INSTITUTO INFNET
ESCOLA SUPERIOR DE TECNOLOGIA

RDC – Graduação em Redes de Computadores

Projeto de Bloco: Infraestrutura Lógica de Redes

Teste de Performance

Aluno: Pedro Cremonezi Cardoso Andrioti Alves
Email: pedro.alves@al.infnet.edu.br
Professora: Natália Oliveira

Data de Entrega: 27 de Junho de 2021

Sumário

1.1 Sobre a HCloe

A HCloe é uma Clínica de oftalmologia, fundada a mais de 30 anos e conta com 4 clínicas localizadas no estado de São Paulo.
Seu alto nível de investimentos com equipamentos, infraestrutura, treinamentos e serviços geram uma grande qualidade no atendimento de seus pacientes, resultando em clínicas com muito movimento e satisfação por parte de seus pacientes.
Para atender os requisitos dos projetos foi considerado apenas 3 unidades.

1.2 Objetivo do Projeto

Este Projeto tem como objetivo principal colocar em prática todos os conceitos, boas práticas e aplicações que vimos durante as aulas e na realização das outras atividades em um cenário real.

Para concluir esse projeto foi necessário desde os conhecimentos básicos como o protocolo IPv4 até conceitos de roteamento, protocolos, alta disponibilidade e segurança dentro da infra estrutura de redes.

É importante ressaltar que as unidades foram usadas apenas como uma referência, desde plantas até quantidade de dispositivos.

2. Cronograma

O cronograma foi uma das partes essenciais para a realização do projeto, pois foi aonde delimitamos marcos para entregas e conclusões de atividades.

Ele foi dividido em 5 Etapas para facilitar a visualização e realização de cada etapa, desde o levantamento de informações, configurações mais detalhadas até a apresentação do projeto em si.

	JAN	FEV	MAR	ABR	MAI	JUN
ETAPA 1						
Escolha das Unidades	Feito					
Primeiro contato com as Unidades	Feito					
Visita técnica	Feito					
Conversa com a Área de TI responsável	Feito					
Levantamento de Requisitos	Feito					
ETAPA 2						
Mapeamento da Estrutura Física		Feito				
Mapeamento da Planta Baixa		Feito				
Desenho do Diagrama Físico da Rede		Feito				
ETAPA 3						
Mapeamento da Estrutura Lógica da Rede			Feito			
Criação da Tabela de endereçamento IPv4			Feito			
Criação da Tabela de VLANs			Feito			
Construção do Diagrama Lógico			Feito			
ETAPA 4						
Construção da Topologia Inicial no Packet Tracer			Feito			
Configuração dos equipamentos				Feito		
Configuração de Protocolos				Feito		
Configuração de ACLs				Feito		
Configuração de NAT				Feito		
Configuração do Servidor					Feito	
Configuração de Conexão Entre as Unidades					Feito	
Configuração dos Switches					Feito	
Configuração dos Roteadores					Feito	
Configuração dos Firewalls					Feito	
ETAPA 5						
Escolha de equipamentos						Feito
Precificação do Projeto						Feito
Apresentação do Projeto						Feito

3. Sobre as Unidades

As três clínicas que iremos trabalhar estão localizadas na região Oeste, Leste e Sul, são clínicas localizadas em prédios comerciais que mantém sua configuração de planta baixa a mesma devido a regras de padronizações que existem.

As unidades contam com 5 Salas para atendimento, 3 Salas de espera, um espaço de funcionários, 2 banheiros, uma ilha com a recepção e uma sala de documentos.

3.1 Unidade Perdizes

A unidade de Perdizes é uma das mais novas foi inaugurada em 2019.

- Endereço: Av. Marquês de São Vicente, 2219, 17 - º andar, sala 1703 - Perdizes, São Paulo - SP, 05036-040
- Central de Atêndimento: (11) 3124-0999
- Horário de funcionamento: Segunda à Sexta das 8:00 às 18:00
  Sábado das 8:00 às 12:00

3.2 Unidade Tatuapé

A unidade do Tatuapé foi a primeira unidade das 3.

- Endereço: Rua Emílio Mallet, 317 – 7º Andar - Tatuapé, São Paulo – SP, 03320-000

- Central de Atêndimento: (11) 3124-0999

- Horário de funcionamento: Segunda à Sexta das 8:00 às 20:00
  Sábado das 8:00 às 12:00

3.3 Unidade Bela Vista

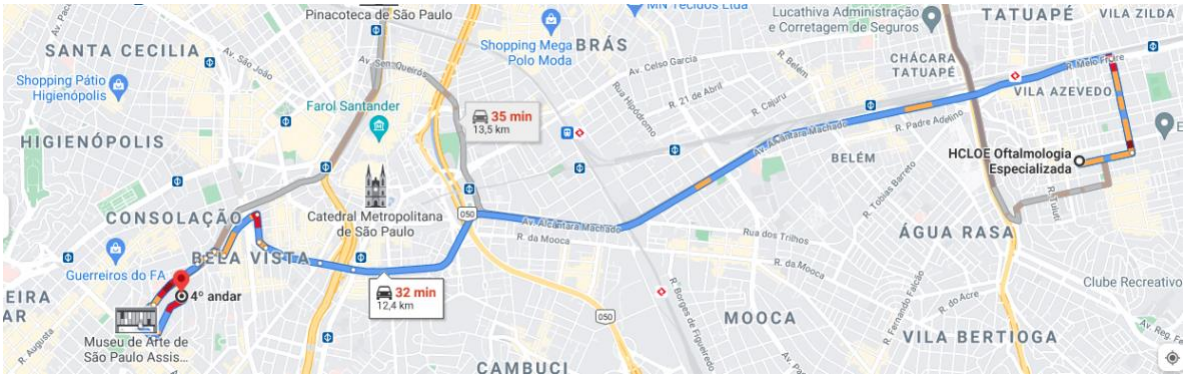
A unidade da Bela Vista hoje é que conta com a maior movimentação entre as 3, e foi a segunda unidade a ser construída.

- Endereço: Rua Itapeva, 240 – 4º Andar - Bela Vista, São Paulo – SP, 01332-000
- Central de Atêndimento: (11) 3124-0999
- Horário de funcionamento: Segunda à Sexta das 8:00 às 21:00
  Sábado das 8:00 às 12:00

É importante ressaltar que as unidades foram usadas apenas como uma referência, desde plantas até quantidade de dispositivos.

