



Universidade de São Paulo  
Instituto de Ciências Matemáticas e de Computação  
Departamento de Sistemas de Computação

**SSC0540 - Redes de Computadores**

Docente: Prof. Jo Ueyama  
Monitor: Rodrigo Dutra Garcia

## ***PROJETO 2***

### **COMUNICAÇÃO ENTRE DUAS REDES**

Laura Fernandes Camargos - [laura.camargos@usp.br] - 13692334

São Carlos, June 21, 2024

# 1 Empresa

A Raízen é uma empresa brasileira líder no setor de energia, dedicada à produção e comercialização de biocombustíveis, açúcar e energia proveniente de fontes renováveis.

No terceiro trimestre do ano-safra 2023/2024, correspondente ao período de outubro a dezembro, a empresa anunciou um lucro líquido impressionante de 754,4 milhões de reais em seu balanço, sendo a 3<sup>a</sup> maior empresa em faturamento no Brasil. No Brasil, possui escritórios no Rio de Janeiro, em São Paulo e Piracicaba, e ao todo conta com uma equipe de mais de 46 mil colaboradores e 15 mil parceiros de negócios, se consagrando uma potência verde.

Além de sua presença nacional, a Raízen expande suas operações para a Argentina e o Paraguai, com ambições de alcançar ainda mais territórios além das Américas. Movida pela missão de impulsionar a sociedade com soluções em energia, a Raízen é mais do que uma empresa; é uma força transformadora que molda o futuro da energia em escala global.

# 2 Projeto

O projeto envolveu a melhoria da solução implementada no projeto 1. Sendo assim, foram implementadas três áreas: a filial de São Paulo, a filial de Piracicaba e o backbone. A topologia da rede implementada envolve duas principais localidades (filiais), cada uma com três departamentos (TI, Vendas, RH). Cada departamento foi segmentado em VLANs separadas, usando switches multilayer para roteamento interVLAN. Foi configurado um servidor DHCP dedicado para cada VLAN, fornecendo gerenciamento eficiente de endereços IP.

O backbone implementado interliga as filiais. Neste backbone, foram implementados serviços críticos como HTTP, FTP, SMTP e DNS, centralizando esses recursos para melhorar a eficiência operacional e a segurança da rede. Um servidor dedicado foi reservado para o gerenciamento de dispositivos IoT, protegido por um firewall para controlar o acesso ao servidor IoT(HTTP).

Essa organização oferece várias vantagens significativas, como melhor desempenho e segurança devido à redução no domínio de broadcast, gerenciamento simplificado através da administração centralizada dos switches multilayer, escalabilidade que suporta o crescimento da empresa sem comprometer

a performance, e maior confiabilidade com a atribuição eficiente de endereços IP e redundância da rede.

Em suma, essa implementação melhorar o desempenho e a segurança, uma vez que organiza os departamentos em VLANs separadas, centraliza os serviços críticos no backbone para simplificar o gerenciamento e melhorar a disponibilidade e implementa políticas de segurança, como o FireWall, para proteger os serviços e dados críticos, garantindo que apenas tráfego autorizado tenha acesso.

Além disso, foi implementado o protocolo OSPF para gerenciar a comunicação entre os roteadores e definir as áreas OSPF de acordo com a estrutura da empresa. A área 1 foi designada para São Paulo, que tem uma infraestrutura de rede maior e mais complexa em comparação com Piracicaba, a área 0 representa o backbone ou área compartilhada, enquanto a área 2 foi configurada para a filial em Piracicaba.

## 3 Localidade 1 (São Paulo)

### 3.1 Segmentação das Redes

Table 1: Endereços IPs e Máscaras de Sub-rede da filial de SP

Rede	Endereço IP	Máscara de Sub-rede
VLAN10/Departamento TI	192.168.1.0/24	255.255.255.0
VLAN20/Departamento Vendas	192.168.2.0/24	255.255.255.0
VLAN30/Departamento RH	192.168.3.0/24	255.255.255.0

A configuração da máscara de sub-rede "/24" foi implementada pensando em escalabilidade, uma vez que oferece grande capacidade de endereçamento IP em uma única rede. Logo, isso é adequado para um ambiente empresarial onde cada departamento pode ter várias estações de trabalho, impressoras, e outros dispositivos conectados.

