XXIX INIC Encontro Latino Americano de Iniciação Científica
XXV EPG Encontro Latino Americano de Pós-Graduação
XIX INIC Jr. Encontro Latino Americano de Iniciação Científica Júnior
V ENEXUN Encontro Nacional de Extensão Universitária
XV INID Encontro de Iniciação à Docência
INIC 2025
A Ciência do NANO e seu impacto transformador no MACRO

OTIMIZAÇÃO DE ENDEREÇAMENTO IP COM SLSM E VLSM PARA MÚLTIPLOS DEPARTAMENTOS EM UMA WAN E LAN SIMULADAS

Laura Luiz Trigo, Josiely Aparecida do Espírito Santo Toledo, Wagner dos Santos Clementino de Jesus.

Universidade do Vale do Paraíba, Avenida Shishima Hifumi, 2911, Urbanova - 12244-000 - São José dos Campos-SP, Brasil, ltrigo@univap.br, josielytoledo@univap.br, wagner@univap.br.

Resumo
Este trabalho apresenta a implementação de uma rede corporativa simulada, utilizando o software *Cisco Packet Tracer,* com foco na segmentação lógica por meio das técnicas SLSM (*Same Length Subnet Mask),* VLSM (*Variable Length Subnet Mask*) e VLANs. A rede foi organizada em três departamentos diversos, Projetos, Recursos Humanos e Jurídico, com configuração de sub-redes e aplicação de políticas de roteamento e isolamento. A metodologia envolveu a construção da topologia, atribuição de endereços IP otimizados e testes de conectividade utilizando comandos como *ping* e *arp*. Os resultados demonstraram eficiência no endereçamento IP, isolamento seguro do setor jurídico por meio de VLANs e estabilidade na comunicação entre setores. O projeto busca suprir a carência de boas práticas em redes locais corporativas, apresentando como o planejamento lógico e a segmentação adequada podem melhorar significativamente a segurança, o desempenho e a escalabilidade da infraestrutura de rede.

Palavras-chave: Redes de Computadores. *Cisco Packet Tracer*. SLSM. VLSM.

Área do Conhecimento: Engenharia da Computação.

Introdução

As redes de computadores são essenciais para a comunicação em ambientes corporativos, permitindo o compartilhamento de recursos, a troca de informações e a integração de serviços críticos (Tanenbaum; Wetherall, 2011). De maneira geral, uma rede pode ser definida como um conjunto de computadores e dispositivos interligados por meio de cabos, sinais ou sistemas sem fio, que trocam informações através de protocolos padronizados, permitindo a interconexão de dispositivos para o compartilhamento de dados, serviços e recursos (Kurose; Ross, 2006). Essa infraestrutura é fundamental para garantir comunicação eficiente, segura e escalável em diferentes contextos, desde ambientes domésticos até grandes organizações. O planejamento adequado de uma rede envolve não apenas a escolha de dispositivos físicos, mas também a definição lógica de endereçamento, roteamento e protocolos de comunicação, assegurando desempenho, segurança e escalabilidade (Tanenbaum; Wetherall, 2011).

Nesse cenário, a arquitetura TCP/IP (*Transmission Control Protocol/Internet Protocol*) foi consolidada como padrão global de interconexão, organizando a comunicação em camadas e permitindo o endereçamento e roteamento de informações tanto em redes locais (LAN - *Local Area Network*) quanto em redes de longa distância (WAN - *Wide Area Network*) (Tanenbaum; Wetherall, 2011). Essa padronização é relevante em ambientes corporativos, pois garante interoperabilidade entre dispositivos de diferentes fabricantes e possibilita a implementação de políticas consistentes de segurança e controle de tráfego. Além disso, o uso de máscaras de sub-rede, em especial as variações SLSM (*Same Length Subnet Mask*) e VLSM (*Variable Length Subnet Mask*), aliado à aplicação de VLAN (*Virtual Local Area Network*), possibilita otimizar a utilização de endereços IP, segmentar setores e aprimorar o controle de acesso às informações (Neto, 2005).