4. Rotas entre as Unidades

4.1 Tatuapé - Bela Vista

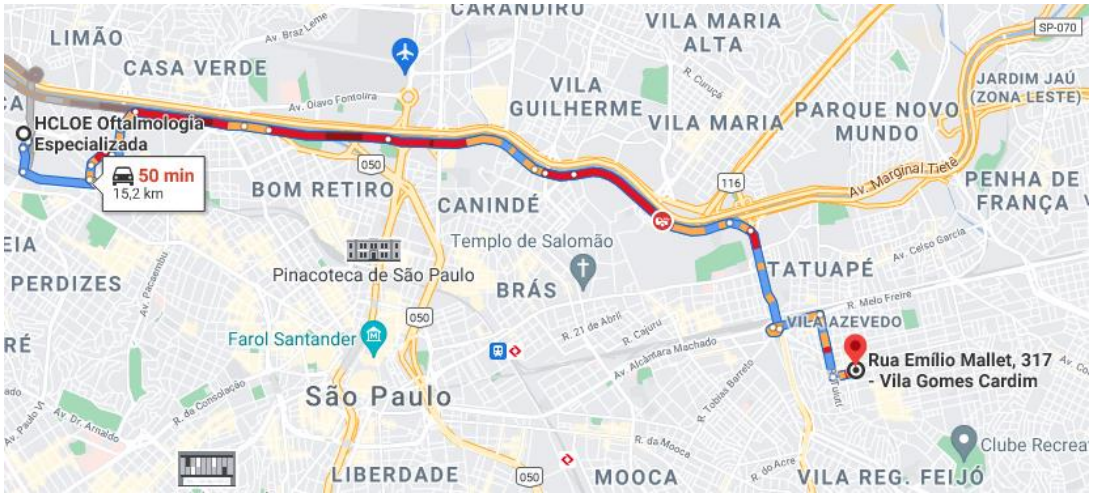


A imagem acima representa a distância entre as unidades do Tatuapé até a unidade da Bela Vista, uma distância de 12,9 Km e um tempo em média de 33 minutos, dependendo do horário.

4.2 Bela Vista – Perdizes

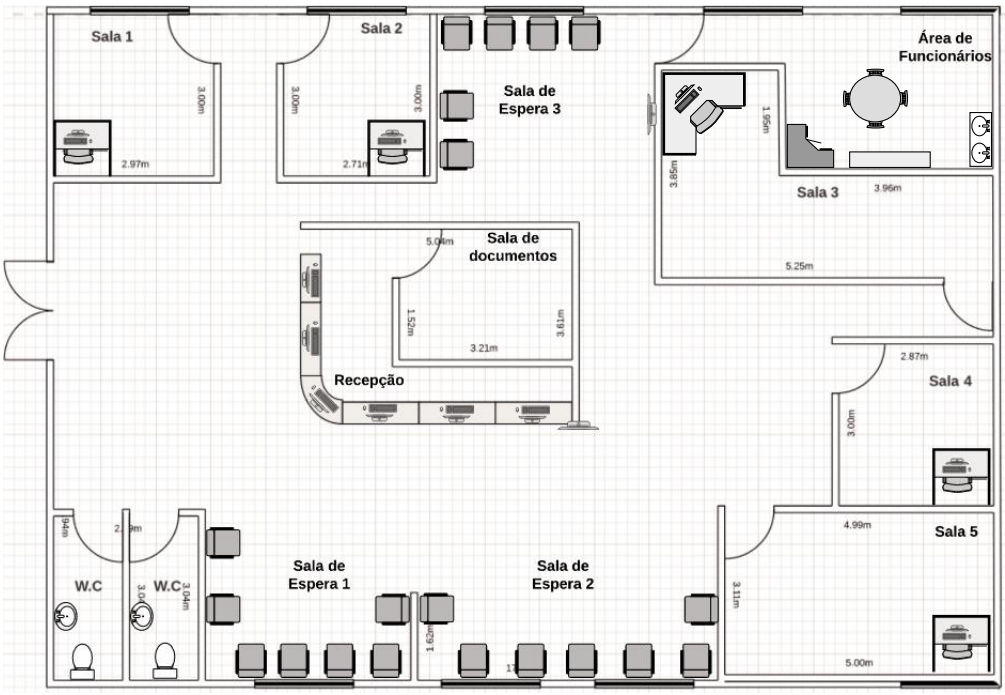
A imagem acima representa a distância entre as unidades da Bela Vista até a unidade de Perdizes, uma distância de em média 11,1 Km e um tempo em média de 36 minutos, dependendo do horário.

4.3 Perdizes – Tatuapé



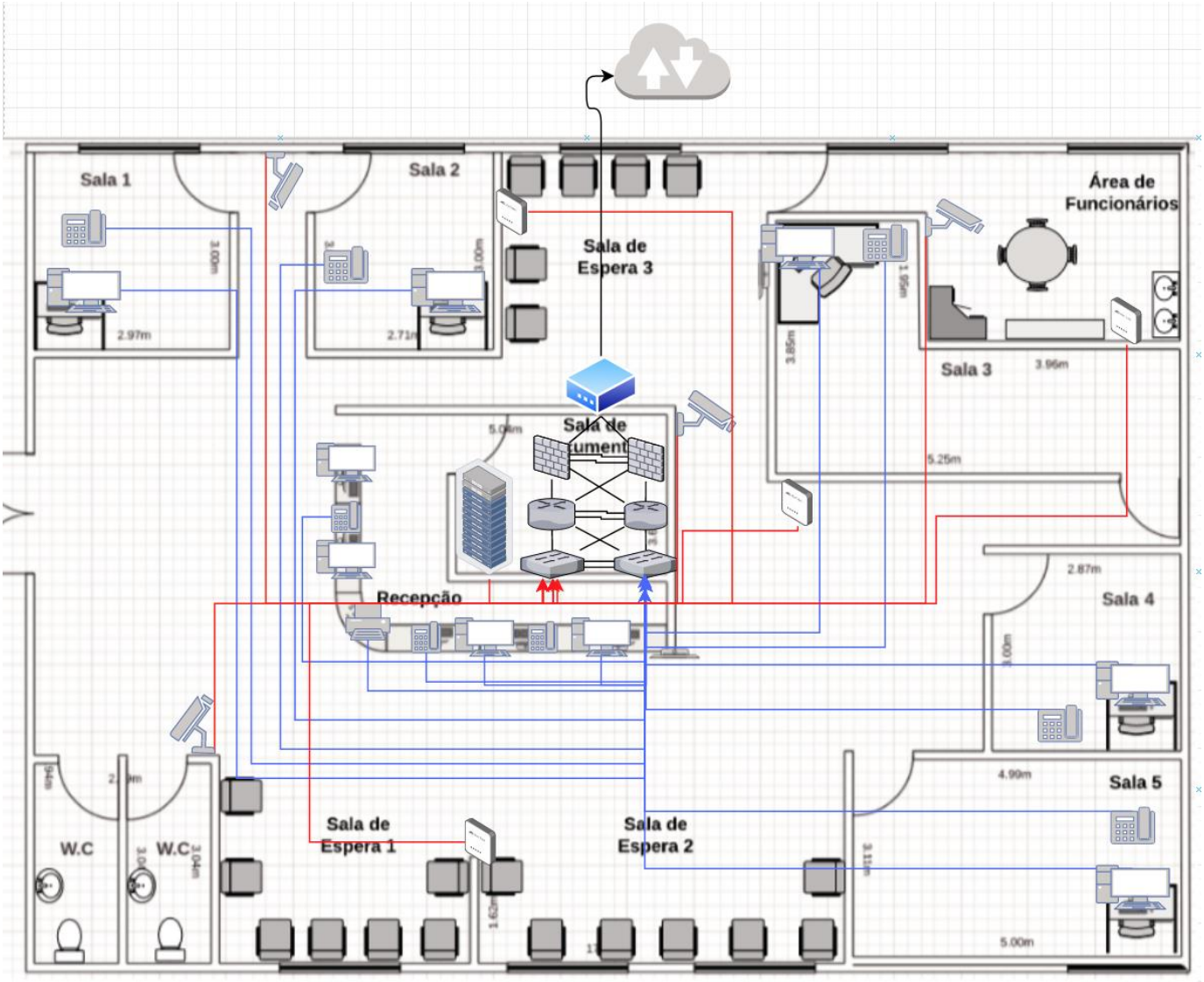
A imagem acima representa a distância entre as unidades de Perdizes até a unidade do Tatuapé, uma distância de 15,2 Km e um tempo em média de 50 minutos, dependendo do horário.