### 3.2 Equipamentos Utilizados

- 3 Switches (Switch-PT)

- 2 Switches Multilayer 3560-24PS
- 2 Access Point (AccessPoint-PT)
- 12 Computadores
- 4 Laptop
- 2 Smartphones
- 2 Tablets
- 6 Ar Condicionado
- 6 Monitores de Temperatura

## 4 Localidade 2 (Piracicaba)

### 4.1 Segmentação das Redes

Table 2: Endereços IPs e Máscaras de Sub-rede

Rede	Endereço IP	Máscara de Sub-rede
<b>VLAN40/Departamento TI</b>	192.168.4.0/24	255.255.255.0
<b>VLAN50/Departamento Vendas</b>	192.168.5.0/24	255.255.255.0
<b>VLAN60/Departamento RH</b>	192.168.6.0/24	255.255.255.0

A configuração da máscara de sub-rede ”/24” foi implementada pensando em escalabilidade, uma vez que oferece grande capacidade de endereçamento IP em uma única rede. Logo, isso é adequado para um ambiente empresarial onde cada departamento pode ter várias estações de trabalho, impressoras, e outros dispositivos conectados.

## 4.2 Equipamentos Utilizados

- 3 Switches (Switch-PT)
- 2 Switches Multilayer 3560-24PS
- 2 Access Point (AccessPoint-PT)
- 12 Computadores
- 4 Laptop
- 2 Smartphones
- 2 Tablets
- 6 Ar Condicionado
- 6 Monitores de Temperatura

## 5 Backbone

A área 0, também conhecida como área compartilhada, interconecta todas as outras áreas por meio do protocolo OSPF e é responsável pela distribuição de informações de roteamento. Utilizamos três roteadores na área 0 para garantir redundância e resiliência à infraestrutura, assegurando que a rede permaneça operacional mesmo se um roteador falhar. Essa configuração do "backbone", baseada em VLANs, permite separar fisicamente a rede em múltiplas redes lógicas independentes, o que proporciona maior segurança, eficiência e flexibilidade.

Nesse contexto, foram implementadas as alterações nos servidores conforme solicitado, permitindo que os serviços HTTP, FTP, SMTP e DNS fossem compartilhados entre as filiais. Ao concentrar esses serviços críticos em um único servidor no backbone da rede, simplifica-se a administração e manutenção. Em vez de distribuir esses serviços em múltiplos locais físicos (nas filiais), é possível gerenciá-los de forma centralizada. Isso reduz a complexidade operacional e os custos associados à manutenção de vários servidores. Além disso, implementar tais serviços no backbone é pensar em escalabilidade, uma vez que essa infraestrutura pode suportar facilmente o crescimento das operações da empresa. Adicionar novas filiais ou aumentar

o número de usuários não exige a expansão física dos serviços em cada localidade, pois o backbone pode ser dimensionado para lidar com mais carga conforme necessário. Um segundo servidor foi dedicado ao gerenciamento de dispositivos IoT, protegido por um firewall que controla rigorosamente o acesso a sua página HTTP. No projeto, a permissão pode ser dada a uma rede

## 5.1 Segmentação das Redes

Table 3: Endereços IPs e Máscaras de Sub-rede

Rede	Endereço IP	Máscara de Sub-rede
<b>Servidor DNS,HTTP,SMTP,FTP</b>	30.0.0.0/24	255.255.255.0
<b>Servidor IoT</b>	40.0.0.0/30	255.255.255.252

As redes 30.0.0.0/24 foram alocadas para os serviços de DNS, HTTP e outros serviços essenciais para garantir que cada filial tenha acesso rápido e seguro aos recursos compartilhados na área 0. A rede 40.0.0.0/30 foi reservada especificamente para o servidor IoT, garantindo um ambiente controlado e protegido para dispositivos IoT. A conexão entre esses dois servidores é feita por meio de um roteador (representa a área0), que se conecta aos demais roteadores das filiais, formando um triângulo de conexão. As máscaras de sub-rede /30 garantem que os roteadores possam se comunicar eficientemente sem sobrecarregar a rede com endereços IP desnecessários.

## 5.2 Equipamentos Utilizados

- 3 Roteadores (2911)
- 2 Servidores
- 1 Switch (2960-24TT)
- 1 FireWall (4406-X)

## 6 Escalabilidade

A implementação do protocolo OSPF proporciona adaptação dinâmica à medida que a rede cresce, facilitando o balanceamento de carga e a segmentação eficiente da rede em áreas hierárquicas. Isso reduz significativamente o processamento necessário em cada roteador e melhora a eficiência operacional geral.

A segmentação dos diferentes departamentos (TI, Vendas, RH) utilizando VLANs isola o tráfego de rede de cada área, o que reduz o domínio de broadcast e aprimora o desempenho da rede à medida que ela se expande. Cada VLAN pode ser gerenciada de forma independente, permitindo mudanças e ajustes conforme necessário.

Além disso, a atribuição de um pool DHCP dedicado para cada departamento evita conflitos de endereços IP e simplifica o gerenciamento dos endereços atribuídos. Isso é essencial em ambientes corporativos com muitos dispositivos, garantindo conectividade confiável e eficiente.

Os switches multilayer desempenham um papel crucial ao permitir um gerenciamento centralizado mais eficiente. Isso inclui a configuração de VLANs, roteamento interVLAN e implementação de políticas de segurança de forma integrada. Sua capacidade de suportar um grande número de VLANs e tráfego de rede sem comprometer o desempenho faz com que sejam ideais para escalabilidade.

