



UNIFACS (UNIVERSIDADE SALVADOR)

ARIEL SOARES FRANCO (RA: 12722210594)

GABRIEL COUTINHO (RA: 1272412136)

MANUELLE REIS SANTANA (RA: 1272116405)

**MARCELA TOURINHO MACHADO BARRETO (RA:
12724139040)**

YARA CAROLINA LEITE DOS SANTOS (RA: 12724136783)

AMBIENTES COMPUTACIONAIS E CONECTIVIDADE (A3)

Salvador

2024

SUMÁRIO

1. INTRODUÇÃO	3
2. DESCRIÇÃO DO CENÁRIO DO PROJETO	4
3. ENDEREÇAMENTO DE REDE E MÁSCARA DE REDE	5
4. CONFIGURAÇÃO DE PROTOCOLOS E SERVIÇOS.....	8
5. REDUNCÂNCIA E ALTA DISPONIBILIDADE	10
6. SERVIDORES DNS E WEB.....	11
7. CENÁRIO DE IOT E ENERGIA ACESSÍVEL E LIMPA.....	12
8. TESTES E VALIDAÇÃO.....	13
9. CONCLUSÃO.....	14

1 INTRODUÇÃO

O desenvolvimento das tecnologias de comunicação e a crescente demanda por soluções integradas têm transformado as infraestruturas de redes de computadores. Este projeto tem como objetivo criar uma rede metropolitana conectando duas empresas e um cenário de Internet das Coisas (IoT) interligados por uma rede metropolitana central, utilizando o Cisco Packet Tracer para simulação da montagem e protocolos necessários.

A rede proposta será composta por roteadores configurados com o protocolo OSPF, garantindo a redundância e continuidade dos serviços. Cada empresa terá servidores com DHCP e web, além de serviços de DNS na rede metropolitana. A integração da IoT permitirá a comunicação entre dispositivos inteligentes e a rede, oferecendo soluções de automação e monitoramento.

Além disso, o projeto será relacionado aos Objetivos de Desenvolvimento Sustentável (ODS) 7 (Energia Limpa e Acessível), 9 (Indústria e Inovação) e 11 (Cidades Sustentáveis), promovendo cidades mais inteligentes e eficientes. A seguir, serão apresentadas as especificações do projeto, suas configurações e a integração com os ODS.

2 DESCRIÇÃO DO CENÁRIO DO PROJETO

A rede em si é composta por 4 cenários principais, vamos cobrir cada um deles passando por sua montagem e configuração.

2.1 Rede metropolitana

A rede metropolitana é a área principal do projeto sendo esta a responsável por guardar entidades importantes como o registro das rotas principais, o servidor DNS e os servidores Web de cada empresa.

2.2 Redes das empresas

Aqui cobrimos duas entidades ao mesmo tempo, já que a única diferença significativa entre as duas empresas pedidas na proposta era que uma delas tivessem 100 hosts e a outra 500, ademais as duas entidades são idênticas pois ambas cobrem requisitos como uso do protocolo DHCP para alocação dinâmica de IP's e utilização do protocolo NAT para tradução de endereços privados para públicos.

2.3 Rede Doméstica/IOT

Esta é a única rede que se sobressai em relação às outras pois utiliza conexões via wireless para que assim tenhamos mais flexibilidade na criação de um cenário IOT. Nesta também foram consideradas as ODS 7, 9 e 11.

3. ENDEREÇAMENTO DE REDE E MÁSCARAS DE REDE

A escolha de Endereçamento IP e máscaras de rede foi um passo essencial para que conseguíssemos ter uma boa comunicação que cumprisse os requisitos sem extrapolar ou faltar endereços válidos em nenhum dos cenários.

3.1 Endereçamento da Rede Metropolitana

Na rede metropolitana decidimos por utilizar o endereçamento **200.10.0.0/30** (com máscara **255.255.255.252**) devido a alguns pontos notáveis deste cenário, por exemplo:

- Nesta rede teríamos no máximo 5 roteadores interconectados, logo escolher uma máscara maior como /29 ou /28, resultaria em desperdício de endereços.
- A divisão da rede em sub-redes com máscara **/30** torna a configuração mais simples e facilita a identificação das conexões ponto-a-ponto entre os roteadores. Cada link terá sua própria sub-rede, minimizando ambiguidades.
- Neste cenário teríamos de utilizar o protocolo OSPF para simplificação de rotas, o protocolo **OSPF** se beneficia de sub-redes pequenas e bem definidas, pois isso reduz a quantidade de informações de roteamento compartilhadas entre os roteadores.