5. Planta Baixa



Essa é uma representação da planta baixa, onde vemos a divisão das salas dentro do consultório, também é possível ver aonde estão localizadas as máquinas que utilizaram a rede, essa planta é padronizada e vemos essa mesma distribuição para as 3 unidades.

6. Topologia Física



O acesso a internet é feito através de dois links de internet e o controle de acesso é feito através de um firewall;

O Firewall é responsável pela comunicação entre as filiais e recebe os links para acesso a internet, além de proteger a rede;

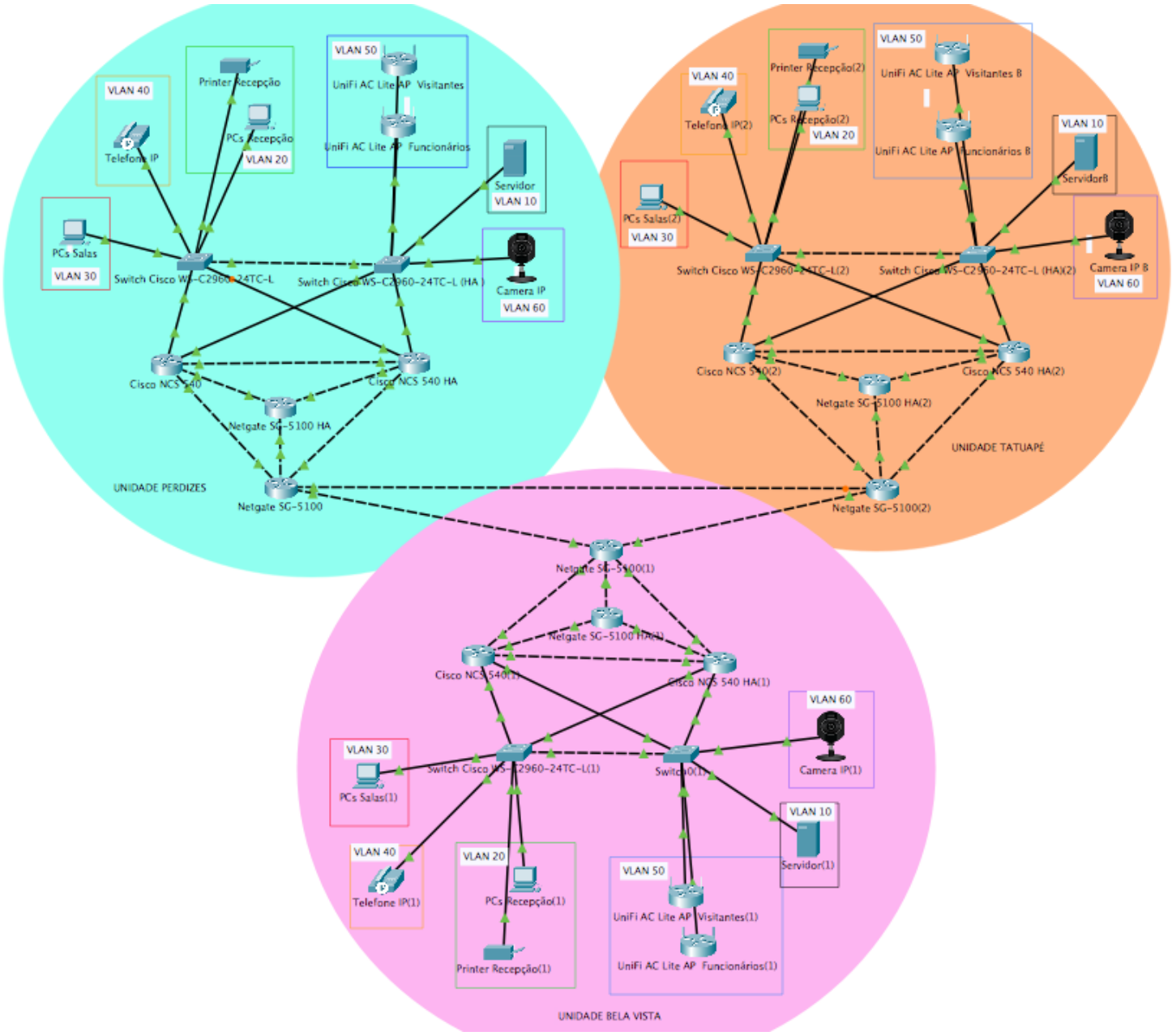
O Roteador é responsável por fornecem acesso a rede para para os dispositivos e equipamentos;

O Switch conecta todas as áreas do consultório, PCs das salas, PCs da recepção, e a impressora da unidade, servidores, telefones, câmeras e o access point, tudo divido em diferentes VLANs e sub-redes;

O Access point é responsável por fornecer acesso a rede sem fio para funcionários e visitantes.

É importante ressaltar que as unidades foram usadas apenas como uma referência, desde plantas até quantidade de dispositivos.

7. Modelo de Simulação e Teste



O diagrama acima representa a topologia lógica do projeto, onde temos o funcionamento em si, e como os equipamentos estão dispostos, configurados e interligados dentro da rede, vemos também a conexão entre as unidades a partir do firewall na borda da rede.

8. Funcionamento da rede

A rede tem como principal equipamento o roteador, que é responsável por separar as sub redes, fazer a comunicação entre elas e estabelecer a comunicação da rede interna com a internet, todo o fluxo de dados na comunicação da rede passa pelo roteador, desde um teste de ping entre os PCs até uma requisição na internet.

Temos conectados no roteador o firewall que filtra todo dado e conteúdo que entra que sai da rede, método fundamental de segurança e também temos o switch conectado.

O Firewall é uma das diversas ferramentas que temos para proteção da nossa rede, através de regras que podem ser configuradas é possível filtrar o conteúdo e fluxo de dados da rede, além de proteger contra ataques hackers, e o modelo de firewall do projeto conta com um recurso chamado IPS/IDS umas das mais eficazes tecnologias para reconhecimento de ameaças e ataques.

Todo dado que sai para internet ou que entra na rede é filtrado pelo firewall, assim agregando mais segurança para a rede.