Em ambientes corporativos, a aplicação dessas tecnologias busca enfrentar desafios relacionados à integração de múltiplos departamentos, à definição de políticas de segurança e à necessidade de escalabilidade da rede (Silva; Borges; Ferreira, 2019). A divisão em setores distintos, como Projetos, Recursos Humanos e Jurídico, permite estruturar o tráfego de dados de acordo com as demandas específicas de cada área, garantindo acesso controlado e protegendo informações sensíveis. Assim, a configuração lógica da rede deve atender simultaneamente a requisitos de conectividade, desempenho

e segurança, enquanto a estruturação em departamentos, com sub-redes, máscaras e *gateways* próprios, facilita o gerenciamento e reforça a proteção dos dados corporativos.

Com base nesse contexto, este trabalho teve como objetivo a implementar uma rede corporativa simulada no software *Cisco Packet Tracer* (Scott, 2019), como estudo de caso da disciplina de Redes de Computadores. A simulação partiu de um roteador já conectado à internet WAN, ao qual foram integrados os demais dispositivos e setores. Foram aplicados conceitos de roteamento, segmentação de rede por SLSM e VLSM, uso de VLANs e análise de protocolos de comunicação, além da exploração de diferentes topologias. O principal desafio concentrou-se no isolamento das estações do Departamento Jurídico, configuradas para se comunicar exclusivamente por meio do roteador R2, assegurando a confidencialidade das informações e a proteção do ambiente corporativo.

Metodologia

O estudo refere-se à análise e solução de um problema de rede simulado no *software Cisco Packet Tracer*. A topologia, previamente disponibilizada como estudo de caso da disciplina de Redes de Computadores, deveria ser reproduzida de forma rigorosa no ambiente de simulação. Como base para essa construção, foi fornecido um arquivo modelo contendo um roteador Cisco 2911 já conectado à internet WAN a partir do qual foi implementado o restante da topologia. Para a composição da rede, foram utilizados 8 *switches* de 24 portas, dois roteadores R1 (modelo 2911) e R2 (modelo 1841), além de 15 dispositivos finais, sendo 6 estações de trabalho nomeadas e 9 PCs (*Personal Computer*) genéricos.

O Departamento de Projetos é composto pelas estações de trabalho 1 e 2, conectadas ao *Switch* A, que por sua vez se interliga ao *Switch* 2 e, posteriormente, aos *switches* 1 e 3, formando uma topologia em barramento. Todos os dispositivos desse setor foram configurados com a mesma máscara de sub-rede. Já o Departamento de Recursos Humanos adota uma topologia estrela, composta pelos *switches* B, 4, 5 e 6, sendo o *Switch* B o nó central, responsável pela conexão com os demais. Nesse setor, cada *switch* possui um PC genérico conectado, enquanto as estações 3 e 4 estão ligadas diretamente ao *Switch* B. Assim como no departamento anterior, todos os dispositivos utilizam a mesma máscara de sub-rede, embora com valor distinto. Por fim, o Departamento Jurídico conta com as estações 5 e 6, que se comunicam por meio do roteador R2: a Estação 5 conecta-se ao *Switch* B, que estabelece o enlace com o roteador, enquanto a Estação 6 se conecta diretamente ao R2. Os endereços IP atribuídos a esse setor estão detalhados na Tabela 1.

Tabela 1 - IPs dos dispositivos do Departamento Jurídico.

Roteador	IP
R1	52.85.213.1/8 (WAN) 172.17.11.1/16 (Projetos) 192.168.10.1/28 (RH/Jurídico)
R2	192.168.10.1/28 (RH/Jurídico) 10.0.0.1/6 (Jurídico)

Fonte: Autores (2025).

A tabela evidencia a configuração de múltiplas interfaces nos roteadores, demonstrando a integração entre os setores e o isolamento lógico do departamento Jurídico.