Aqui segue os endereços e as conexões de cada roteador da rede metropolitana:

Rede escolhida 200.10.0.0/30 (máscara 255.255.255.252):

Sub-rede	Endereço de rede	Endereço usável 1	Endereço usável 2	Endereço de Broadcast
Sub rede 1	200.10.0.0	200.10.0.1	200.10.0.2	200.10.0.3
Sub rede 2	200.10.0.4	200.10.0.5	200.10.0.6	200.10.0.7
Sub rede 3	200.10.0.8	200.10.0.9	200.10.0.10	200.10.0.11
Sub rede 4	200.10.0.12	200.10.0.13	200.10.0.14	200.10.0.15
Sub rede 5	200.10.0.16	200.10.0.17	200.10.0.18	200.10.0.19
Sub rede 6	200.10.0.20	200.10.0.21	200.10.0.22	200.10.0.23

Endereçamento na rede:

Link	Sub-rede(CIDR)	Interface Roteador A	Interface Roteador B
R1 ↔ R2	200.10.0.0	200.10.0.1	200.10.0.2
R1 ↔ R3	200.10.0.4	200.10.0.5	200.10.0.6
R1 ↔ R4	200.10.0.8	200.10.0.9	200.10.0.10
R2 ↔ R3	200.10.0.12	200.10.0.13	200.10.0.14
R2 ↔ R3	200.10.0.16	200.10.0.17	200.10.0.18
R3 ↔ R4	200.10.0.20	200.10.0.21	200.10.0.22

3.2 Endereçamento das redes empresariais

Cada empresa tinha um requisito em específico, uma delas abrigaria 100 hosts enquanto a outra abrigaria 500. Para isso levamos alguns pontos em consideração nas escolhas de endereçamentos, por exemplo:

1. Empresa com 100 hosts: 192.168.1.0/25 (máscara 255.255.255.128)
 - A máscara **255.255.255.128** divide a rede em sub-redes de 128 endereços cada, dos quais 126 são utilizáveis para hosts.
 - Como a empresa precisa de 100 hosts, a sub-rede **192.168.1.0/25** é suficiente, deixando ainda uma margem de 26 endereços utilizáveis para expansão futura.
 - Essa escolha evita o desperdício de IPs, pois sub-redes maiores resultariam em endereços ociosos.
2. Empresa com 500 hosts: 192.168.2.0/23 (máscara 255.255.254.0)
 - A máscara **255.255.254.0** permite 512 endereços, dos quais 510 são utilizáveis para hosts.
 - Com 500 hosts na empresa, essa sub-rede atende à necessidade com uma margem pequena para dispositivos adicionais, evitando o uso de uma máscara ainda maior, que geraria desperdício.
 - Uma máscara menor, como **/24** (255.255.255.0), seria insuficiente, pois oferece apenas 254 endereços utilizáveis.

Aqui estão os endereçamentos de cada empresa:

Empresa 1 (Máximo de 100 hosts):

Dispositivo	Endereço
Roteador principal	192.168.1.1/25 (Máscara 255.255.255.128)
Servidor com serviço DHCP	192.168.1.2/25 (Máscara 255.255.255.128)

Empresa 2 (Máximo de 500 hosts):

Dispositivo	Endereço
Roteador principal	192.168.2.1/23 (Máscara 255.255.254.0)
Servidor com serviço DHCP	192.168.2.2/23 (Máscara 255.255.254.0)

4. CONFIGURAÇÃO DE PROTOCOLOS E SERVIÇOS

Em se tratando de protocolos de rede, nesta ocasião teríamos 3 para focar:

- Protocolo DHCP, responsável por alocar endereços dinamicamente nas redes privadas empresariais.
- Protocolo NAT, responsável por atuar na tradução de endereços IP privados em endereços IP públicos, uma vez que endereços IP privadas são incapazes de serem publicados na internet.
- Protocolo OSPF, atuando no descobrimento de rotas menos “custosas” segundo o algoritmo de Dijkstra, responsável pelo processo principal ao escolher qual rota será a mais curta ou mais “barata” no tráfego de informações.

4.1 Protocolo DHCP

Nas redes empresarias era necessário que os hosts além de terem uma experiência mais transparente à configuração de suas máquinas, também não pudessem escolher endereços específicos da rede, para evitar problemas relacionados a conflitos. Para isto foi utilizado o protocolo DHCP, aonde alocamos previamente quais endereços deveriam ser atribuídos aos usuários de maneira dinâmica, como está explicitado na tabela abaixo.

Empresa	Default gateway	Servidor DNS	Endereço IP inicial	Máscara de sub-rede	Máximo de hosts
Empresa 1	192.168.1.1	190.190.190.2	192.168.1.3	255.255.255.128	110
Empresa 2	192.168.2.1	190.190.190.2	192.168.2.10	255.255.254.0	502

4.2 Protocolo NAT

Mesmo com as configurações da rede empresarial funcionando perfeitamente, ainda seria necessária a configuração tanto de rotas estáticas no roteador principal de cada empresa como a tradução dos endereços IPs privados para que os mesmos pudessem ser publicados na rede metropolitana. E para tal foi utilizado o protocolo NAT, que viria a ser o responsável por conseguirmos enviar pacotes da rede privada para a rede pública fora da empresa, então foi configurada uma porta como entrada e duas para saída já que os roteadores principais das empresas estão ligados em outros dois da rede metropolitana, roteadores estes que receberam uma rota estática aonde os endereços das redes privadas seriam redirecionados via tradução.