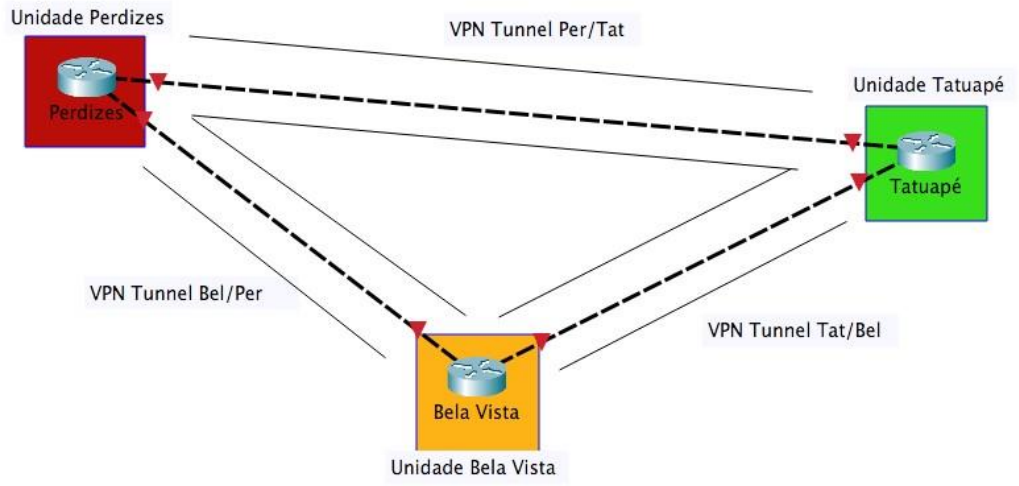
O switch tem a função de ligar todos os equipamentos da rede, desde a impressora, PCs, Telefones IP, câmeras, os access points e o servidor, ele funciona como uma expansão de portas a mais para o roteador, mas que pode gerenciar o tráfego de dados e pacotes, melhorando a gestão da rede por inteira.

Access Points são responsáveis por fazer a conexão dos dispositivos que se conectam pela rede sem fio, pelo wi-fi, todos os dados são encaminhados para o AP, dele passa ara o switch, do switch para o roteador e o firewall até chegar na conexão com a internet.

A Rede tem um funcionamento simples, porém eficaz, é uma rede pequena e esse modelo será replicado para as demais unidades, já que por norma interna os equipamentos e infraestrutura devem ser padronizados da mesma forma que a planta baixa do local.

9. Sobre a Rede

9.1 Representação da VPN



A representação da VPN foi feita no Packet Tracer a partir de diversas referencias, nele vimos a conexão dos tuneis de conexão entre as unidades. No Packet Tracer não temos a representação de um firewall, que será responsável pela VPN e pelas listas de controle de acesso.

9.2 Velocidade dos Link de Internet

As clínicas contam com 2 links de internet para ter alta disponibilidade, caso um link fique indisponível o outro assume como principal e as clínicas não perdem a conexão com a internet. Os dois links são da Vivo, um é Vivo fibra de 100MB e o outro é um Vivo ADSL de 10MB.

10. Endereçamento IP

10.1 O que é o IPv4

O IPv4 é um protocolo de endereçamento e comunicação que utilizamos hoje na maioria dos dispositivos que temos, smartphones, computadores, televisões e outros dispositivos que se conectam na rede de internet.

É um dos principais protocolos baseados em métodos de interconexão de rede e foi a primeira versão usada no lançamento da ARPANET, a antecessora da internet.

10.2 Motivo da escolha do IPv4

A escolha de utilizar IPv4 nesse projeto, é devida a uma rede pequena, com poucas sub-redes e pouca quantidade de usuários, outro motivo é a simplicidade de configurar os endereços nas máquinas, seja via DHCP ou manualmente, mas nada impede a implementação de endereços IPv6 futuramente.

10.3 Cálculos

Primeiro foi decidido o endereço de rede, como padrão para redes LAN comerciais foi escolhido o endereço 10.0.0.0/24, após isso foi decidido quantas sub-redes deveriam existir para a divisão dos setores dentro das clínicas.

Foi calculado a quantidade de bits que seriam dedicados à rede e quantos seriam dedicados à hosts, chegamos a um prefixo /24, utilizando uma rede convencional para distribuir a rede e organizar de acordo com a unidade e as VLANs.

O endereçamento varia de acordo com a unidade e a VLAN, e foi configurado da seguinte forma, o número da unidade é representado pelo segundo octeto do IP, ou seja, a unidade de Perdizes é a primeira e o endereçamento da rede ficou 10.1.0.0/24, a segunda unidade na ordem do endereçamento é a unidade do Tatuapé e seu endereço de rede ficou 10.2.0.0/24 e por fim a unidade da Bela Vista tem seu endereço 10.3.0.0/24.

Logo após temos os endereços das VLANs que são representadas no terceiro octeto do endereço, apesar de termos um grande range de IPs por sub-rede, isso não é um problema já que esses são todos IPs privados e não existem um desperdício já que não estamos usando IPs público.

Teremos um total de 254 endereços para cria VLANs e para 254 endereços para hosts dentro de cada VLAN.

Unidade	Endereço
PERDIZES	10.1.0.0 /24
TATUAPÉ	10.2.0.0 /24
BELA VISTA	10.3.0.0 /24

11. Tabela de Endereçamento das Unidades

Unidade	PERDIZES
Endereço da Rede	10.1.0.0 /24
Máscara da Rede	255.255.255.0

Divisão	Sub-rede	Hosts	Broadcast
Servidores	10.1.1.0/24	10.1.1.1->10.1.1.254	10.1.1.255
Recepção	10.1.2.0/24	10.1.2.1->10.1.2.254	10.1.2.255
Salas	10.1.3.0/24	10.1.3.1->10.1.3.254	10.1.3.255
Telefones	10.1.4.0/24	10.1.4.1->10.1.4.254	10.1.4.255
Wifi	10.1.5.0/24	10.1.5.1->10.1.5.254	10.1.5.255
Câmeras	10.1.6.0/24	10.1.6.1->10.1.6.254	10.1.6.255

Unidade	TATUAPÉ
Endereço da Rede	10.2.0.0 /24
Máscara da Rede	255.255.255.0

Divisão	Sub-rede	Hosts	Broadcast
Servidores	10.2.1.0/24	10.2.1.1->10.2.1.254	10.2.1.255
Recepção	10.2.2.0/24	10.2.2.1->10.2.2.254	10.2.2.255
Salas	10.2.3.0/24	10.2.3.1->10.2.3.254	10.2.3.255
Telefones	10.2.4.0/24	10.2.4.1->10.2.4.254	10.2.4.255
Wifi	10.2.5.0/24	10.2.5.1->10.2.5.254	10.2.5.255
Câmeras	10.2.6.0/24	10.2.6.1->10.2.6.254	10.2.6.255

Unidade	BELA VISTA
Endereço da Rede	10.3.0.0 /24
Máscara da Rede	255.255.255.0

Divisão	Sub-rede	Hosts	Broadcast
Servidores	10.3.1.0/24	10.3.1.1->10.3.1.254	10.3.1.255
Recepção	10.3.2.0/24	10.3.2.1->10.3.2.254	10.3.2.255
Salas	10.3.3.0/24	10.3.3.1->10.3.3.254	10.3.3.255
Telefones	10.3.4.0/24	10.3.4.1->10.3.4.254	10.3.4.255
Wifi	10.3.5.0/24	10.3.5.1->10.3.5.254	10.3.5.255
Câmeras	10.3.6.0/24	10.3.6.1->10.3.6.254	10.3.6.255

12. Configuração dos Equipamentos

12.1 Configuração dos Firewalls

Os firewalls são os equipamentos responsáveis pela segurança da rede, através das Listas de Controle de Acesso, é permitido ou negado o acesso de um determinado endereço na rede, além da funcionalidade de filtrar a rede, ele também é responsável pela conexão site-to-site entre as unidades, através de VPN.