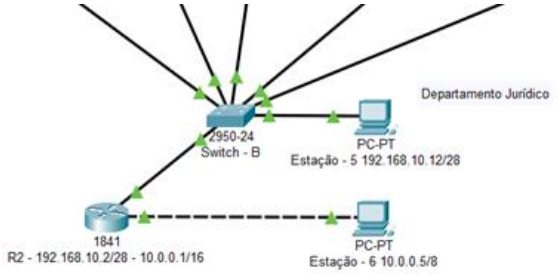
Resultados

Comentado [AA1]: Sugestão:
Tabela resumo de sub-redes → síntese clara e objetiva.
Gráfico dos testes de ping → reforça a análise de desempenho.
Figura destacando VLANs e isolamento → aumenta impacto visual.
(Opcional) **Fluxo de comunicação** → ilustra restrições aplicadas.

Após a implementação da rede proposta, foram realizados testes de conectividade entre as estações. O uso do comando *ping* entre redes permitiu identificar e resolver problemas de comunicação. O principal desafio enfrentado foi o bloqueio de acesso à internet das estações 5 e 6 por

meio do roteador R2. A estação 6 foi isolada com maior facilidade por utilizar uma máscara de sub-rede distinta e possuir ligação direta com o roteador, o que viabilizou a implementação de uma VLAN simples. Já para a estação 5, foi necessária a criação de uma VLAN no *Switch* B e a configuração de uma subinterface no roteador R2, limitando sua comunicação apenas a esse roteador e bloqueando o tráfego com o restante da rede. A Figura 1 apresenta a seção da topologia onde foi aplicada a VLAN para o isolamento das estações 5 e 6.

Figura 1 – Seção das estações 5, 6 e do Switch B, com destaque para aplicação da VLAN.



Fonte: Autores (2025).

Em seguida, a comunicação com a *internet* para as demais estações por meio do roteador R1 foi estabelecida. A transferência de arquivos entre diferentes setores ocorreu da seguinte forma: a estação de origem enviava os pacotes ao roteador, que então identificava o IP de destino e realizava o encaminhamento adequado. Com a resolução dos problemas identificados, a rede passou a funcionar conforme o esperado, permitindo o acesso à *internet* com tempos de resposta consistentes e garantindo o isolamento eficaz do departamento jurídico.

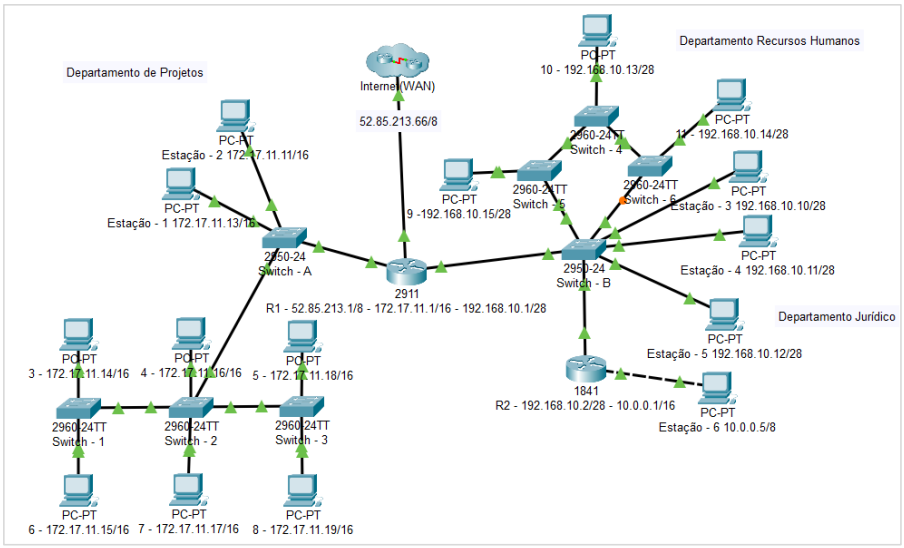
Durante os testes, confirmou-se ainda que as sub-redes foram alocadas de forma eficiente. No setor de Recursos Humanos, a máscara /28 disponibilizou 14 endereços utilizáveis, atendendo ao número de *hosts* do departamento. Já o setor de Projetos, configurado em VLSM, demonstrou flexibilidade no uso do espaço de endereçamento, evitando desperdício de IPs. O comando *arp -a* exibiu as tabelas ARP (*Address Resolution Protocol*) confirmando que toda comunicação entre redes distintas ocorreu por meio dos roteadores, validando o papel de *gateway*. Além disso, os pacotes ICMP (*Internet Control Message Protocol*) evidenciaram tempos de resposta estáveis, mesmo após a aplicação das restrições de acesso.