Por fins de organização, as interfaces das empresas que foram conectadas à rede metropolitana foram configuradas com IP's públicos diferentes do padrão adotado neste cenário, segue tabela com os endereçamentos das traduções:

Aparelho	Interface de entrada	Interface de saída 1	Interface de saída 2
Roteador principal da empresa 1	GigabitEthernet 2/0 192.168.1.1/25	GigabitEthernet0/0 200.200.200.1	GigabitEthernet1/0 200.200.200.5
Roteador principal empresa 2	GigabitEthernet2/0 192.168.2.1/23	GigabitEthernet0/0 201.201.201.1/30	GigabitEthernet1/0 201.201.201.5

4.3 Protocolo OSPF

Responsável por automatizar, simplificar e registrar rotas comuns na rede, o protocolo OSPF, atua na rede metropolitana como o coração do sistema, interligando as redes empresariais, o ambiente IOT e o servidor DNS. Em cada roteador da rede metropolitana as rotas OSPF foram registradas no backbone(área 0) simplificando assim a comunicação entre diferentes ambientes. O endereçamento utilizado no OSPF é o mesmo utilizado para a configuração da rede metropolitana, já que esta foi feita em cima deste protocolo.

5. REDUNCÂNCIA E ALTA DISPONIBILIDADE

Sendo um dos requisitos ativos do projeto, era necessário fazer com que as redes operassem em redundância mesmo com alguns roteadores falhando, tanto na rede metropolitana quanto nas redes empresariais.

Para tal foram feitas algumas configurações específicas.

- Nas redes metropolitanas todos os roteadores tiveram cada outro roteador cadastrado em uma rota via protocolo OSPF, para que assim o roteamento fosse dinâmico e intuitivo.
- Nas empresas os roteadores principais receberam configuração de prioridades em suas rotas estáticas para que assim quando uma das rotas falhasse a outra ainda atuaria como principal, desse jeito as duas entidades sempre teriam conexão com a internet

6. SERVIDORES DNS E WEB

Na rede metropolitana foi criada uma rede aparte destinada ao serviço DNS e aos servidores HTTP de cada empresa aonde seriam guardados suas páginas de index. A rede em questão possui o endereçamento 190.190.190.0/16 (Com máscara 255.255.0.0).

O servidor principal atua como DNS, sendo responsável pelo nomeamento de cada servidor web registrado no sistema, registrando seus respectivos domínios.

Já os servidores web atuam como host para as páginas index de apresentação de cada empresa.

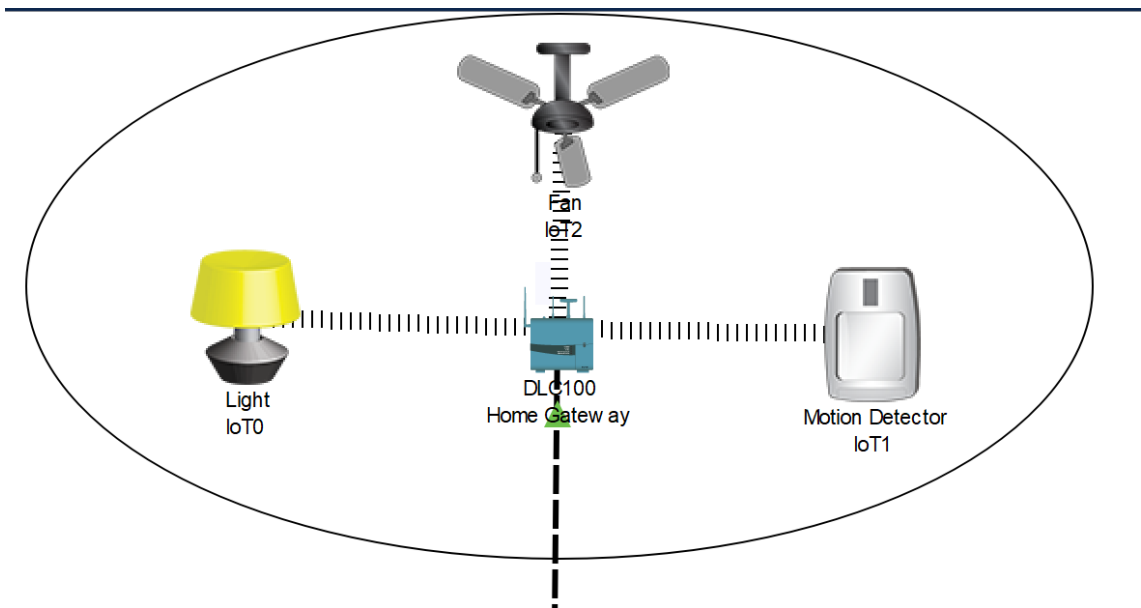
Segue tabela de endereçamentos:

Nome do servidor	Endereço IP	Máscara de sub-rede	Domínio
Servidor DNS	190.190.190.2	255.255.0.0	-----
Locadora Ariel Server	190.190.190.6	255.255.0.0	locadorariel.com
Lan House Manuelle	190.190.190.5	255.255.0.0	lanhousemanuelle.com

7. CENÁRIO DE IOT E ENERGIA ACESSÍVEL E LIMPA

Como requisito funcional também é necessário que o sistema tenha relação com as ODS's (11, 9 e 7), escolhemos a de número 7(ODS 7: Energia Acessível e Limpa), por motivo de que o packet tracer possui mais ferramentas com suporte a este cenário que aos demais.

No nosso cenário simulamos um ambiente residencial aonde controlamos o consumo de energia das lâmpadas e o funcionamento do ventilador via sensor de movimento de acordo com a presença ou ausência de atividade no recinto.



8. TESTES E VALIDAÇÃO

Após todas as etapas de construção, já seria possível que as redes estivessem se comunicando perfeitamente de maneira redundante sem alta latência ou falhas de comunicação

8.1 Testes de funcionalidades dos protocolos e serviços

Para teste dos protocolos foram feitos vários cortes de conexões em diferentes áreas da rede para que fossem testadas as funcionalidades de alocação dinâmica de endereços IP's nas empresas e também foram feitos vários cortes de conexão proposital na rede metropolitana para que fosse averiguado se o protocolo OSPF funcionaria corretamente ao realocar rotas dinamicamente. Também foram feitos testes de redundância para averiguar se as configurações gerais geravam o comportamento esperado tanto nos roteadores quanto no protocolo NAT.

Após essa bateria de testes, o sistema continuava resiliente, dinâmico e redundante, ou seja, todas as configurações relacionadas foram feitas com sucesso.

8.2 Verificação de comunicação entre hospedeiros

Para averiguar se os hosts estavam se comunicando entre si perfeitamente, foram realizados testes de ping entre hosts da empresa e roteadores da rede metropolitana. Após vários testes, vindo de diferentes hosts e roteadores, foi constatado que tanto as empresas, quanto os hosts conseguem se comunicar sem latência e sem timeout.

9. CONCLUSÃO

Este projeto apresentou uma abordagem abrangente para o design, configuração e implementação de uma infraestrutura de rede complexa, integrada com serviços de conectividade entre múltiplas empresas, comunicação inter-redes e suporte à Internet das Coisas (IoT). Durante sua execução, exploramos a importância de conceitos como roteamento dinâmico com OSPF, NAT para tradução de endereços, e a implementação de serviços críticos como DNS e HTTP em um ambiente corporativo.

Entre os pontos altos do projeto, destacam-se:

1. **Planejamento de Rede Estruturado:**

A escolha de sub-redes bem definidas e máscaras apropriadas foi crucial para atender às necessidades de cada empresa, garantindo escalabilidade e evitando desperdício de endereços IP.

2. **Integração de Roteamento e Tradução de Endereços:**

Configuramos o OSPF para facilitar a comunicação entre as redes, enquanto o NAT assegurou o acesso à Internet sem comprometer a segurança ou a estabilidade do ambiente local.

3. **Serviços de Rede Essenciais:**

A implementação de servidores dedicados para DNS e HTTP na rede metropolitana não apenas reforçou a centralização dos serviços, mas também garantiu que as empresas mantivessem independência operacional em seus respectivos servidores.

4. **Suporte a IoT:**

A inclusão de uma rede IoT básica mostrou como a tecnologia pode ser incorporada para automação e eficiência operacional, alinhando-se às ODS (Objetivos de Desenvolvimento Sustentável) da ONU, como cidades inteligentes e energia acessível.

5. **Resiliência e Redundância:**

Foram configuradas rotas de failover para garantir que, mesmo em casos de falhas de conectividade, o acesso aos serviços fosse mantido com o mínimo de impacto.

Este trabalho evidenciou o papel fundamental de uma infraestrutura de TI robusta no suporte às operações corporativas modernas. Ao integrar diferentes tecnologias e metodologias, conseguimos não apenas atender às necessidades de comunicação e serviços das empresas, mas também criar um ambiente preparado para crescimento futuro e desafios tecnológicos. A experiência adquirida neste projeto reforça a importância de planejamento detalhado, execução precisa e revisão contínua para garantir o sucesso de implementações em redes complexas.