Eles estão ligados e configurados para obter uma alta disponibilidade e tolerância a falhas dentro da rede. Foi configurado também todas boas práticas de segurança dentro do roteador, desde habilitar senhas para o acesso, até colocar em estado shutdown as interfaces que não estão sendo utilizadas.

12.2 Configuração dos Roteadores

Os roteadores são responsáveis por fazer a conexão entre as VLANs e garantir comunicação de todos os equipamentos da rede, configurados com o protocolo HRSP para obter uma alta disponibilidade e tolerância a falhas dentro da rede.

Foi configurado também todas boas práticas de segurança dentro do roteador, desde habilitar senhas para o acesso, até colocar em estado shutdown as interfaces que não estão sendo utilizadas.

12.3 Configuração dos Switches

Os Switches estão as configurações das VLANs as quais encaminham para os roteadores, eles também estão ligados e configurados para obter uma alta disponibilidade e tolerância a falhas dentro da rede.

Foi configurado também todas boas práticas de segurança dentro do switch, desde habilitar senhas para o acesso, até colocar em estado shutdown as interfaces que não estão sendo utilizadas.

12.4 Configuração dos Computadores

A configuração dos computadores é baseada no protocolo DHCP, o qual funciona a partir de um roteador que distribui o endereçamento IP a partir do Range configurado e dos intervalos de sub rede.

Os computadores estão divididos para a VLAN 20, Recepção, a qual aceitam endereços a partir de 10.X.2.1, e a VLAN 30, Salas, a qual aceitam endereços a partir de 10.X.3.1, variando a unidade que estão.

13. Configurações Básicas

13.1 Firewalls

- **Hostname** – Para os nomes dos Firewalls foi decidido 1 sendo o principal e o 2 para o secundário, e foram divididos por unidades.

  Na unidade Perdizes temos os F1P, e o F2P;

  Na unidade Tatuapé temos o F1T, e o F2T;

  Na unidade Bela Vista temos o F1B e o F2B.
- **Enable secret** – A configuração enable secret é utilizado para proteção do equipamento contra acesso de pessoas que não são autorizadas e para isso é configurado uma senha com esse comando para que nem todos possam acessa-lo.
- **Banner Motd** – Assa configuração faz a criação de banner logo no início da tela de console do equipamento e nele esta escrito:

  #Acesso Somente a Pessoas Autorizadas#
- **Interface description** – A configuração de descrição de interfaces faz parte das boas práticas dentro de uma infraestrutura facilitando um possível troubleshooting futuro.
- **Line Console** – Mais um configuração de segurança aonde é colocada uma senha para o acesso ao modo de configuração global.
- **Service password-encryption** – Configuração que criptografa as senhas para que até mesmo tendo acesso total não seja possível ver a palavra-chave.
- **Exec-Timeout** – Configuração na qual delimitamos um tempo de inatividade dentro da console, para que o usuário que estiver acessando não corra riscos de deixar aberto a interface para o acesso de todos, então caso o usuário não faça nenhuma interação na console em 45 segundos, a sessão é encerrada automaticamente, exigindo as credenciais de acesso para login novamente.

13.2 Roteadores

- **Hostname** – Para os nomes dos Firewalls foi decidido 1 sendo o principal e o 2 para o secundário, e foram divididos por unidades.

  Na unidade Perdizes temos os R1P, e o R2P;

  Na unidade Tatuapé temos o R1T, e o R2T;

  Na unidade Bela Vista temos o R1B e o R2B.
- **Enable secret** – A configuração enable secret é utilizado para proteção do equipamento contra acesso de pessoas que não são autorizadas e para isso é configurado uma senha com esse comando para que nem todos possam acessa-lo.
- **Banner Motd** – Assa configuração faz a criação de banner logo no início da tela de console do equipamento e nele esta escrito:

  #Acesso Somente a Pessoas Autorizadas#
- **Interface description** – A configuração de descrição de interfaces faz parte das boas práticas dentro de uma infraestrutura facilitando um possível troubleshooting futuro.
- **Line Console** – Mais um configuração de segurança aonde é colocada uma senha para o acesso ao modo de configuração global.
- **Service password-encryption** – Configuração que criptografa as senhas para que até mesmo tendo acesso total não seja possível ver a palavra-chave.
- **Exec-Timeout** – Configuração na qual delimitamos um tempo de inatividade dentro da console, para que o usuário que estiver acessando não corra riscos de deixar aberto a interface para o acesso de todos, então caso o usuário não faça nenhuma interação na console em 45 segundos, a sessão é encerrada automaticamente, exigindo as credenciais de acesso para login novamente.

13.3 Switches

- **Hostname** – Para os nomes dos Firewalls foi decidido 1 sendo o principal e o 2 para o secundário, e foram divididos por unidades.

  Na unidade Perdizes temos os S1P, e o S2P;

  Na unidade Tatuapé temos o S1T, e o S2T;

  Na unidade Bela Vista temos o S1B e o S2B.
- **Enable secret** – A configuração enable secret é utilizado para proteção do equipamento contra acesso de pessoas que não são autorizadas e para isso é configurado uma senha com esse comando para que nem todos possam acessa-lo.
- **Banner Motd** – Assa configuração faz a criação de banner logo no início da tela de console do equipamento e nele esta escrito:

  #Acesso Somente a Pessoas Autorizadas#
- **Interface description** – A configuração de descrição de interfaces faz parte das boas práticas dentro de uma infraestrutura facilitando um possível troubleshooting futuro.
- **Line Console** – Mais um configuração de segurança aonde é colocada uma senha para o acesso ao modo de configuração global.
- **Service password-encryption** – Configuração que criptografa as senhas para que até mesmo tendo acesso total não seja possível ver a palavra-chave.
- **Exec-Timeout** – Configuração na qual delimitamos um tempo de inatividade dentro da console, para que o usuário que estiver acessando não corra riscos de deixar aberto a interface para o acesso de todos, então caso o usuário não faça nenhuma interação na console em 45 segundos, a sessão é encerrada automaticamente, exigindo as credenciais de acesso para login novamente.

14. Configurações básicas na Console

As configurações a seguir são referentes aos equipamentos da Unidade Perdizes, mas foram aplicadas as mesmas configurações para os demais equipamentos das outras unidades.