A figura 2 mostra a topologia da rede corporativa simulada, dividida nos departamentos de Projetos, Recursos Humanos e Jurídico. Os dispositivos estão interligados por *switches* e dois roteadores (R1 e R2), com segmentação de rede por SLSM e VLSM. O roteador R1 conecta a rede à internet WAN, enquanto o R2 garante o isolamento das estações 5 e 6 do setor Jurídico, que só se comunicam por ele. Cada departamento utiliza sub-redes específicas, demonstrando o uso de VLANs, *gateways* e planejamento hierárquico para segurança e escalabilidade.

A estrutura adotada possibilitou a segmentação eficiente da rede, combinando sub-redes estáticas e variáveis para atender às necessidades específicas de cada departamento. A utilização de VLANs reforçou o isolamento lógico, prevenindo interferências e acessos não autorizados entre setores. Além disso, o emprego de roteadores com múltiplas interfaces e subinterfaces facilitou o gerenciamento do tráfego e a aplicação de políticas de segurança, garantindo o controle centralizado do fluxo de dados. Essa arquitetura demonstrou ser flexível e adaptável, permitindo futuras expansões sem comprometer a integridade e o desempenho da rede.

Além da validação funcional, foi possível observar que a configuração das VLANs e o uso combinado de SLSM e VLSM resultaram em uma significativa otimização do uso do espaço de endereçamento IP, minimizando desperdícios comuns em redes corporativas tradicionais. A segmentação lógica implementada contribuiu para a redução do tráfego *broadcast* entre departamentos, o que aumenta a eficiência da rede e a segurança dos dados trafegados.

Figura 2 - Topologia Geral da Rede Implementada no *Cisco Packet Tracer*.



Fonte: Autores (2025).

Discussão

No modelo SLSM, foi configurada a rede 192.168.10.0/28, destinada aos departamentos de Recursos Humanos e Jurídico. A faixa 192.168.10.x pertence originalmente à classe C, cuja máscara padrão é /24 (255.255.255.0). Contudo, ao utilizar a máscara /28 (255.255.255.240), a rede foi subdividida em blocos menores, cada um com até 16 endereços (14 utilizáveis). No modelo VLSM, aplicou-se a rede 172.17.0.0/16. A análise dos endereços atribuídos (172.17.11.1 até 172.17.11.19) mostra que todos pertencem à mesma rede principal, de classe B, com máscara padrão /16 (255.255.0.0). Entretanto, os endereços foram distribuídos em diferentes segmentos da topologia, conforme a necessidade de cada setor. Esse comportamento caracteriza o uso de VLSM, em que uma rede maior é dividida em sub-redes menores de tamanhos variáveis, otimizando o uso de IPs e possibilitando maior flexibilidade de planejamento.

O comando *ping* foi utilizado para validar a conectividade. Nesse processo, uma estação do setor de Projetos enviou um pacote ICMP ao *gateway* configurado (R1). O roteador, ao reconhecer que o destino pertencia a outra rede, realizou o encaminhamento, permitindo que a estação de Recursos Humanos respondesse. O retorno percorreu o mesmo caminho, confirmando a comunicação entre redes distintas. Durante o teste de *ping,* os pacotes atravessaram diferentes camadas do modelo OSI. Na camada de rede (3), foram definidos os endereços IP de origem e destino, como no caso da estação 1 (172.17.11.13/16) ao se comunicar com a estação 3 (192.168.10.10/28). Na camada de enlace (2), o pacote IP foi encapsulado em quadros *Ethernet* contendo endereços MAC (*Media Access Control*), inicialmente direcionados ao roteador. Este, ao receber o quadro, descapsulou o pacote, verificou a rota e o reencapsulou com o MAC de destino. Por fim, na camada física (1), os dados foram transmitidos como sinais pelo meio físico.

