



COMUNICADO

ESPELHO DE CORREÇÃO DA PROVA ESCRITA

EDITAL PROGEP N° 121/2026

A Comissão Julgadora torna público o espelho de correção da Prova Escrita do Concurso Público para contratação de professor efetivo da Unidade Acadêmica - FEELT, área: Engenharia Elétrica/, subárea: Telecomunicações.

TEMA SORTEADO: Camada de rede e roteamento.

O que deveria ser abordado na dissertação do(a) candidato(a) para a obtenção da nota máxima:

A Camada de Rede (*Network Layer*) tem como principal finalidade permitir a **comunicação entre dispositivos que podem estar em redes diferentes, realizando a entrega de pacotes desde a origem até o destino**. As principais funções são: endereçamento lógico, encaminhamento (*forwarding*), roteamento (*routing*), interconexão de redes, fragmentação e remontagem e entrega de pacotes entre origem e destino.

1 - Protocolo IP: Endereçamento IPv4 e IPv6, fragmentação e sub-redes.

O Protocolo IP (*Internet Protocol*) é responsável pelo **endereçamento lógico dos dispositivos** e pelo **encaminhamento de pacotes entre diferentes redes**. Atualmente, coexistem duas versões principais do protocolo: o IPv4 e o IPv6. A principal **diferença** entre eles está no **espaço de endereçamento**, mas o IPv6 também introduz modificações importantes na estrutura do cabeçalho, na configuração de endereços e no tratamento da fragmentação.

1.1 - Endereçamento

O datagrama **IPv4** tem um total de **20 bytes de cabeçalho** onde os campos de endereço de origem e de destino utiliza **32 bits (equivalente a 4 bytes)**. Esse endereço é representado em **quatro números decimais separados por pontos**, denominados notação decimal pontuada. **Cada octeto pode assumir valores de 0 a 255**. Dessa forma, o **espaço teórico** de endereçamento IPv4 possui 2^{32} , aproximadamente 4,3 bilhões de endereços.

Uma motivação importante para o desenvolvimento do sucessor do protocolo IPv4 é o entendimento de que o espaço de endereços IP de 32 bits estava escassear, com novas sub-redes e nós IP sendo anexados à

Internet. A utilização de NAT (*Network Address Translation*) prolongou a vida útil do IPv4, permitindo que vários dispositivos compartilhassem endereços públicos, mas não resolveu a limitação fundamental do espaço de endereçamento.

O datagrama IPv6 tem um total de 40 bytes de cabeçalho onde os campos de endereço de origem e de destino utiliza 128 bits proporcionando um espaço de endereçamento de 2^{128} possibilidades. Os endereços são representados em hexadecimal, divididos em oito grupos de 16 bits, separados por dois pontos, por exemplo: 2001:0db8:0000:0000:ff00:0042:8329. A representação pode ser simplificada pela remoção de zeros à esquerda e pela substituição de uma sequência contínua de grupos iguais a zero por ::, desde que essa substituição seja realizada apenas uma vez no endereço. Assim, o endereço anterior pode ser representado como: 2001:db8::ff00:42:8329.

Na prática, um computador que possua somente IPv4 não consegue enviar diretamente um datagrama IPv4 para um computador que possua somente IPv6, pois IPv4 e IPv6 são protocolos distintos e não são diretamente interoperáveis. Por outro lado, sistemas habilitados para IPv6 que também implementam IPv4, como ocorre em uma arquitetura Dual Stack, podem enviar, encaminhar e receber datagramas tanto IPv4 quanto IPv6. Os mecanismos de tradução permitem, por exemplo, que um dispositivo ou uma rede IPv6 se comunique com serviços que ainda utilizam exclusivamente IPv4. Já os mecanismos de tunelamento permitem transportar tráfego IPv6 sobre uma infraestrutura IPv4 durante o processo de migração.