14.1 Firewalls

```
F1P#sh r
Building configuration...

Current configuration : 2535 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname F1P
!
!
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
banner motd ^CAcesso Somente a Pessoas Autorizadas^C
!
!
!
!
!
line con 0
 exec-timeout 45 0
 password 7 0822404F1A0A
 login
!
line aux 0
!
line vty 0 4
 exec-timeout 45 0
 password 7 0822404F1A0A
 login
line vty 5 15
 exec-timeout 45 0
 password 7 0822404F1A0A
 login
!
!
!
end
```

```
F2P#sh r
Building configuration...

Current configuration : 2535 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname F2P
!
!
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
banner motd ^CAcesso Somente a Pessoas Autorizadas^C
!
!
!
!
!
line con 0
 exec-timeout 45 0
 password 7 0822404F1A0A
 login
!
line aux 0
!
line vty 0 4
 exec-timeout 45 0
 password 7 0822404F1A0A
 login
line vty 5 15
 exec-timeout 45 0
 password 7 0822404F1A0A
 login
!
!
!
end
```

14.2 Roteadores

```
R1P#sh r
Building configuration...

Current configuration : 2158 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R1P
!
!
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
banner motd ^CAcesso Somente a Pessoas Autorizadas^C
!
!
!
!
!
line con 0
 exec-timeout 45 0
 password 7 0822404F1A0A
 login
!
line aux 0
!
line vty 0 4
 exec-timeout 45 0
 password 7 0822404F1A0A
 login
line vty 5 15
 exec-timeout 45 0
 password 7 0822404F1A0A
 login
!
!
!
end
```

```
R2P#sh r
Building configuration...

Current configuration : 2158 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R2P
!
!
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
banner motd ^CAcesso Somente a Pessoas Autorizadas^C
!
!
!
!
!
line con 0
 exec-timeout 45 0
 password 7 0822404F1A0A
 login
!
line aux 0
!
line vty 0 4
 exec-timeout 45 0
 password 7 0822404F1A0A
 login
line vty 5 15
 exec-timeout 45 0
 password 7 0822404F1A0A
 login
!
!
!
end
```

14.3 Switches

```
S1P#sh r
Building configuration...

Current configuration : 2103 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname S1P
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
banner motd ^CAcesso Somente a Pessoas Autorizadas^C
!
!
!
line con 0
 password 7 0822404F1A0A
 login
 exec-timeout 45 0
!
line vty 0 4
 exec-timeout 45 0
 password 7 0822404F1A0A
 login
line vty 5 15
 exec-timeout 45 0
 password 7 0822404F1A0A
 login
!
!
!
!
end
```

```
S2P#sh r
Building configuration...

Current configuration : 2103 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname S2P
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
banner motd ^CAcesso Somente a Pessoas Autorizadas^C
!
!
!
line con 0
 password 7 0822404F1A0A
 login
 exec-timeout 45 0
!
line vty 0 4
 exec-timeout 45 0
 password 7 0822404F1A0A
 login
line vty 5 15
 exec-timeout 45 0
 password 7 0822404F1A0A
 login
!
!
!
!
end
```

15. Lista de Controle de Acesso

As Listas de Controle de Acesso ou, *Access Control List (ACL),* são as listas que verificam o que e quem acessa a rede, seja através de um IP ou de um nome, elas têm um papel fundamental na segurança da rede pois é nela que são colocadas as regras de acesso a rede, permitindo ou bloqueando os acessos dependendo das regras.

15.1 IPs Permitidos

Como é o Firewall quem faz a conexão das VPNs e é ele quem recebe os links de internet a lista de controle é aplicada nele. Na lista de permissão foram incluídos os IPs dos Links de internet e os IPs dos outros Firewalls das unidades.

Cada unidade terá uma lista própria de acesso, devido ao endereçamento mudar a lista de controle também é alterada de acordo com a unidade.

15.2 IPs Negados

Todos os nomes e IPs que não forem os IPs das unidades e dos links de internet serão bloqueados, incluindo alguns nomes de sites que passam pelo processo de DNS para acesso a internet.

Firewall(config)#access-list 1 deny any

Esse comando bloqueia qualquer endereço ou IP que tente acessar a rede, a não ser os que estão na lista de permissão.

O Firewall escolhido para esse projeto apresenta 6 interfaces para conexão, foi necessárias apenas 5 interfaces, um ficara no estado Shutdown, enquanto nas outras, serão aplicadas a ACL com as regras de acesso e todas serão configuradas como Inbound rules, para que todos os *request* de ICMP e outros protocolos vindo de outras redes não tenham exitô.

15.3 Unidade Perdizes

Firewall(config)#access-list 1 permit host 50.223.20.10
Firewall(config)#access-list 1 permit host 50.223.20.11
Firewall(config)#access-list 1 permit host 172.30.30.20
Firewall(config)#access-list 1 permit host 172.30.30.30
Firewall(config)#access-list 1 permit host 200.10.1.1
Firewall(config)#access-list 1 deny any

Endereço	Tipo	Origem
50.223.20.10	Link	Internet
50.223.20.11	Link	Internet
172.30.30.20	VPN	Unidade Tatuapé
172.30.30.30	VPN	Unidade Bela Vista
200.10.1.1	NAT	Sub-redes

Configuração no dispositivo

```
!
access-list 1 permit host 50.223.20.10
access-list 1 permit host 50.223.20.11
access-list 1 permit host 172.30.30.20
access-list 1 permit host 172.30.30.30
access-list 1 permit host 200.10.1.1
access-list 1 deny any
!
```

15.4 Unidade Tatuapé

Firewall(config)#access-list 1 permit host 50.223.20.20
Firewall(config)#access-list 1 permit host 50.223.20.21
Firewall(config)#access-list 1 permit host 172.30.30.10
Firewall(config)#access-list 1 permit host 172.30.30.30
Firewall(config)#access-list 1 permit host 200.10.2.1
Firewall(config)#access-list 1 deny any

Endereço	Tipo	Origem
50.223.20.20	Link	Internet
50.223.20.21	Link	Internet
172.30.30.10	VPN	Unidade Perdizes
172.30.30.30	VPN	Unidade Bela Vista
200.10.2.11	NAT	Sub-redes

Configuração no dispositivo

```
!
access-list 1 permit host 50.223.20.20
access-list 1 permit host 50.223.20.21
access-list 1 permit host 172.30.30.10
access-list 1 permit host 172.30.30.30
access-list 1 permit host 200.10.2.1
access-list 1 deny any
!
```

15.5 Unidade Bela Vista

Firewall(config)#access-list 1 permit host 50.223.20.30
Firewall(config)#access-list 1 permit host 50.223.20.31
Firewall(config)#access-list 1 permit host 172.30.30.10
Firewall(config)#access-list 1 permit host 172.30.30.20
Firewall(config)#access-list 1 permit host 200.10.3.1
Firewall(config)#access-list 1 deny any

Endereço	Tipo	Origem
50.223.20.30	Link	Internet
50.223.20.31	Link	Internet
172.30.30.10	VPN	Unidade Perdizes
172.30.30.20	VPN	Unidade Tatuapé
200.10.3.10	NAT	Sub-redes

Configuração no dispositivo

```
!
access-list 1 permit host 50.223.20.30
access-list 1 permit host 50.223.20.31
access-list 1 permit host 172.30.30.10
access-list 1 permit host 172.30.30.20
access-list 1 permit host 200.10.3.1
access-list 1 deny any
!
```