O protocolo ICMP desempenhou papel de diagnóstico e monitoramento, verificando disponibilidade e tempo de resposta. O protocolo IP cuidou do endereçamento e roteamento entre redes distintas, enquanto o *Ethernet* atuou no transporte local, definindo quadros e endereços MAC. Dessa forma, observou-se a integração entre os três protocolos para garantir conectividade eficiente. O comando arp-a exibiu as tabelas ARP, listando os endereços IP e MAC pertencentes à mesma rede local. No

caso da estação 4 e da WAN, por estarem em redes diferentes, a comunicação ocorreu por meio do roteador, que funcionou como intermediário. Assim, a tabela apresentou apenas os endereços MAC da estação de origem e do roteador. No setor de Recursos Humanos, a máscara utilizada foi 255.255.255.240 (/28). Esse prefixo reserva 28 dos 32 bits para a rede, restando 4 para os *hosts*. Em notação binária, corresponde a *11111111.11111111.11111111.11110000*. Dessa forma, são possíveis 16 endereços por sub-rede, dos quais 14 são utilizáveis.

O roteador R2 foi configurado com duas interfaces distintas. A primeira, 192.168.10.2/28, de classe C, foi adaptada para uma máscara /28, criando 16 sub-redes com 14 *hosts* cada. A segunda, 10.0.0.1/16, de classe A, normalmente associada à máscara /8, foi configurada com /16, resultando em 256 sub-redes, cada uma suportando até 65.534 *hosts*. O papel do R2 foi central: interligou sub-redes distintas, encaminhou pacotes e aplicou regras de acesso, especialmente no setor Jurídico. As estações 5 e 6 tiveram sua comunicação restrita, sendo que a estação 6 foi isolada em uma VLAN dedicada, permitindo contato apenas com o roteador e bloqueando acessos externos.

Quanto à topologia, os *switches* 1, 2 e 3 utilizaram a configuração em barramento, caracterizada por simplicidade, baixo custo e facilidade de expansão, mas limitada em escalabilidade e vulnerável a falhas e colisões. Portanto os *switches* 4, 5 e 6 adotaram a topologia em árvore, que combina aspectos de estrela e barramento. Essa estrutura favorece a escalabilidade e a organização da rede, sendo mais adequada a ambientes corporativos maiores, embora demande maior gerenciamento e dependa do funcionamento do nó raiz.

A carência de configurações em redes LANs com segmentação lógica, controle de acesso e otimização de endereçamento IP ainda é uma realidade comum em muitos ambientes corporativos. Mesmo com o avanço das tecnologias de rede, é frequente encontrar infraestruturas locais sem o uso de boas práticas como VLANs eficientes, o que compromete o desempenho, a segurança e a escalabilidade da rede. O presente estudo busca contribuir para essa lacuna ao demonstrar, por meio de uma simulação prática, como a aplicação combinada de VLANs, SLSM e VLSM pode aprimorar significativamente a organização, o controle e a eficiência das redes locais. Por meio da implementação de sub-redes específicas para cada departamento, o uso estratégico de roteadores com múltiplas interfaces e a configuração de VLANs para isolar setores críticos demonstram uma arquitetura LAN moderna, segura e funcional, alinhada às necessidades de ambientes corporativos reais.

A proposta da rede implementada neste trabalho, em colaboração com os princípios da área de Tecnologia da Informação, consiste em apresentar uma configuração estruturada de uma rede corporativa local utilizando VLANs, segmentação IP e políticas de roteamento. Essa abordagem é altamente relevante para o contexto atual da Engenharia da Computação, pois reflete situações reais enfrentadas por profissionais da área ao projetar redes que exigem não apenas conectividade, mas também segurança, escalabilidade e organização lógica. Ao propor soluções práticas para problemas como o isolamento de setores sensíveis e a comunicação eficiente entre departamentos, o projeto serve como base de referência para a aplicação acadêmica e profissional de conceitos fundamentais de redes. Dessa forma, reforça-se a importância do planejamento detalhado da infraestrutura de TI e da adoção de boas práticas na construção de redes locais em ambientes corporativos.

