NGNs. O desafio, no entanto, é localizar e endurecer o monitoramento do desempenho e sistemas de gestão uniformemente na rede sem sobrecarregar o serviço de criação, gerenciamento e entrega de módulos.

O monitoramento passivo requer o uso de divisores nos *links* de transmissão e *hardware* especial para filtragem *off-line*, armazenamento e análise dos dados capturados. Medições ativas podem ser realizadas sem sobrecarga significativa, em qualquer tempo, e para qualquer período desejado.

Para *links* de transmissão, os parâmetros de interesse são: taxa de transferência e utilização, tempo de atividade, de inatividade, tempo para recuperar-se graciosamente de sobrecargas e desastres etc. Para dispositivos nodais como *switches* e roteadores, parâmetros como atraso, tempo de resposta, tempo de alternância local ou remoto para serviço de manutenção de qualidade durante falhas e sobrecarga são vitais.

### 3.3.5 Gerenciamento de segurança

O NGN inclui identificação, autenticação, autorização, certificado etc. do usuário em um acesso. Caso contrário, será muito difícil manter a continuidade do serviço quando o usuário (ou sessão) se desloca de uma rede de acesso para outra ou faz *roaming* de um prestador de serviços para o outro.

Como a NGN usa transporte baseado em IP, são necessários mecanismos para proteger o serviço e a rede contra *worms*, vírus, intrusos, negação de serviço e outros ataques. Mecanismos simples de monitoramento podem não ser suficientes.

Medidas proativas devem ser invocadas. Grupos de estudo da UIT (T 13 e 17) abordam esses problemas. Mais uma vez, quando os serviços abrangem várias tecnologias e domínios administrativos, como seria o caso da interoperabilidade de redes e serviços, são necessários um ou mais mecanismos de gestão de segurança por acordo bilateral. Isso ajudará a manter a transparência do serviço com segurança, sobretudo em termos das funções da Rede de Gerenciamento de Telecomunicações (TMN). Isso auxiliará a manter a transparência do serviço com segurança, o que envolve as camadas de gerenciamento de elemento e gerenciamento de rede.



#### Lembrete

As cinco áreas de gerenciamento são: gerenciamento de falhas, de configuração, de contabilização, de segurança e de desempenho.

### 3.4 Funções das aplicações

Este bloco funcional suporta interfaces de programação de aplicativos de serviço (API), controle de sessão, lógica de serviço, tradução e lógica de roteamento, diretório e política de funções de gerenciamento em toda a rede. Algumas das funções específicas das aplicações devem providenciar:

- Serviços de mensagens, como aqueles usados em *e-mail* e correio de voz.
- Serviços de processamento, como reconhecimento automático de fala e cartão de crédito em processamento.
- Serviços de telefonia IP com valor agregado, como a segunda linha virtual, baseada nas chamadas gratuitas via *web*.
- Serviços habilitados para diretório, como conversão de números (Freephone, 8xx), portabilidade numérica e serviços de acompanhamento de número único para telefonia local.
- Serviços de nomenclatura e endereçamento IP, incluindo DNS, DHCP e Radius (DNS significa Domain Name System, conforme definido no IETF RFC 1035, protocolo de configuração dinâmica de *hosts* ou DHCP, definido no IETF RFC 2131, discagem de autenticação remota no serviço do usuário ou Radius, como definido em IETF RFC 2865).
- Serviços Class 5/7, tais como chamada em espera, reencaminhamento de chamadas, conferência pedindo serviço de comunicações de voz (aplicativos de telefonia).
- Rede Privada Virtual (VPN) para voz e dados.
- Serviços de largura de banda, VPN ótica (IETF RFC 2547) etc.

#### Outras redes: domínios de terceiros

Os domínios são definidos pela administração da rede para dar estrutura à rede e para tornar o gerenciamento da rede o mais simples possível. A estrutura de domínio pode representar o alcance de um domínio com a alocação de um endereço específico, fixar o alcance do protocolo de roteamento interno – Interior Gateway Protocol (IGP), definir as extremidades do protocolo de roteamento externo – Exterior Gateway Protocol (EGP), corresponder à região de qualidade de serviço garantida e equivaler à região definida por um nível de segurança assegurada.

#### Funções do usuário final: cliente, dispositivos e redes domésticas

Tradicionalmente, esse domínio contém equipamentos, cabos e funções necessárias nas instalações residenciais do cliente ou nas instalações de pequenas e médias instituições. Desde que as tradicionais empresas de telecomunicações entraram no negócio de entretenimento, elas evoluíram os pares de fios de cobre trançados para *links* de alta velocidade DSL ou fibra – ou cabos coaxiais – para que possam oferecer serviços de banda larga (vídeo e internet) aos seus clientes. Para tal, exige-se a instalação de *modems* adicionais, roteador, dispositivos de segurança, videoconversores e decodificadores para residências.

Da mesma forma, operadoras de TV a cabo tradicionais estão oferecendo serviços de telefonia digital baseados na internet usando a versão do Docsis (Data Over Cable Specification Service Interface) e outros padrões (para mais detalhes, consulte <[www.cablelabs.com](http://www.cablelabs.com)>). Esses tipos de evolução para apoiar serviços multimídia criam uma infinidade de redes e dispositivos dentro de casa, e não é fácil solucionar o problema de depuração, diagnóstico e instalação de serviços.

### Protocolo de Internet (IP): sempre presente em redes NGN

Independentemente de ser fixo ou sem fio na camada física, a camada de rede vai usar de forma ubíqua o IP (IETF RFC 791 para IPv4 e RFC 2460 para IPv6). As variantes de IP acentuadas a seguir e o complemento de recursos estão atualmente disponíveis na indústria para mantê-lo como a cola mais útil na camada de rede. Concebido para ser o protocolo da internet e de Ethernet LAN (Local Area Network) e firmado como protocolo padrão para transferência do tráfego de dados, ele será naturalmente o protocolo predominante também nas redes públicas, porém essas redes deverão ser desenhadas para uma operação otimizada de pacotes nesse protocolo.

Além dos protocolos IPv4 e IPv6, foi desenvolvido o protocolo Mobile Internet Protocol versão 6 (MIPv6). Com o intuito de apoiar a mobilidade de dispositivos, um conjunto de extensões para o IPV6 original foi proposto no IETF (RFC 3775 e 3776).

Assim, as informações são transportadas da fonte para o destino do modo mais otimizado possível. Com essa filosofia, houve vasta proliferação de aplicações e a crescente integração de pequenos dispositivos que usam IP, como em *tablets*, telefones, carros, equipamentos para uso em imóveis e dispositivos pessoais como *wearables*. Se esses dispositivos possuírem uma única identificação global (endereço IP), a faixa do atual protocolo IPv4 não será suficiente e a faixa do IPv6 deverá ser implementada. O IPv6 também incorpora novas facilidades para segurança, QoS, autoconfiguração e mobilidade, entre outras.

## 3.5 Principais equipamentos de uma rede NGN

Existem diversos *gateways* presentes em uma rede NGN, como Media Gateway, Softswitch, Media Gateway Controller, Signaling Gateway e Access Gateway.