1.2 - Fragmentação

A fragmentação IP ocorre quando um pacote possui tamanho superior ao MTU (*Maximum Transmission Unit*) da rede pela qual deverá ser transmitido. O MTU representa o tamanho máximo, em bytes, do pacote que pode ser transportado por determinado enlace sem que seja necessária fragmentação. **A fragmentação aumenta o processamento e a sobrecarga da rede.** Além disso, a perda de um dos fragmentos pode comprometer a reconstrução do datagrama original, exigindo seu descarte.

No IPv4, um **roteador pode fragmentar um datagrama quando seu tamanho excede o MTU do próximo enlace, desde que a fragmentação não tenha sido proibida pelo remetente.** Para permitir que os fragmentos sejam posteriormente reconstruídos, o **IPv4 utiliza campos específicos no cabeçalho, como Identification, Flags e Fragment Offset.** O campo Identification permite associar os fragmentos ao mesmo datagrama original, enquanto o Fragment Offset indica a posição de cada fragmento no pacote original. A tarefa de **reconstrução de datagramas** é alocada aos **sistemas finais**, e não aos roteadores da rede.

Para exemplificar, um datagrama constituído de 20 bytes de cabeçalho e 3.980 bytes de carga útil IP chega a um roteador e deve ser repassado a um enlace com MTU de 1.500 bytes. Os 3.980 bytes de dados do datagrama original devem ser alocados a três fragmentos separados (1.480 + 1.480 + 1020). No destino, a carga útil do datagrama é passada para a camada de transporte apenas após a camada IP ter reconstruído o datagrama IP original.

No IPv6, **os roteadores não fragmentam pacotes em trânsito.** O nó de origem deve descobrir o MTU adequado ao caminho, por meio de mecanismos como o Path MTU Discovery, e ajustar o tamanho dos pacotes enviados. Caso seja **necessária fragmentação**, ela é **realizada pela origem por meio do Fragment Extension Header.** Essa alteração reduz o processamento de fragmentação nos roteadores e contribui para uma estrutura de encaminhamento mais simples.

Para exemplificar, suponha um datagrama constituído de 40 bytes de cabeçalho e 1.960 bytes de carga útil IP se ele chega em algum ponto do caminho cuja MTU seja **1280 bytes**, roteador descarta o pacote e envia uma mensagem ICMPv6 Packet Too Big para a origem. A origem então deve ajustar o tamanho dos pacotes enviados utilizando o Fragment Extension Header (Cabeçalho de Extensão de Fragmentação) do IPv6.

1.3 – Sub-rede

A subnetting, ou subdivisão em sub-redes, consiste em dividir uma rede IP em redes menores. **Essa técnica permite utilizar de maneira mais eficiente o espaço de endereçamento, organizar a infraestrutura, reduzir domínios de broadcast no IPv4 e facilitar o gerenciamento e o roteamento da rede.**

A estratégia de atribuição de endereços da internet é conhecida como CIDR (*Classless Inter-Domain Routing*) que generaliza o endereço IP **dividido** conceitualmente em uma **parte de rede** e uma **parte de host (dispositivos / sistemas finais)**. Por exemplo, no endereço 223.1.1.0/24 tem-se os primeiros **24 bits correspondendo ao prefixo da rede e os 8 bits identificando hosts dentro dessa rede**. A utilização do CIDR substituiu a antiga classificação rígida de endereços em classes A, B e C com endereços de sub-rede de 8, 16 e 24, respectivamente, **permitindo maior flexibilidade na alocação de endereços e na criação de sub-redes**. A máscara /24, por exemplo, corresponde a 255.255.255.0. Em uma sub-rede IPv4 convencional /24, existem 256 combinações de endereços, sendo normalmente 254 utilizáveis para hosts, pois o primeiro endereço identifica a rede e o último é utilizado como endereço de broadcast.