Com VLANs bem definidas e endereços IP organizados em sub-redes /24, a expansão da empresa pode ser facilmente realizada adicionando novos dispositivos e departamentos sem a necessidade de reconfigurar toda a infraestrutura de rede. Isso não apenas economiza tempo e recursos, mas também garante uma operação contínua e eficiente à medida que a empresa cresce e suas necessidades de rede se expandem.

## 7 Aplicação IoT

Utilizou-se um sensor de temperatura IoT para constantemente monitorar a temperatura ambiente em cada departamento.

Lógica de Controle: Com base na leitura do sensor, foi estabelecida uma lógica de controle para o ar condicionado:

Condição de Ligar: Se a temperatura ambiente for igual ou superior a 27 graus Celsius, o ar condicionado é ligado automaticamente. Condição

de Desligar: Quando a temperatura cair abaixo de 27 graus Celsius, o ar condicionado é desligado.

Essa automação permite manter um ambiente confortável e eficiente em termos de energia nos departamentos, respondendo automaticamente às mudanças de temperatura ambiente sem intervenção manual e ajuda a reduzir o consumo de energia ao ligar o ar condicionado apenas quando necessário, com base na temperatura ambiente real.

## 8 Segurança

Em relação a segurança da rede, alguns tópicos implementados devem ser destacados:

- Segregação de VLANs: A segmentação por VLANs ajuda a limitar o tráfego de rede dentro de cada departamento, reduzindo o impacto de possíveis ataques internos de rede.
- Políticas de Controle de Acesso (ACLs): A implementação de ACLs restringe o acesso apenas aos dispositivos/redes autorizados dentro do ambiente controlado. Isso ajuda a proteger contra acessos não autorizados e garante que somente os usuários e dispositivos apropriados possam interagir com os recursos do servidor IoT, mantendo a integridade e a confidencialidade dos dados.
- Firewall: O uso de firewalls é crucial para controlar o acesso aos serviços críticos e proteger contra ameaças externas. Por exemplo, você mencionou que o servidor IoT está protegido por um firewall que permite apenas o acesso HTTP. Isso restringe potenciais vulnerabilidades e ataques.



## 9 Custo

Para calcular o custo aproximado dos equipamentos necessários para o projeto descrito, considerei os custos dos equipamentos e da hora de trabalho:

### 9.1 Custo dos Equipamentos

Table 4: Custo dos Equipamentos em reais

Equipamento	Custo Unitário	Quantidade
Roteadores Cisco 2911	R\$7.500 - R\$10.000	3
Servidores	R\$10.000 - R\$15.000	2
Switch Cisco 2960-24TT	R\$2.500 - R\$5.000	1
Firewall Cisco ASA 4406-X	R\$15.000 - R\$25.000	1
Switches genéricos (Switch-PT)	R\$250 - R\$500	3
Switches Multilayer 3560-24PS	R\$2.500 - R\$5.000	2
Access Points (AccessPoint-PT)	R\$250 - R\$500	2
Computadores	R\$2.500 - R\$5.000	12
Laptops	R\$2.500 - R\$5.000	4
Smartphones	R\$1.000 - R\$2.500	2
Tablets	R\$1.000 - R\$2.500	2
Ar Condicionados	R\$1.000 - R\$2.500	6
Monitores de Temperatura	R\$1.000 - R\$2.500	6

### 9.2 Custo de Trabalho

Considerando um valor de hora de trabalho de R\$90,00 e um total de 150 horas dedicadas ao projeto, o custo do planejamento da rede seria:

- **Custo por hora de trabalho:** R\$90,00
- **Horas totais dedicadas ao projeto:** 150 horas

O custo total do projeto seria:

Custo total do projeto = Custo por hora de trabalho  $\times$  Horas dedicadas ao projeto

$$\text{Custo total do projeto} = \text{R\$90,00/h} \times 150\text{h}$$

$$\text{Custo total do projeto} = \text{R\$13.500,00}$$

Assim, uma estimativa fictícia do custo do trabalho de planejamento do projeto de rede para os escritórios da Raízen seria de R\$13.500,00.

## 10 Ajustes Previstos e Considerações Finais

Durante o desenvolvimento do projeto de implementação da infraestrutura de rede para os escritórios da Raízen em São Paulo e Piracicaba, alguns ajustes foram identificados para garantir o sucesso e a eficiência da operação.

Uma das principais considerações diz respeito à escalabilidade da infraestrutura. Por mais que o projeto tenha sido desenvolvido para atender às necessidades atuais da empresa, é importante estar preparado para futuros crescimentos e demandas adicionais. Nesse sentido, o planejamento é manter uma abordagem modular e flexível, permitindo fácil expansão e adaptação conforme necessário.