### 3.5.1 Media Gateway

É o elemento essencial que faz a interconexão entre a rede comutada e a rede de pacotes, possibilitando a conversão da mídia de voz da rede telefônica para a rede de dados e vice-versa. Assim, Media Gateway é o componente de transição entre NGN-IP e TDM (Time Division Multiplexing). Além dessa conversão e manipulação de mídias, realiza outras atividades como compressão, cancelamento de eco, notificação de eventos, envio e retenção de tons. Também faz conexões ponto a ponto e conferências.

O Media Gateway retém a informação de todos os recursos e, em caso de enlaces ocupados, ele garante o tratamento apropriado de gerenciamento para cada situação. Até o encerramento de uma chamada, esse tipo de *gateway* provê o MGC (Media Gateway Controller) de informações da qualidade de serviço para fins de bilhetagem. O Media Gateway poderá terminar uma conexão de circuitos, sejam



elas linhas, troncos ou *loop*, transformando em pacotes o *stream* de dados se a chamada ainda não estiver nesse estado, e então liberar o tráfego para a rede IP.

Como *gateway*, esse elemento de rede apenas manipula a mídia, não possuindo nenhuma inteligência agregada e necessitando de um controle de um elemento de rede hierarquicamente superior, o Softswitch, via um protocolo de controle, como o MGCP ou Megaco/H.248. A falta de inteligência de um *gateway* possui motivo, pois demandaria que Media Gateways fossem constantemente atualizados para a introdução de novos serviços e usuários, tornando a rede de difícil gerenciamento e pouca evolução.

Desse modo, é possível a interligação de assinantes convencionais com assinantes IP ou *softphones* (PCs com *software* apropriado), ou mesmo a outros assinantes convencionais através de um trecho da rede IP.

### Requerimentos de um Media Gateway

É possível classificar suas principais características:

- Interfaces diretas aos mundos PSTN/ISDN e IP/ATM.
- Conversão em tempo real de Voz sobre TDM para Voz sobre IP.
- Protocolo de controle para uma inteligência de serviços centralizada e separação dos serviços do transporte.
- Integração densa para uma baixa ocupação de espaço e consumo.



Figura 18 – Símbolo para o Media Gateway

### 3.5.2 Softswitch

Também chamado de Call Feature Server ou Media Gateway Controller, é o elemento central da rede NGN, que contém sua inteligência e controla todos os demais elementos da rede, sendo considerado o cérebro da rede NGN. Ele tem autonomia de controlar vários *medias gateways* de uma rede TCP/IP. Pelo fato de o Softswitch fazer a divisão entre a sinalização, controle e manipulação da mídia pelos *gateways*, permite uma maior flexibilidade para a evolução das redes e realiza o controle da chamada, bem como implementa as facilidades e serviços suplementares ofertados. Para realizar o controle da chamada, envolvendo elementos distintos da rede, é um manipulador de sinalizações, seja da rede comutada (SS7 – Isup), seja da rede de pacotes (H.323, SIP, MGCP ou Megaco).

Para efetivar as centenas de serviços suplementares, o Softswitch deve ser capaz de entender a lógica de cada serviço e traduzi-la em comandos adequados a qualquer elemento da rede.

Um dos pontos principais da rede NGN é a separação na arquitetura entre manipulação da mídia (pelos *gateways*) e a manipulação da sinalização e controle envolvidos na chamada (pelo Gatekeeper e Softswitch). Funções de controle de chamada e manipulação de mídias separadas em dois planos distintos proveem a máxima flexibilidade para a evolução da rede.

A centralização da inteligência dos serviços e controle da chamada permite uma gerência da rede simplificada e eficiente, e é a base para reações rápidas às demandas do mercado por novos serviços e oportunidades de negócios. Também possibilita a integração de serviços providos por aplicações de terceiros, que se interligam ao Softswitch via uma interface aberta (*open API*).

### Requerimentos de um Softswitch

Vejamos suas principais características:

- Separação do controle de chamadas e serviços do transporte de dados.
- Inteligência de serviço em aplicações de serviços de voz.
- Inteligência centralizada para rápida introdução de novos serviços convergentes.
- Interface aberta para dispositivos e aplicativos comerciais ou de outros fabricantes como *e-commerce*.
- Confiabilidade e segurança na tarifação e medição de desempenho e controle dos recursos.
- Inteligência para tratar e ter interface com os protocolos de sinalização, como SS7-Isup, H.323-SIP, dentre outros.



Figura 19 – Símbolo para o Softswitch

O tráfego convergente trouxe um considerável interesse para os administradores de rede e tem levado os provedores de serviços a implementar soluções que vão ao encontro com os requerimentos dos usuários. Tanto os tradicionais serviços legados de telefonia como os novos serviços providos pelas NGNs não serão competitivos apenas pela redução dos custos de transmissão. Um ponto-chave é a Qualidade dos Serviços (QoS), e características como *performance*, disponibilidade, flexibilidade e adaptabilidade tornam-se padrão de mercado.