16. Serviço DHCP

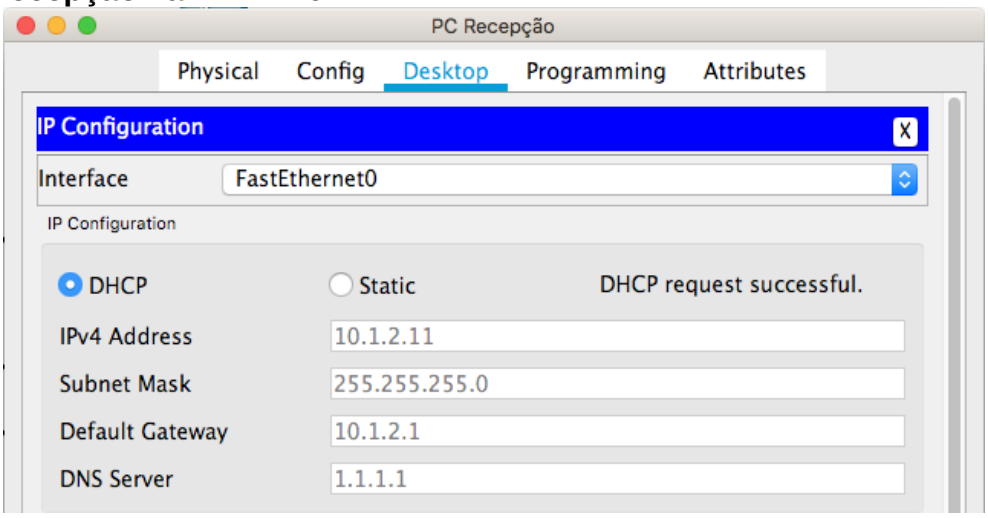
O roteador foi escolhido para distribuir os endereços DHCPs, foi decidido o range de IP que o rotador iria distribuir de acordo com a VLAN e a sub-rede que esse dispositivo se encontra, além disso foi criado regras para determinados IPs que seriam estáticos na rede assim não ocorreria problema na hora da distribuição.

A distribuição de IPs pelo DHCP é muito útil para grandes redes onde temos milhares de máquinas que precisar receber um certo IP para ter conexão a rede sem precisar adicionar um IP por vez.

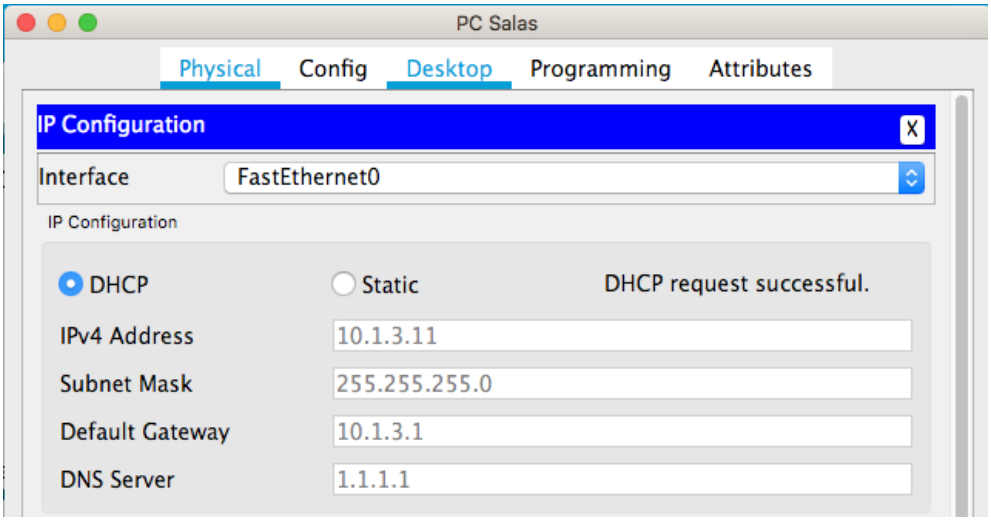
Temos um range de 10 endereços estáticos para que possam ser implementados em situações que exijam endereços fixos.

16.1 Configuração nos PCs

PCs da Recepção na VLAN 20



Pcs das Salas na VLAN 30



16.2 Configuração DHCP nos roteadores

Roteador da Unidade Perdizes

```
hostname R1P
!
!
!
!
ip dhcp excluded-address 10.1.1.1 10.1.1.10
ip dhcp excluded-address 10.1.2.1 10.1.2.10
ip dhcp excluded-address 10.1.3.1 10.1.3.10
ip dhcp excluded-address 10.1.4.1 10.1.4.10
ip dhcp excluded-address 10.1.5.1 10.1.5.10
ip dhcp excluded-address 10.1.6.1 10.1.6.10
!
ip dhcp pool vlan10
 network 10.1.1.0 255.255.255.0
 default-router 10.1.1.1
ip dhcp pool vlan20
 network 10.1.2.0 255.255.255.0
 default-router 10.1.2.1
ip dhcp pool vlan30
 network 10.1.3.0 255.255.255.0
 default-router 10.1.3.1
ip dhcp pool vlan40
 network 10.1.4.0 255.255.255.0
 default-router 10.1.4.1
ip dhcp pool vlan50
 network 10.1.5.0 255.255.255.0
 default-router 10.1.5.1
ip dhcp pool vlan60
 network 10.1.6.0 255.255.255.0
 default-router 10.1.6.1
!
```

Roteador da Unidade Tatuapé

```
hostname R1T
!
!
!
!
ip dhcp excluded-address 10.2.1.1 10.2.1.10
ip dhcp excluded-address 10.2.2.1 10.2.2.10
ip dhcp excluded-address 10.2.3.1 10.2.3.10
ip dhcp excluded-address 10.2.4.1 10.2.4.10
ip dhcp excluded-address 10.2.5.1 10.2.5.10
ip dhcp excluded-address 10.2.6.1 10.2.6.10
!
ip dhcp pool vlan10
 network 10.2.1.0 255.255.255.0
 default-router 10.2.1.1
ip dhcp pool vlan20
 network 10.2.2.0 255.255.255.0
 default-router 10.2.2.1
ip dhcp pool vlan30
 network 10.2.3.0 255.255.255.0
 default-router 10.2.3.1
ip dhcp pool vlan40
 network 10.2.4.0 255.255.255.0
 default-router 10.2.4.1
ip dhcp pool vlan50
 network 10.2.5.0 255.255.255.0
 default-router 10.2.5.1
ip dhcp pool vlan60
 network 10.2.6.0 255.255.255.0
 default-router 10.2.6.1
!
```

Roteador da Unidade Bela Vista

```
hostname R1B
!
!
!
!
ip dhcp excluded-address 10.3.1.1 10.3.1.10
ip dhcp excluded-address 10.3.2.1 10.3.2.10
ip dhcp excluded-address 10.3.3.1 10.3.3.10
ip dhcp excluded-address 10.3.4.1 10.3.4.10
ip dhcp excluded-address 10.3.5.1 10.3.5.10
ip dhcp excluded-address 10.3.6.1 10.3.6.10
!
ip dhcp pool vlan10
 network 10.3.1.0 255.255.255.0
 default-router 10.3.1.1
ip dhcp pool vlan20
 network 10.3.2.0 255.255.255.0
 default-router 10.3.2.1
ip dhcp pool vlan30
 network 10.3.3.0 255.255.255.0
 default-router 10.3.3.1
ip dhcp pool vlan40
 network 10.3.4.0 255.255.255.0
 default-router 10.3.4.1
ip dhcp pool vlan50
 network 10.3.5.0 255.255.255.0
 default-router 10.3.5.1
ip dhcp pool vlan60
 network 10.3.6.0 255.255.255.0
 default-router 10.3.6.1
!
```

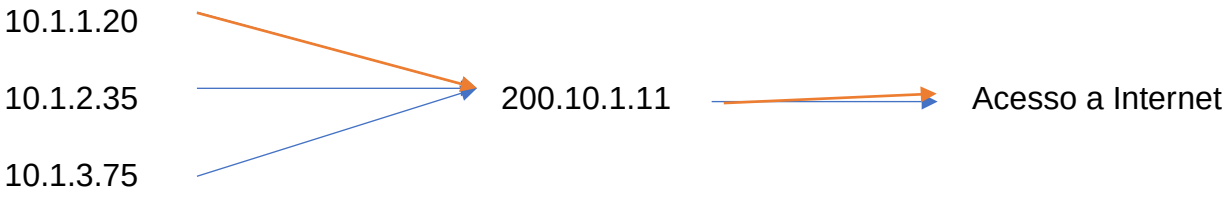
17. Network Address Translation

17.1 O que é o NAT

O NAT, ou Network Address Translation, é utilizado para que um IP em uma rede privada tenha acesso a internet por outro IP com a utilização de sockets, isso acontece em redes de residências por exemplo, quando um computador tenta acessar a internet ele passa pelo roteador que faz a tradução daquele IP para um IP comum de saída, um IP que outros aparelhos na mesma rede usaram para fazer a mesma conexão.