Conclusão

A implementação da rede simulada no *Cisco Packet Tracer*, baseada no projeto proposto pelo docente, possibilitou não apenas a consolidação de conceitos essenciais de redes de computadores, mas também a vivência prática de situações comumente encontradas em ambientes corporativos. Foram aplicados princípios de roteamento, segmentação em sub-redes, uso de *gateways*, VLANs, controle de acesso, além da exploração dos modelos SLSM e VLSM, fundamentais para o planejamento e a otimização de endereços IP. A experiência demonstrou a importância da organização lógica da rede, evidenciada pela correta aplicação de máscaras, pela distribuição eficiente de endereços e pelo isolamento de setores com diferentes necessidades de comunicação.

O maior desafio identificado foi o isolamento seguro do Departamento Jurídico (estações 5 e 6), que foi superado por meio da configuração de VLANs e regras de roteamento no R2, garantindo que apenas os fluxos de dados autorizados fossem permitidos. Essa solução assegurou a confidencialidade das informações e demonstrou a relevância do controle de acesso em redes corporativas. Os testes de conectividade com o comando *ping* reforçaram a confiabilidade da configuração (Awati, 2021) confirmando o encaminhamento correto entre setores, o bloqueio de acessos indevidos e a eficiência

do roteamento aplicado. Além disso, a análise da comunicação permitiu observar na prática a atuação dos protocolos ICMP, IP e *Ethernet*, assim como a interação das camadas 1, 2 e 3 do modelo OSI, evidenciando a importância de cada nível para o funcionamento da rede como um todo.

Outro aspecto relevante foi a análise das topologias adotadas. A configuração em barramento nos *switches* 1, 2 e 3, embora simples e de baixo custo, mostrou suas limitações em termos de escalabilidade e confiabilidade. Já a topologia em árvore nos *switches* 4, 5 e 6 demonstrou maior adequação para redes mais complexas, ainda que demande maior gerenciamento. Essa comparação contribuiu para compreender como a escolha da topologia física influencia diretamente o desempenho, a manutenção e a segurança da rede. Portanto, conclui-se que a rede foi projetada e configurada de forma eficaz, atendendo aos requisitos de segurança, funcionalidade e escalabilidade. Além disso, o projeto permitiu desenvolver uma visão mais crítica sobre os desafios do planejamento de redes e sobre a importância de soluções que conciliem eficiência, flexibilidade e proteção dos dados.

Referências

AWATI, R. **Máscara de sub-rede de comprimento variável (VLSM)**. TechTarget Btasil, 18 out. 2021. Disponível em: https://www.techtarget.com/searchnetworking/definition/variable-length-subnet-mask. Acesso em: 20 maio 2025.

KUROSE, J.; ROSS, K. **Redes de computadores e Internet**. São Paulo: Person, 2006.

NETO, C. C. **A arquitetura TCP/IP e a configuração das redes de computadores por meio das máscaras de sub-rede**. *Cadernos de Estudos e Pesquisas*, n. 23, p. 15-28, 2005. ISSN 1517-5758.

SCOTT, E. **Portable Command Guide: All the Ccna 200-301 Commands in One Compact**, **Portable Resource**. 5. ed. Indoanapolis: CiscoPress, 2019.

SILVA, J. E. da; BORGES, A. M.; FERREIRA, M. F. **Implantação de nova rede de computadores em ambiente corporativo utilizando tecnologia IEEE 802.11-AX**. Revista Agroveterinária, Negócios e Tecnologias, Coromandel, v. 5, n. 2, p. 17-25, jul./dez. 2019. ISSN 2595-007X.

TANENBAUM, A. S.; WETHERALL, D. **Redes de Computadores**. 5. ed. São Paulo: Pearson, 2011.

Comentado [AA2]: Deixar as referências em ordem alfabética, letras maiúsculas e o título em negrito. Verifiquem o modelo de artigo.

Agradecimentos

Gostaríamos de agradecer à Universidade do Vale do Paraíba (UNIVAP) pelo suporte institucional durante o desenvolvimento deste trabalho. Agradecemos especialmente ao Prof. Wagner, responsável pela disciplina de Redes de Computadores I, pela orientação e dedicação em sala de aula.