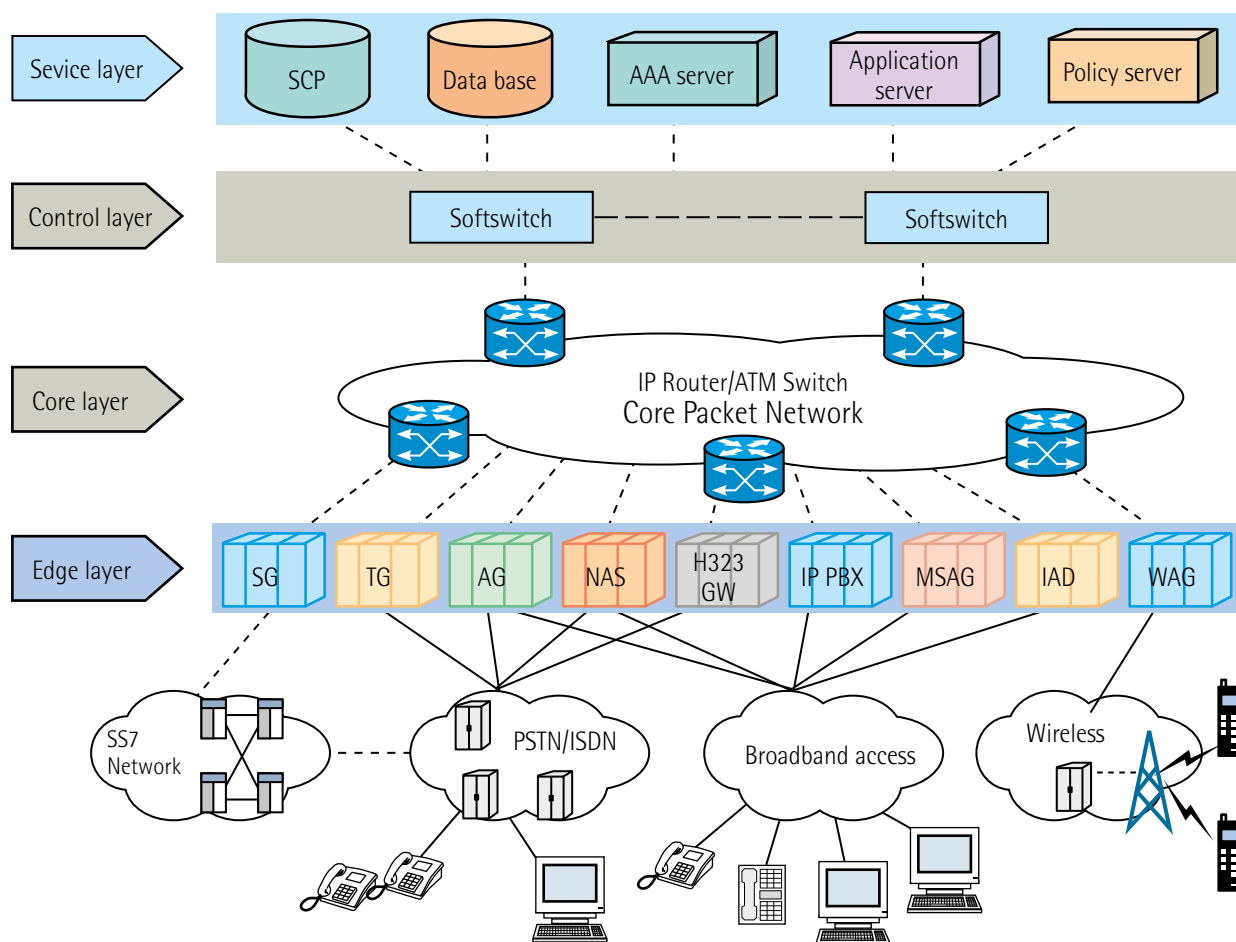


Figura 20 – Estrutura de camadas

### 3.5.3 Media Gateway Controller (MGC)

Executa funções de estabelecimento e finalização de sessões na rede IP. Ele mantém o estado de todas as chamadas e dos recursos alocados para elas. Possui interfaces para vários bancos de dados em redes IP e SS7 (por exemplo, políticas de diretórios) a fim de acessar usuários e serviços.

O MGC também possui a facilidade de prover endereços e um protocolo de tradução entre elementos de diferentes redes necessários para invocar uma chamada. Até o fim de uma chamada, o MGC coleta informações para bilhetagem. Existem dois protocolos básicos que são utilizados para controle: o Media Gateway Control Protocol (MGCP) e o Megaco, também conhecido como H.248.

A interface com as redes SS7 são feitas através dos protocolos SS7/IP. A política de acesso a diretórios no ambiente IP usa os protocolos LDAP (Lightweight Directory Access Protocol) e Cops (Common Open Policy Service).

No caso de um cliente IP, o MGC irá usar o SIP ou o H.323 para estabelecer a chamada e alocar os recursos e serviços necessários. O MGC também faz a tradução entre o H.323 e SIP para a interconexão de clientes com diferentes protocolos.

### 3.5.4 Signaling Gateway

Executa as funções de conversão entre as mensagens SS7 transmitidas através dos circuitos telefônicos e as mensagens SS7 por meio das redes IP. Os atuais protocolos de conectividade para IP-SS7 são o Sigtran, Tali e Q.2111. Em todos os casos, a regra do Signaling Gateway é estabelecer e encerrar uma ou mais conexões IP-SS7 e manter o estado de conexão entre as duas redes, mantendo a sequência de números, confirmações de conexões, retransmissões e notificações da existência de pacotes fora de sequência. O controle de congestionamento, a detecção de falhas nas sessões e segurança são outras funções importantes que ele pratica.

### 3.5.5 Access Gateway

Um Access Gateway, que combina informações do Signaling Gateway com o Trunking Gateway, é usado pelo ISDN ou CAS (Common Access Signaling) para inserir a sinalização em uma rede TDM. O Access Gateway extrai uma informação de controle dos protocolos de sinalização como o DMTF (Dual-Tone MultiFrequency) ou PRI (Primary Rate Interface) e a envia para o MGC para processamento. Os problemas encontrados entre domínios, quando uma conexão entre os pontos finais requer o roteamento em diferentes redes de provedores de telecomunicações, em geral não são cobertas pelos atuais padrões.

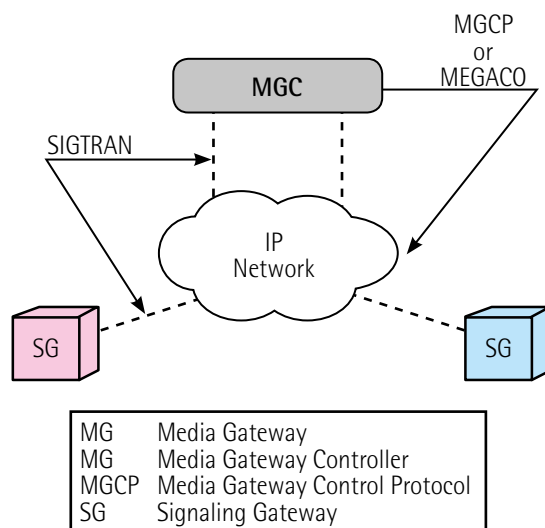


Figura 21 – Estrutura de rede

## 3.6 Desempenho do meio de transmissão

O meio de transmissão, ou enlace, refere-se aos dispositivos utilizados para transportar informações entre os elementos de uma rede. No projeto das novas redes de telecomunicações, são utilizados protocolos que incorporam esquemas de correção de erros que implementam solicitações ao transmissor para a retransmissão de elementos que se perderam por algum motivo. Então, torna-se importante medir o desempenho para determinar a eficiência dessas redes e estipular as soluções de caráter prático para resolver os possíveis problemas que ocasionam a perda desses dados. A seguir, acentuaremos os diferentes parâmetros de *performance* que podemos medir em uma rede.

### Vazão normalizada ou *goodput*

Mede a eficiência do meio e diz respeito à capacidade do enlace de transmissão em transportar pacotes não retransmitidos. Quando algum tempo é usado para a transmissão do cabeçalho introduzido pelos protocolos de rede em uso, as colisões dos pacotes e as retransmissões não são contadas para o valor *goodput* de desempenho.

Em um ambiente ideal, sem perdas de pacotes no meio devido a congestionamentos ou outros fatores, o valor do *goodput* equivale a 1,0. Contudo, a maioria dos protocolos e dos sistemas em uso nas redes atuais têm valores de *goodput* entre 1,0 e 0,95.

Para seu cálculo, são necessárias as seguintes informações:

- velocidade/largura de banda do enlace de telecomunicações (em *bps*);
- tamanho médio do pacote (em *bits*/pacote);
- valor de pico da vazão atual do enlace de transmissão (em pacotes/seg).

A partir desses valores, inicialmente será calculada a capacidade transportada pela rede, em pacotes/seg, através da seguinte relação:

Capacidade transportada = largura de banda/tamanho médio do pacote

Em seguida, pode-se calcular o valor de *goodput* através da seguinte relação:

*Goodput* = valor de pico/capacidade transportada

### Atraso médio

Representa o tempo médio que o pacote aguarda no transmissor antes de ser enviado, mais o tempo para transmitir o pacote. Os fatores que afetam esse valor incluem as características intrínsecas do dispositivo que está transmitindo e as características do meio de transmissão.

### Estabilidade

Refere-se à capacidade do método de acesso à rede de tratar aumentos de tráfego sem afetar a vazão. Quanto mais dispositivos se comunicam através do meio de comunicação, maiores são as chances de colisão nesse meio e, quando se atinge um determinado patamar, o sistema torna-se instável, ficando indisponível.