Na prática, imagine que uma organização possua três setores: o Setor A, com 100 computadores; o Setor B, com 50 computadores; e o Setor C, com 20 computadores. Não seria eficiente atribuir uma rede /24 para cada setor, pois haveria um desperdício significativo de endereços IP. Nesse caso, podem ser utilizadas sub-redes de tamanhos diferentes, de acordo com a necessidade de cada setor, aproveitando a flexibilidade proporcionada pelo CIDR e pelo VLSM (*Variable Length Subnet Mask*). Para o Setor A, que necessita de 100 endereços para hosts, pode-se utilizar uma rede /25, que possui 128 endereços no total, sendo 126 utilizáveis para hosts. Para o Setor B, que necessita de 50 endereços, pode-se utilizar uma rede /26, com 64 endereços no total e 62 utilizáveis. Para o Setor C, que necessita de 20 endereços, pode-se utilizar uma rede /27, com 32 endereços no total e 30 utilizáveis.

Em redes IPv6, é comum a utilização de /64 para cada sub-rede. Na prática, imagine que uma organização que receba o bloco 2001:db8:1234::/48 dispõe de 16 bits (64 - 48) adicionais para identificar sub-redes, podendo criar até 2^{16} sub-redes/64. Assim, diferentes departamentos ou segmentos da organização podem receber prefixos como 2001:db8:1234:0001::/64, 2001:db8:1234:0002::/64 e 2001:db8:1234:0003::/64.

2 - Algoritmos de Roteamento: Fundamentos dos algoritmos de Vetor de Distância (*Distance Vector*) e Estado de Enlace (*Link State*).

A camada de rede executa o serviço de comunicação hospedeiro a hospedeiro. Uma distinção importante entre as funções de repasse e roteamento da camada de rede. **Repasse** envolve a transferência de um pacote de um enlace de entrada para um enlace de saída dentro de um único roteador. **Roteamento** deve

determinar a rota ou o caminho tomado pelos pacotes ao fluírem de um remetente a um destinatário. O processo de roteamento envolve a obtenção de informações sobre a **topologia da rede**, a **avaliação dos possíveis caminhos** e a **seleção da melhor rota de acordo com determinada métrica de roteamento**. A meta natural de um algoritmo de roteamento é identificar o **caminho de menor custo** entre origens e destinos. Quando **todas as arestas possuem o mesmo custo**, o **caminho de menor custo corresponde ao caminho com o menor número de enlaces**.

A teoria de algoritmos de roteamento é concentrada em duas classes mais predominantes: algoritmos de estado de enlace e de vetor de distâncias.

2.1 - Algoritmos de Estado de Enlace

Nos algoritmos de Estado de Enlace (*Link State*), **cada roteador obtém informações sobre a topologia do domínio de roteamento, incluindo a identificação de seus vizinhos e as características dos enlaces diretamente conectados**, como seus respectivos custos. Essas informações são distribuídas aos demais roteadores, **permitindo que cada um construa uma visão da topologia da rede**. A partir das informações recebidas, cada roteador constrói uma Base de Dados de Estado de Enlace (LSDB - *Link-State Database*), que representa a topologia conhecida do domínio de roteamento e os custos associados aos enlaces.

Com base nessa representação da topologia, cada roteador executa um algoritmo de caminho mínimo para determinar as melhores rotas até os demais destinos. **O algoritmo mais associado à abordagem de Estado de Enlace é o algoritmo de Dijkstra, também denominado *Shortest Path First* (SPF)**. Nesse processo, **cada roteador considera a si próprio como nó de origem e calcula os caminhos de menor custo entre a origem e os demais nós da rede**. O resultado desse cálculo é utilizado para construir a tabela de roteamento, determinando a melhor rota para cada destino.

O funcionamento do **algoritmo de Dijkstra pode ser descrito por uma etapa de inicialização seguida de iterações sucessivas**. Inicialmente, atribui-se custo zero ao nó de origem e custos provisórios aos demais nós. A cada iteração, o algoritmo seleciona o nó ainda não processado que apresenta o menor custo conhecido, atualiza os custos dos nós vizinhos e incorpora esse nó ao conjunto de nós já processados. **O processo é repetido até que sejam determinados os caminhos de menor custo a partir da origem para os demais nós alcançáveis da rede**.