A técnica de acesso adotada deve incluir a capacidade de se adaptar a situações de sobrecarga na rede, tratando os casos de aumento de tráfego.

### Equidade

A equidade significa que todo dispositivo que quer transmitir (e tem permissão para isso) deve ter igual acesso ao meio dentro de um intervalo especificado.

### Gerenciamento de congestionamento

Quando a capacidade de tráfego de uma rede aproxima-se da capacidade máxima possível do meio de transmissão, ocorre um atraso na transmissão da informação, ocasionando o que conhecemos por "congestionamento" e, por conseguinte, a vazão de dados diminui.

Embora atraso e congestionamento sejam tópicos diferentes, existe uma relação entre eles que permite estimar a quantidade de atraso a partir do percentual da capacidade da rede que está sendo usada. A capacidade da rede atualmente em uso é chamada de **utilização**, em geral expressa em percentagem. O atraso efetivo de uma rede pode ser determinado pela seguinte relação, onde  $I$  é o atraso da rede quando o meio de transmissão está vazio,  $U$  representa a utilização e  $D$  é o atraso efetivo:  $D = I / (1 - U)$ . Por exemplo, para um atraso de rede ( $I$ ) igual a 10 ms e a utilização ( $U$ ) é 5%, o atraso efetivo ( $D$ ) será de:  $D = 0,1 / (1 - 0,05) \Rightarrow 0,1 / 0,95 = 10,53$  ms.

Quando não houver tráfego, o valor de  $U$  é zero, assim o atraso efetivo é equivalente ao atraso da rede. Com o aumento do tráfego, a utilização aumenta e o atraso efetivo fica maior.

Um uso aceitável da rede depende das necessidades e dos custos financeiros envolvidos. Entretanto, não é nada recomendado a operação de uma rede com nível de utilização igual ou superior a 90%. Em redes de comutação por pacotes, por exemplo, em que existe uma alta demanda de tráfego e atrasos podem ocasionar o acúmulo de pacotes nos *buffers* dos dispositivos de comutação, o congestionamento pode ser um problema sério. Para redes desse tipo, nas quais são necessários atrasos pequenos, a máxima utilização aceitável deve situar-se em torno de 50%.

A tecnologia convergente incluiu suporte total às características do sistema de sinalização número 7 (SS7) e interfaces padrões de telefonia, além de uma completa interoperabilidade com a infraestrutura da PSTN existente, suportando todas as características de voz as quais os usuários estão acostumados, assim como o tráfego de dados. Ela ainda pode prover uma ponte para o acesso e desenvolvimento de novos serviços.

Com a arquitetura convergente, foi possível alavancar os investimentos existentes em infraestrutura, como equipamentos tradicionais de comutação por circuito, enquanto suportava o crescimento do tráfego de dados. A arquitetura pode unificar diversas redes sobrepostas necessárias para a comunicação do momento.

A ideia geral da NGN é ter uma única rede capaz de transportar todos os tipos de informações, serviços e mídias. Esta rede é construída sob o protocolo IP com o princípio da estruturação e divisão dos planos funcionais em: acesso, transporte e *switching*, controle e inteligência e serviço. As camadas são independentes e podem ser modificadas, substituídas ou atualizadas sem afetar os outros níveis funcionais.

Antes da NGN, o modelo de serviços era em estruturas verticais com tecnologias dedicadas a cada tipo de acesso incorrendo na duplicação de funcionalidades entre os vários sistemas isolados, mas agora a NGN propõe a simplificação deste modelo de serviço estruturando horizontalmente as camadas e unificando as funcionalidades para oferecer os serviços e conteúdos a todos os meios de acesso.

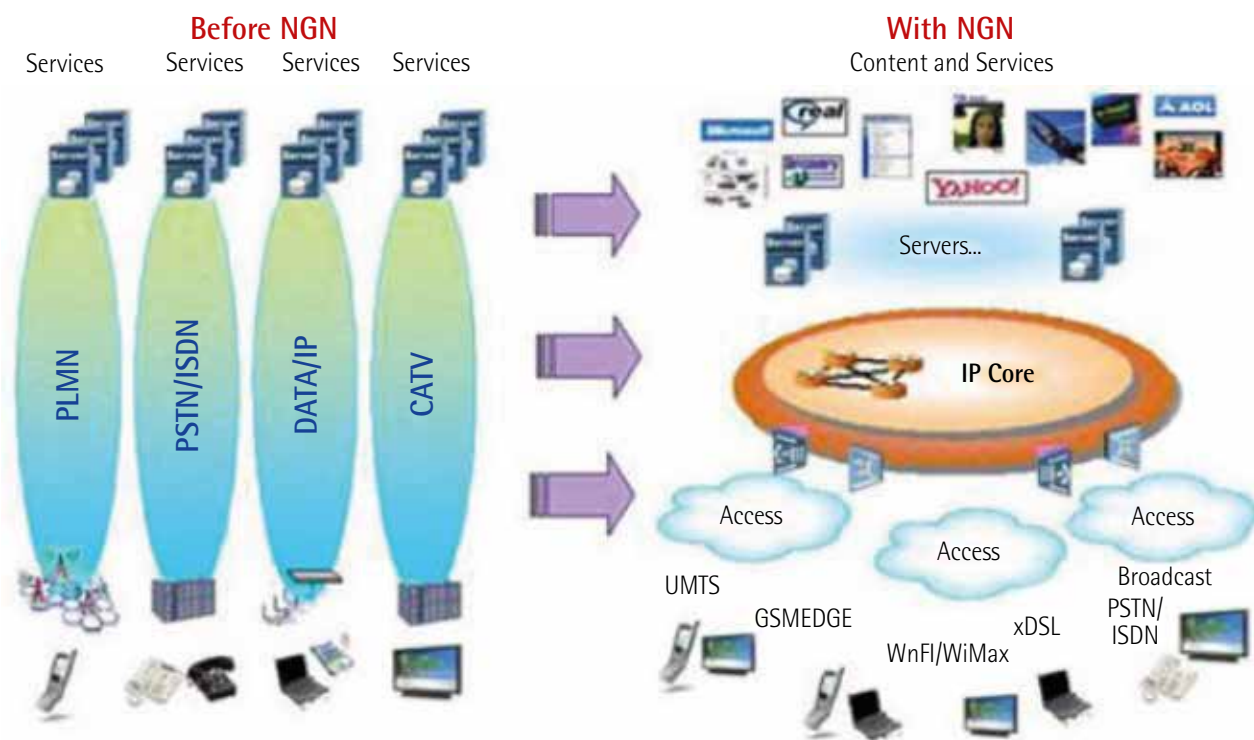


Figura 22 – Comparativo de arquiteturas antes e depois da NGN

### 4 REDES IP E CRIAÇÃO DO MPLS

Em uma rede IP, os pacotes de dados são encaminhados um a um e de forma independente. Não é estabelecida uma conexão ou circuito virtual que defina um caminho predeterminado para eles.

Nesse contexto, o envio dos pacotes de dados é feito por roteadores. Roteadores são dispositivos da camada 3, que, ao receber um pacote IP, analisa o endereço destino carregado pelo pacote IP, consulta uma tabela de roteamento mantida pelo roteador e toma uma decisão de para onde direcioná-lo. A tabela de roteamento é mantida pelo roteador usando informação trocada entre roteadores e procedimentos definidos pelo protocolo de roteamento utilizado.

Um roteador pode ser configurado com múltiplos protocolos de roteamento. Como exemplo, citamos: Open Shortest Path First (OSPF), Routing Information Protocol (RIP) e Border Gateway Protocol (BGP). Como a decisão é tomada pacote a pacote, dois pacotes enviados pelo computador X podem seguir caminhos diferentes até o computador Y, passando, por exemplo, pelo roteador 1 e indo direto para o roteador 3, ou passando pelos roteadores 1, 2 e 3.

A figura a seguir ilustra uma rede IP tradicional, na qual existem três redes (A, B e C) e três roteadores (1, 2 e 3).

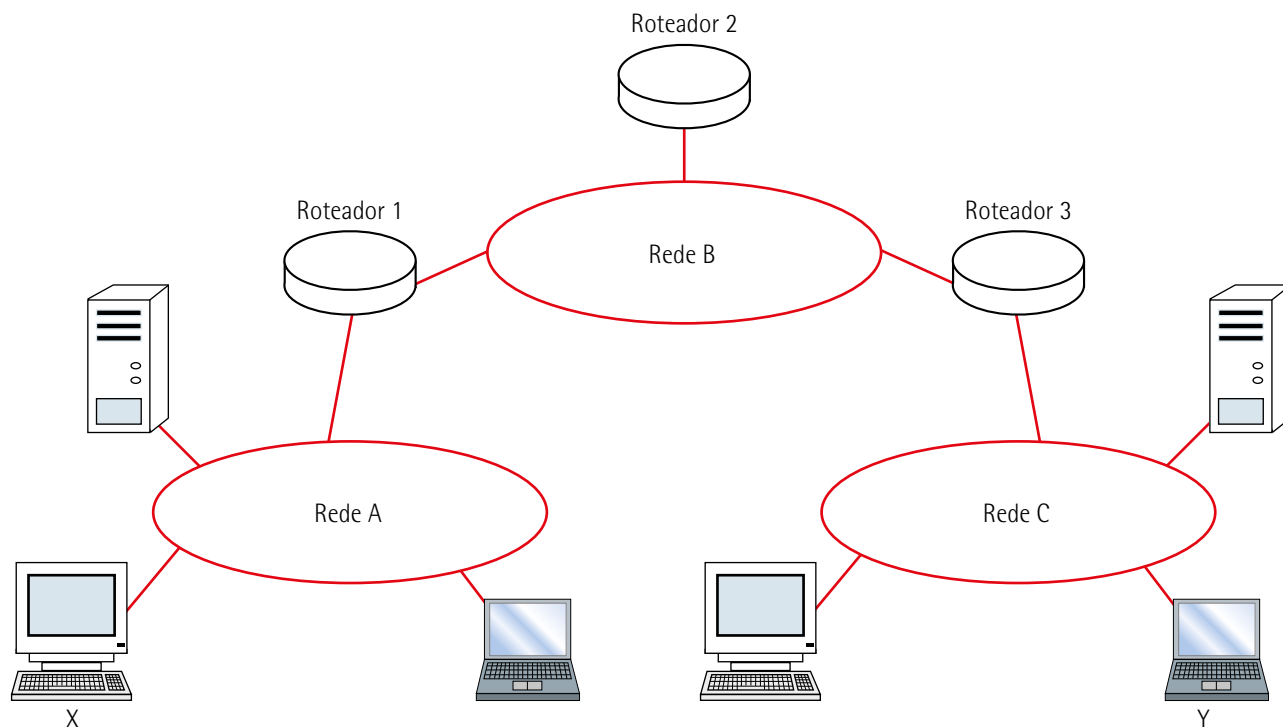


Figura 23 – Rede IP tradicional

A tabela de roteamento pode ser vista também como uma forma de dividir o conjunto de pacotes possíveis que um roteador pode passar adiante em um número finito de subconjuntos disjuntos. Pacotes de cada subconjunto são passados adiante pelo roteador da mesma forma. Esses subconjuntos são chamados de classes de equivalência para roteamento (FECs – Forwarding Equivalence Classes).

O Multiprotocol Label Switching (MPLS) foi padronizado para resolver uma série de problemas das redes IP, entre eles:

- possibilitar a utilização de *switches*;
- escalabilidade;
- adicionar novas funcionalidades ao roteamento.

Multiprotocol Label Switching (MPLS) é uma tecnologia utilizada em larga escala pelas provedoras de serviço de internet. Seu funcionamento baseia-se na inserção de um rótulo, em vez de um endereço de destino para mover os pacotes dentro da sua rede. Essa técnica diminuiu muito o tempo de encaminhamento de pacotes, visto que o rótulo é usado como índice numa tabela interna, que direciona a interface de saída correta.



Conforme a definição de Tanenbaum e Wetherall (2011, p. 295):

O cabeçalho MPLS genérico tem 4 bytes de extensão e quatro campos. O mais importante é o campo Rótulo, que mantém o índice. O campo QoS indica a classe do serviço. O campo S relaciona-se ao empilhamento de vários rótulos. O campo TTL indica quantas vezes o pacote pode ser encaminhado.

O MPLS, Multiprotocol Label Switching, tem por objetivo otimizar os níveis de desempenho de uma rede IP organizando recursos em uma rede de maneira mais eficiente, a fim de ampliar a probabilidade de entrega da informação e minimizar custos desta entrega.

Não é um protocolo muito simples de se entender. Nem tudo que é complexo é eficiente, mas neste caso a eficiência com que o MPLS deve prover as redes IP faz jus a sua complexidade.

Através de uma técnica denominada *label switching*, que pode ser traduzida como rótulo de encaminhamento, o MPLS visa estabelecer políticas que definem caminhos ou rotas para a entrega da informação e os níveis de prioridade de serviço que determinados tipos de tráfego devem ter.

O MPLS fornece meios para mapear endereços IP em rótulos simples e de comprimento fixo utilizados por diferentes tecnologias de encaminhamento e chaveamento de pacotes. Este mapeamento é feito apenas uma vez no nó na borda da rede MPLS. A partir daí, o envio dos pacotes é feito utilizando-se a informação contida em um rótulo (*label*) inserido no cabeçalho do pacote. Este rótulo não traz um endereço e é trocado em cada *switch*.

O chaveamento de dados a altas velocidades é possível porque os rótulos de comprimento fixo são inseridos no início do pacote e podem ser usados pelo *hardware*, resultando em um chaveamento rápido.

Apesar de ter sido desenvolvido visando redes com camada de rede IP e de enlace ATM, o mecanismo de direcionamento dos pacotes no MPLS pode ser utilizado para quaisquer outras combinações de protocolos de rede e de enlace, o que explica o nome de Multiprotocol Label Switching dado pelo grupo de trabalho do IETF.



### Saiba mais

Você pode aprofundar seus conhecimentos sobre MPLS em:

ROCHA, A. S. Estudo básico do MPLS (Multi Protocol Label Switching) – I. *Teleco*, 24 jan. 2011. Disponível em: <<http://www.teleco.com.br/pdfs/tutorialmplseb1.pdf>>. Acesso em: 2 ago. 2018.

Na dissertação a seguir, é possível encontrar detalhes mais técnicos e comparações do MPLS com outros protocolos.