2.2 - Algoritmos de Vetor de Distância

O algoritmo de Vetor de Distância (*Distance Vector*) é **iterativo, assíncrono e distribuído**. É distribuído porque cada nó recebe alguma informação de um ou mais vizinhos diretamente ligados a ele, realiza cálculos e distribui os resultados dos cálculos aos seus vizinhos. É iterativo porque esse processo continua até que mais nenhuma informação seja trocada entre vizinhos. E, é assíncrono porque não requer que todos os nós rodem simultaneamente. O roteador **não precisa conhecer toda a topologia da rede**.

O princípio de funcionamento pode ser descrito pelo **algoritmo de Bellman-Ford** onde cada roteador inicialmente conhece apenas as redes diretamente conectadas. Periodicamente, ou quando ocorre uma alteração na rede, **os roteadores trocam informações de roteamento com seus vizinhos**. A partir dessas informações, cada roteador calcula se existe um caminho de menor custo para determinado destino.

Uma característica importante dos algoritmos de Vetor de Distância é que as informações de roteamento são compartilhadas principalmente entre roteadores vizinhos, e não necessariamente entre todos os roteadores

do domínio, o que **reduz a quantidade de informações que cada roteador precisa armazenar, mas pode resultar em convergência mais lenta diante de alterações na topologia**. Nos algoritmos de Estado de Enlace, por outro lado, **tende a proporcionar convergência mais rápida e exige maior capacidade de processamento e memória para armazenar as informações da topologia** e realizar os cálculos dos caminhos.

3 - Roteamento na Internet: Protocolos de roteamento intra-domínio (IGP: OSPF, RIP) e inter-domínio (EGP: BGP).

A Internet é formada por um conjunto de redes interconectadas administradas por diferentes organizações. Para organizar o processo de roteamento em uma estrutura dessa dimensão, as redes são agrupadas em Sistemas Autônomos (AS – Autonomous Systems). Um **Sistema Autônomo corresponde a um conjunto de redes IP e roteadores administrados por uma mesma organização ou sob uma política de roteamento comum**. Um AS pode representar, por exemplo, uma grande organização, um provedor de acesso à Internet, uma empresa ou uma instituição que administra um conjunto de redes.

Os protocolos de roteamento utilizados na Internet podem ser classificados, de maneira geral, em protocolos intra-domínio (IGP – *Interior Gateway Protocol*) e protocolos inter-domínio (EGP – *Exterior Gateway Protocol*). Os IGPs são utilizados para determinar rotas dentro de um Sistema Autônomo, enquanto os protocolos inter-domínio são utilizados para a troca de informações de roteamento entre diferentes Sistemas Autônomos. Entre os principais IGPs encontram-se o RIP (*Routing Information Protocol*) e OSPF (*Open Shortest Path First*). No roteamento inter-domínio, o principal protocolo utilizado na Internet é o BGP (*Border Gateway Protocol*).

3.1 - Protocolos de roteamento intra-domínio (IGP: OSPF, RIP)

Os IGPs são protocolos utilizados para o roteamento dentro de um Sistema Autônomo. Seu objetivo é permitir que os **roteadores pertencentes ao domínio conheçam as redes internas e determinem os caminhos utilizados para encaminhar os pacotes**. Eles podem utilizar diferentes estratégias. O RIP é baseado em Vetor de Distância, enquanto o OSPF é baseado em Estado de Enlace.