KAKIHARA, C. M. *Avaliação e comparação de desempenho entre a arquitetura IP e a arquitetura IP sobre MPLS*. Dissertação (Mestrado em Física Aplicada). Instituto de Física de São Carlos, São Carlos (SP), 2006. Disponível em: <<http://www.teses.usp.br/teses/disponiveis/76/76132/tde-22112006-102117/pt-br.php>>. Acesso em: 2 ago. 2018.

### 4.1 Compromisso do MPLS

Uma opção de tratar o QoS é usar o Multiprotocol Label Switching (MPLS). Incluir rótulo (*label*) ao pacote IP permite interoperabilidade contínua através dos elementos de rede: pacotes são enviados conforme o rótulo em vez do cabeçalho do pacote. Com o rótulo, podem-se incluir prioridades de dados e garantia de QoS para serviços. Inicialmente, MPLS foi utilizado para engenharia de tráfego e aplicações como VPN sobre redes IP e ATM.

Com MPLS, que é um protocolo agnóstico, operadoras podem empacotar suas redes de acesso e propiciar integração contínua com rede IP. Operadoras podem fornecer serviços Ethernet sobre ATM ou sobre Rede Óptica Síncrona (Sonet)/Hierarquia Digital Síncrona (SDH). Elas podem estabelecer túneis ponto a ponto ou ponto-multiponto para serviços diferenciados, estendendo a oferta de sua carteira de serviços com expansão de equipamentos marginais.

Implementações são proprietárias e a maioria não opera com outras implementações. Com a padronização, espera-se que o MPLS torne-se um grande suporte para tornar o tráfego IP aceitável com relação a SLAs. Isto é importante quando operadoras devem garantir serviços IP. Desse modo, MPLS fim a fim está se tornando um critério maior de escolha.

Roteadores de borda ou dispositivos de borda que incorporam MPLS podem determinar o destino dos pacotes e algum tratamento especial requerido. Assim, roteadores de borda podem agir, seja como um *media gateway*, seja como um *switch router* em *backbone* de pacote.

Com excesso de capacidade no núcleo da rede, a borda torna-se um gargalo para entrega de serviços de alta largura de banda. Roteadores que propiciam serviços de borda, *gateways* e centrais de comutação devem todos entregar mais largura de banda aos assinantes enquanto modernizam a operação de rede para as operadoras. As operadoras vislumbram trabalhar com serviço IP com QoS sobre suas redes, embora o tráfego IP necessite de *features* a ser efetivamente gerenciada. Na borda da rede, roteadores de borda integram funções como VPN sobre IP, agregação de faixa larga, aluguel de linha e entrega de serviços IP avançados. Mas roteadores de borda são desafiados a prover serviços IP a uma determinada taxa de velocidade e suportando uma confiabilidade de 99,999% do tempo.

O MPLS fornece meios para mapear endereços IP em rótulos simples e de comprimento fixo usados por diferentes tecnologias de envio e chaveamento de pacotes. Esse mapeamento é feito apenas uma vez no nó na borda da rede MPLS. A partir daí, o encaminhamento dos pacotes é executado utilizando-se a informação contida em um rótulo (*label*) inserido no cabeçalho do pacote. Esse rótulo não traz um endereço e é trocado em cada *switch*. O chaveamento de dados a altas velocidades é possível porque

os rótulos de comprimento fixo são inseridos no início do pacote e podem ser usados pelo *hardware*, resultando em um chaveamento rápido.

O propósito do MPLS não é a substituição do roteamento IP, mas a melhoria dos serviços providos em redes IP através de um roteamento predefinido, oferecendo escopo para gerenciamento de tráfego e garantia de QoS mínimo.

Para implementar QoS, o MPLS ainda incorpora conceitos e ferramentas como os serviços integrados e os serviços diferenciados. Por exemplo, o MPLS provê reserva de banda a ser também especificada no rótulo, e pacotes podem ser "marcados" para indicar sua prioridade. Todas essas ferramentas fazem do MPLS um mecanismo muito adequado para execução de capacidades de gerenciamento de tráfego em redes IP.

### 4.2 Conceitos da arquitetura do MPLS

A figura a seguir mostra uma arquitetura da rede MPLS. Existem roteadores LER que conectam um domínio MPLS com um nó fora deste domínio. Já os roteadores subsequentes LSR são um nó dentro dos domínios do MPLS.

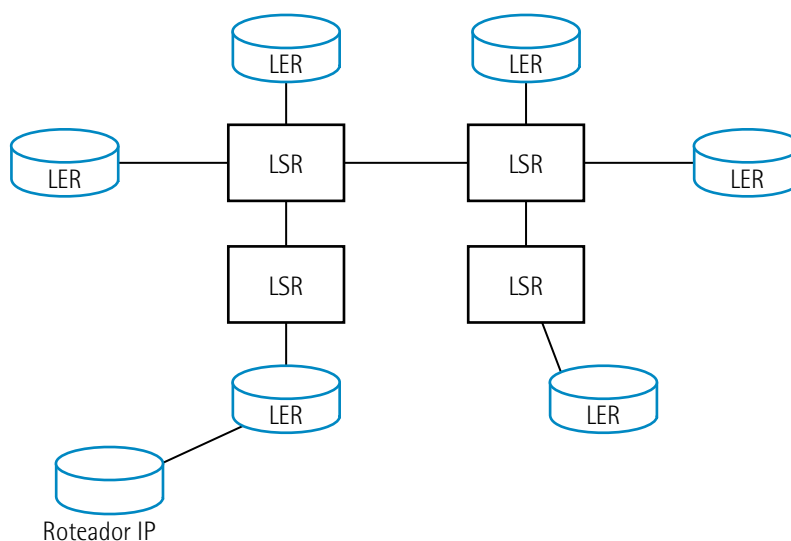


Figura 24 – Estrutura do MPLS

- *Label* (rótulo): identificador de comprimento curto e definido que é usado para identificar uma FEC, tendo geralmente significado local. Quando utilizado sobre protocolos onde o cabeçalho da camada de enlace não pode ser empregado, o rótulo *shim* é inserido entre os cabeçalhos das camadas de enlace e de rede.
- Forward Equivalence Class (FEC): representação de um grupo de pacotes que tem os mesmos requisitos para o seu transporte. Para todos os pacotes neste grupo, é fornecido igual tratamento na rota até o seu destino. FECs são baseados em requisitos de serviço para um dado conjunto de pacotes ou simplesmente por um prefixo de endereçamento.

Assim, é preciso considerar que dois pacotes estão na mesma FEC pela análise do endereço destino do pacote. Quando o pacote anda na rede, em cada roteador ele é reexaminado e atribuído a uma FEC. No MPLS, a atribuição de um pacote particular a uma FEC em particular é feita apenas uma vez, no LER, quando o pacote entra na rede. A FEC atribuída ao pacote é codificada como um valor de comprimento fixo e curto conhecido como *label*.

Quando o pacote é direcionado ao próximo roteador, o rótulo é enviado juntamente com ele, ou seja, o pacote é rotulado antes de ser encaminhado. Nos roteadores subsequentes (LSR), não existe análise do cabeçalho da camada de rede do pacote. O rótulo é usado como um índice em uma tabela que especifica o próximo roteador e um novo rótulo. O rótulo antigo é trocado pelo novo e o pacote é remetido para o próximo roteador. No MPLS, uma vez que um pacote é associado a uma FEC, não é necessário mais nenhum exame do cabeçalho por parte dos outros roteadores, todo o processo é feito a partir do rótulo.

- Label Edge Router (LER): um nó MPLS que conecta um domínio MPLS com um nó fora deste domínio.
- Label Switching Router (LSR): é um nó do MPLS. Ele recebe o pacote de dados, extrai o rótulo do pacote e o utiliza para descobrir na tabela de encaminhamento qual a porta de saída e o novo rótulo. Para executar este procedimento, o LSR tem apenas um algoritmo usado para todos os tipos de serviço. A tabela de envio pode ser única ou existirem várias, uma para cada interface. Elas são compostas utilizando rótulos distribuídos, como Label Distribution Protocols (LDP), RSVP ou protocolos de roteamento como o BGP e o OSPF.
- Label Distribution Protocol (LDP): um conjunto de procedimentos pelo qual um LSR informa outro das associações entre *label*/FEC que ele fez. Dois LSRs que utilizam um LDP para trocar informações de associações *label*/FEC são conhecidos como Label Distribution Peers por conta da informação de associação que trocaram.
- Label Switching Path (LSP): no MPLS, a transmissão de dados ocorre em caminhos chaveados a rótulo (LSPs). Eles são uma sequência de rótulos em todos os nós ao longo do caminho da origem ao destino. São estabelecidos ante a transmissão dos dados ou com a detecção de um fluxo de dados.

O MPLS proporciona também escalabilidade à rede, uma vez que um roteador convencional passa a ter como roteador adjacente o seu LER do *backbone* MPLS, e não todos os roteadores conectados ao *backbone*, a exemplo do que acontece com *backbones* ATM. A utilização de rótulos para envio de pacotes permite ainda adicionar novas funcionalidades ao roteamento independentemente do endereço IP na camada de rede. É possível fixar rotas predefinidas ou prioridades para pacotes quando da definição das FECs.

O MPLS passa a ser, portanto uma ferramenta poderosa para implementação de QoS e classes de serviço em redes IP. Com o MPLS é possível também estruturar túneis utilizados na formação de redes privadas virtuais (VPNs). Considerando tal solução adotada pela maior parte dos provedores de VPN que possuem *backbone* IP.

O protocolo MPLS é considerado como multiprotocolo pois seu cabeçalho não faz parte do pacote da camada de rede e também do quadro da camada de enlace de dados. Desse modo, ele pode direcionar tanto pacotes IP como pacotes que não sejam IP. Os rótulos são adicionados aos pacotes quando estes alcançam um roteador de borda de rótulo, LER. É através dele que o pacote será encaminhado dentro da rede MPLS. A figura a seguir ilustra o processo de encaminhamento de um pacote IP por uma rede MPLS.

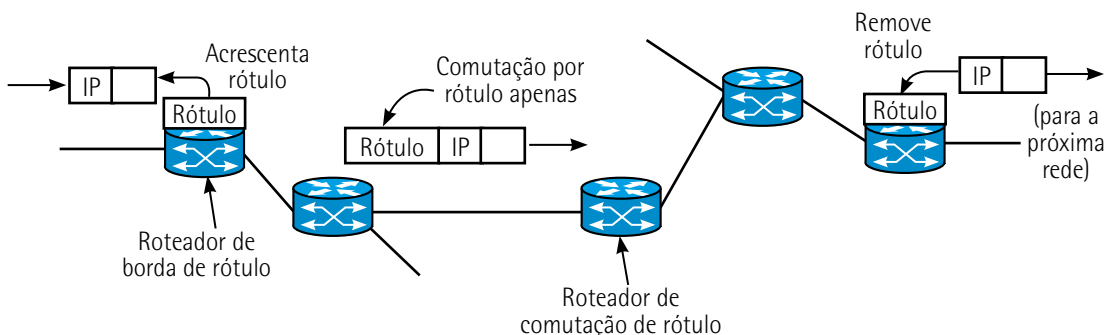


Figura 25 – Encaminhamento de um pacote IP por uma rede MPLS



### Observação

A ideia do MPLS é a de que, quando um pacote de dados for enviado a um destino específico ou um grupo de destinos, uma rota única possa ser definida. Este caminho claro poderia ser usado pelos pacotes que se encaminham para aquele destino ou grupo de destinos, enquanto os roteadores e outros dispositivos de camada 3 do modelo OSI não necessitam perder tempo e processamento para efetuar a verificação do cabeçalho IP desses pacotes de dados.

Vejamos um exemplo do funcionamento básico de uma rede utilizando MPLS.

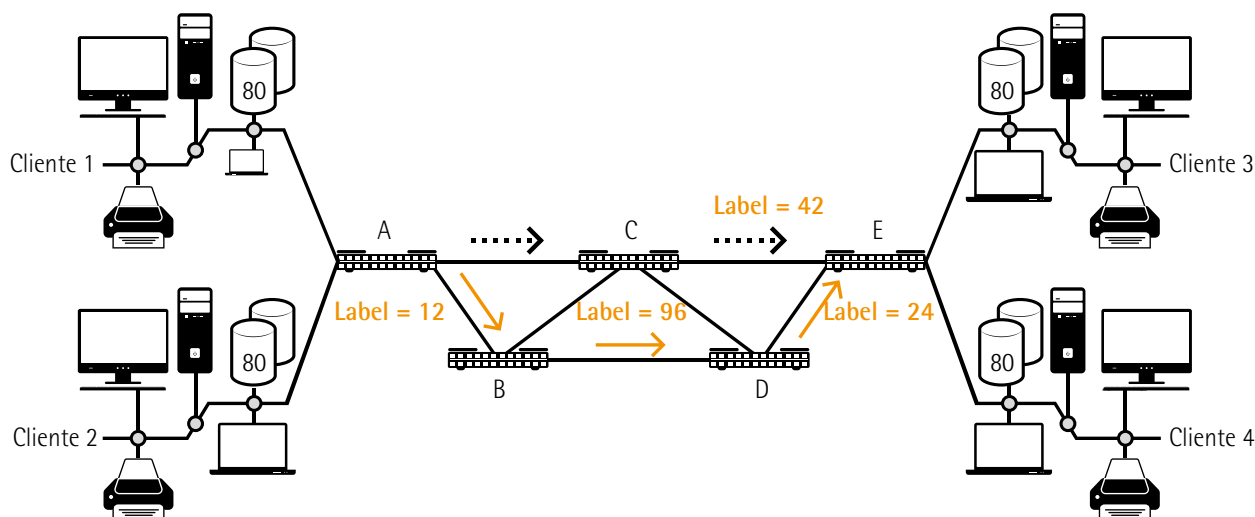


Figura 26 – Funcionamento básico de uma rede utilizando MPLS

No exemplo da última figura, são estabelecidas duas rotas, uma que conecta o cliente 1 e o cliente 3 e outra que interliga os clientes 2 ao 4. No caso da primeira rota, são utilizados os rótulos 23 e 42 sobre o caminho  $A \rightarrow C \rightarrow E$ , levando a informação do cliente 1 para o cliente 3. Na segunda rota, que liga o cliente 2 ao 4, são usados os rótulos 12, 96 e 24 através do caminho  $A \rightarrow B \rightarrow D \rightarrow E$ . Suponha que o cliente 1 deseja enviar pacotes ao cliente 3. Assim, o nó A fixa o rótulo 23 nos pacotes do cliente 1.