O **RIP** é um protocolo de roteamento intra-domínio baseado na abordagem de **Vetor de Distância**. Sua métrica fundamental é o **número de saltos** (hop count) entre o roteador de origem e o destino. Cada roteador mantém uma tabela contendo informações sobre os destinos conhecidos, o número de saltos necessário para alcançá-los e o próximo salto. As informações são obtidas por meio da **troca de atualizações com os roteadores vizinhos**. No RIP, uma rota com até 15 saltos é considerada alcançável, enquanto o valor 16 representa infinito e, portanto, uma rede é considerada inalcançável. Essa limitação contribui para **restringir o uso do protocolo a redes relativamente pequenas**. Esse protocolo apresenta uma **estrutura simples e baixo grau de complexidade**, mas possui **limitações** relacionadas à **escalabilidade e à convergência**. Como utiliza o número de saltos como métrica, ele não considera diretamente características como largura de banda ou atraso dos enlaces para selecionar a rota.

O **OSPF** é um protocolo de roteamento intra-domínio baseado em **Estado de Enlace**. Ele permite que os roteadores construam uma representação da topologia do domínio de roteamento. Os roteadores OSPF **identificam seus vizinhos e obtêm informações sobre os enlaces diretamente conectados**. Essas informações são distribuídas aos demais roteadores por meio de mecanismos de flooding, permitindo que os roteadores construam uma base de dados denominada LSDB (Link-State Database). A partir da LSDB, cada

roteador executa o algoritmo Shortest Path First (SPF), associado ao **algoritmo de Dijkstra**, para determinar os caminhos de menor custo. A métrica utilizada pelo OSPF é denominada custo (cost). O **custo total de uma rota é obtido a partir da soma dos custos dos enlaces que compõem o caminho**. Dessa forma, o OSPF pode **considerar características dos enlaces, como a largura de banda, para determinar seus custos**. Uma característica importante do OSPF é a possibilidade de organização hierárquica do Sistema Autônomo em áreas (areas). Essa divisão em áreas reduz a quantidade de informações de estado que precisa ser processada em determinadas partes da rede e contribui para a escalabilidade.

3.2 - Protocolos de roteamento inter-domínio (BGP)

O BGP (*Border Gateway Protocol*) é utilizado para o roteamento inter-domínio, permitindo a troca de informações de alcançabilidade entre diferentes Sistemas Autônomos. Ele **permite que os Sistemas Autônomos implementem políticas de roteamento**. A **escolha da rota é fortemente relacionada a políticas** e não depende necessariamente do caminho de menor distância física ou do menor número de saltos. A decisão pode considerar atributos do BGP e políticas administrativas definidas pelo operador da rede. Esse protocolo pode ser utilizado em duas situações principais:

- eBGP (External BGP): utilizado para troca de informações de roteamento entre diferentes Sistemas Autônomos;
- iBGP (Internal BGP): utilizado para distribuir informações BGP entre roteadores pertencentes ao mesmo Sistema Autônomo.

O protocolo de roteamento inter-domínio é classificado como um protocolo do tipo Path Vector (vetor de caminho). **Seu funcionamento é baseado no anúncio de prefixos IP acompanhados de atributos de caminho e de políticas de roteamento**. Um dos principais atributos do BGP é o **AS_PATH**, **que registra a sequência de Sistemas Autônomos atravessados por uma rota**. Além de permitir a identificação do caminho, esse atributo desempenha papel importante na prevenção de loops entre Sistemas Autônomos: se um AS receber um anúncio que contenha seu próprio número no AS_PATH, poderá rejeitar essa rota.

O BGP desempenha papel fundamental na **escalabilidade da Internet** porque permite que diferentes organizações mantenham autonomia administrativa sobre seus próprios Sistemas Autônomos e, simultaneamente, troquem informações sobre os prefixos que podem alcançar.

KARINE BARBOSA CARBONARO

Presidente da Comissão Julgadora do Edital 121/2026 - FEELT

Portaria de Pessoal UFU Nº 4938, de 01 de setembro de 2026



Documento assinado eletronicamente por **Karine Barbosa Carbonaro, Presidente**, em 05/10/2026, às 19:09, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site https://www.sei.ufu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **7801225** e o código CRC **25652123**.