Quando o nó C recebe os pacotes "rotulados" do nó A, ele consulta uma tabela de roteamento procurando por uma rota de saída para o rótulo recebido, que no caso é a 42. O nó C substitui o rótulo 23 pelo 42 e envia os pacotes ao nó E. Este nó entende que ele é o fim do caminho que foi previamente definido ( $A \rightarrow C \rightarrow E$ ), remove o rótulo, enviando o pacote ao cliente 3.

Para esse processo de roteamento do MPLS, o caminho que um pacote deve percorrer, é vital estabelecer tudo antes, para que esse processo possa ser usado através dos rótulos de encaminhamento. Essa prévia definição de um caminho é bastante parecida à fixação de circuitos virtuais utilizados no Frame Relay.



### Lembrete

Uma rede MPLS inclui um rótulo ou *label* ao pacote IP, de forma a permitir que este pacote trafegue com maior segurança, melhore a qualidade de serviço em relação à rede IP.

## 4.3 Benefícios da rede MPLS

Uma rede MPLS traz uma série de benefícios em relação a uma rede IP. Como os pacotes recebem um rótulo (*label*), este somente será aberto no destino. Dessa forma, as redes MPLS possuem uma segurança superior a uma rede IP comum. A segurança é equivalente a uma conexão Frame Relay.

Adicionalmente, a rede MPLS permite tratar tipos de tráfego de maneira diferente, porque cada aplicação possui sua necessidade específica. Existe uma maior facilidade no gerenciamento de rede.

Também são implementadas classes de serviço e é possível reduzir o tempo de atraso, isto é, o *delay*.



### Resumo

Nesta unidade, estudamos que a arquitetura NGN é dividida em quatro camadas funcionais: de acesso, de núcleo ou central, de controle e de serviços.

Em redes NGN, existe a separação entre serviços e o transporte é representado por dois blocos distintos, conhecida como estrato de

funcionalidade. As funções de transporte residem no estrato de transporte e as funções relacionadas a aplicações, no estrato serviço.

Um dos elementos que faz parte da rede NGN é o Media Gateway, que faz a interconexão entre a rede comutada e a rede de pacotes, possibilitando a conversão da mídia de voz da rede telefônica para a rede de dados e vice-versa.

Vimos que Softswitch é o elemento central da rede NGN, que contém sua inteligência e controla todos os demais elementos da rede, sendo considerado o cérebro da rede NGN. Ele possui autonomia de controlar vários *medias gateways* de uma rede TCP/IP. Por sua vez, Media Gateway Controller (MGC) executa funções de estabelecimento e finalização de sessões na rede IP. Já o Signaling Gateway realiza as funções de conversão entre as mensagens SS7 transmitidas através dos circuitos telefônicos e as mensagens SS7 através das redes IP.

Há algumas grandezas que podem ser mensuradas nos meios de transmissão com vazão normalizada ou *goodput*, atraso médio e pelo gerenciamento do congestionamento.

Acentuamos que o Multi-protocol Label Switching (MPLS) foi padronizado para resolver problemas oriundos das redes IP, como: possibilitar a utilização de *switches*, escalabilidade e adicionar novas funcionalidades ao roteamento. O objetivo da MPLS é a otimização de níveis de desempenho de uma rede IP, organizando recursos em uma rede de maneira mais eficiente para maximizar a probabilidade de entrega da informação e minimizar os custos dessa entrega.

O MPLS fornece meios para mapear endereços IP em rótulos simples e de comprimento fixo utilizados por diferentes tecnologias de encaminhamento e chaveamento de pacotes. Ele passa a ser, portanto, uma ferramenta poderosa para implementação de QoS e classes de serviço em redes IP.



### Exercícios

**Questão 1.** (FCC 2009) No contexto do gerenciamento de redes de computadores, a disponibilidade:

- A) Deve ser monitorada pelos usuários, somente.
- B) Não deve ser monitorada pelos administradores da rede, por questões de controle interno.

C) É uma estatística de falha.

D) Geralmente almejada pelos administradores da rede é de, no máximo, 70%.

E) É um *toolkit* de controle.

Resposta correta: alternativa C.

### Análise das alternativas

Justificativa geral: a disponibilidade é um conceito intimamente relacionado às falhas. Um sistema de alta disponibilidade é um sistema resistente a falhas, de vários tipos, como *hardware*, *software*, energia. Sendo assim, ela pode ser utilizada como uma estatística de falha.

**Questão 2.** (FCC 2014) O esquema a seguir ilustra uma estrutura de comunicação VoIP entre um computador e um telefone comum.

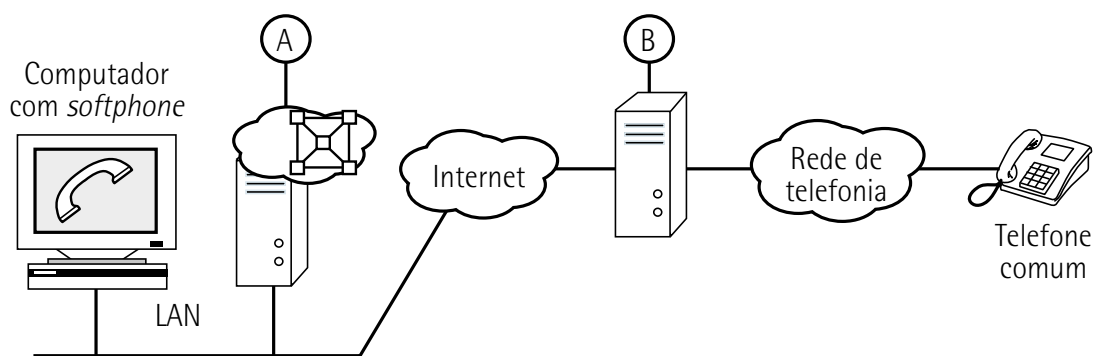


Figura 27

No cenário apresentado, um computador equipado com um programa que possibilita as ligações em VoIP está conectado numa rede local (LAN) com o equipamento A. Primeiro, o computador descobre o equipamento A na rede, que envia ao computador seu endereço IP. O computador se registra com o equipamento A, que, por sua vez, manda de volta uma mensagem de gerenciamento. Após aceitar a mensagem, o computador pede para o equipamento A largura de banda para iniciar a configuração da chamada, com o estabelecimento de uma conexão. Após a largura de banda ser liberada ao computador, ele envia outra mensagem com o número do telefone a ser chamado para o equipamento A, que confirma a solicitação da chamada e encaminha a informação para o equipamento B. Este, que é metade computador e metade comutador de telefonia, faz a chamada telefônica para o telefone comum. O telefone toca e o computador recebe o sinal indicando que ele está tocando. Quando o telefone é atendido, é enviada uma mensagem ao computador indicando que houve a conexão.

A e B são, respectivamente,



- A) Gatekeeper e Gateway.
- B) Multipoint Controller Unit e User Agent Server.
- C) Gateway e Proxy Server.
- D) Proxy Server e Softphone.
- E) Softswitch e Softphone.

Resolução desta questão na plataforma.

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.