Na prática seria assim:

Requisição



Resposta

Endereço IP Público

Dentro dos IPs da rede das clínicas que podemos acessar a internet, existe um range de 254 endereços e que deveram ser traduzidos para 6 endereços de saída de acordo com a sub-rede que ele esteja, para facilitar a organização e a segurança.

E tabela de roteamento é utilizada de acordo com a unidade em que você esta e em qual sub-rede seu equipamento está localizado, existe uma tabela de roteamento para cada unidade.

17.2 Tabelas de Roteamento NAT

Unidade	PERDIZES

Sub-rede	Range de IP	NAT
10.1.1.0/24	10.1.1.1->10.1.1.254	200.10.1.1
10.1.2.0/24	10.1.2.1->10.1.2.254	
10.1.3.0/24	10.1.3.1->10.1.3.254	
10.1.4.0/24	10.1.4.1->10.1.4.254	
10.1.5.0/24	10.1.5.1->10.1.5.254	
10.1.6.0/24	10.1.6.1->10.1.6.254	

Unidade	TATUAPÉ

Sub-rede	Range de IP	NAT
10.2.1.0/24	10.2.1.1->10.2.1.254	200.10.2.1
10.2.2.0/24	10.2.2.1->10.2.2.254	
10.2.3.0/24	10.2.3.1->10.2.3.254	
10.2.4.0/24	10.2.4.1->10.2.4.254	
10.2.5.0/24	10.2.5.1->10.2.5.254	
10.2.6.0/24	10.2.6.1->10.2.6.254	

Unidade	BELA VISTA

Sub-rede	Range de IP	NAT
10.3.1.0/24	10.3.1.1->10.3.1.254	200.10.3.1
10.3.2.0/24	10.3.2.1->10.3.2.254	
10.3.3.0/24	10.3.3.1->10.3.3.254	
10.3.4.0/24	10.3.4.1->10.3.4.254	
10.3.5.0/24	10.3.5.1->10.3.5.254	
10.3.6.0/24	10.3.6.1->10.3.6.254	

18. VLANs

18.1 O que são VLANs

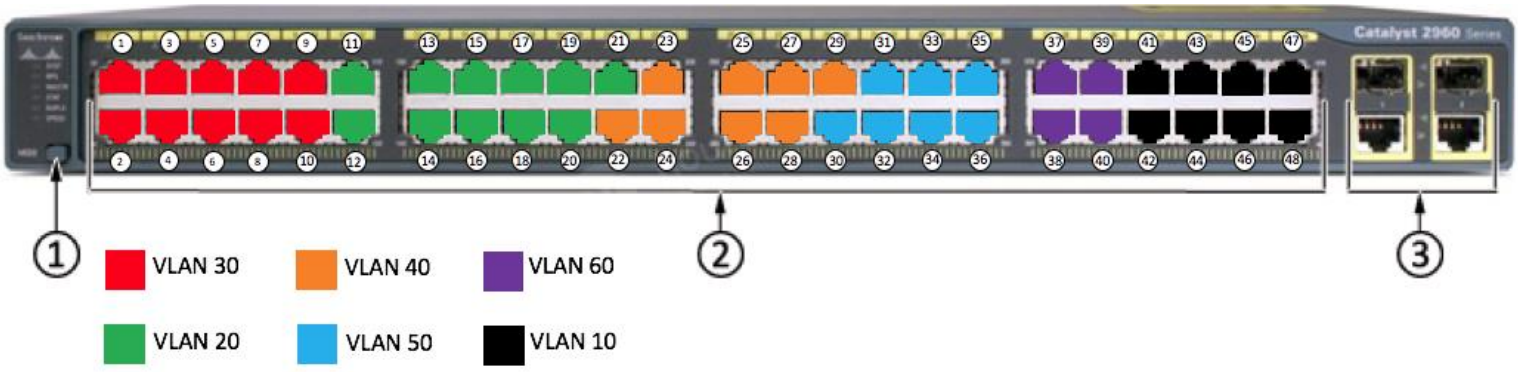
O significado de VLAN é Virtual Local Area Network, ou uma rede local virtual, essa prática consiste em ter uma rede sem ser física para facilitar a administração, separação e segurança dos dispositivos da de sua rede.

Com a utilização das VLANs podemos organizar a infra estrutura da rede sem grandes alterações do cabeamento de equipamentos, apenas criando as redes virtuais e aplicando regras de comunicação.

Da mesma forma que temos endereços diferentes de rede, sub-rede e NAT nas unidades, as VLANs também sofreram alterações em seu endereço, agora cada unidade com um endereço único para as VLANs.

As tabelas a seguir representam todas as VLANs que temos dentro da rede, mostra também qual o nome da VLAN, seu endereço e as interfaces que estão associadas a essa VLAN nos Switches, essa tabela é padronizada assim como outros pontos da rede para as 3 unidades.

18.2 VLANs nas Interfaces do Switch



18.3 Tabelas das VLANs

Unidade	PERDIZES

VLAN	Nome	Endereço	Interfaces
VLAN 10	VLAN Gerencia	10.1.1.1/24	f0/41-48
VLAN 20	VLAN Recepção	10.1.2.1/24	f0/1-10
VLAN 30	VLAN Salas	10.1.3.1/24	f0/11-21
VLAN 40	VLAN Telefones	10.1.4.1/24	f0/22-29
VLAN 50	VLAN Wifi	10.1.5.1/24	f0/30-37
VLAN 60	VLAN Câmeras	10.1.6.1/24	f0/38-40

Unidade	TATUAPÉ

VLAN	Nome	Endereço	Interfaces
VLAN 10	VLAN Gerencia	10.2.1.1/24	f0/41-48
VLAN 20	VLAN Recepção	10.2.2.1/24	f0/1-10
VLAN 30	VLAN Salas	10.2.3.1/24	f0/11-21
VLAN 40	VLAN Telefones	10.2.4.1/24	f0/22-29
VLAN 50	VLAN Wifi	10.2.5.1/24	f0/30-37
VLAN 60	VLAN Câmeras	10.2.6.1/24	f0/38-40

Unidade	BELA VISTA

VLAN	Nome	Endereço	Interfaces
VLAN 10	VLAN Gerencia	10.3.1.1/24	f0/41-48
VLAN 20	VLAN Recepção	10.3.2.1/24	f0/1-10
VLAN 30	VLAN Salas	10.3.3.1/24	f0/11-21
VLAN 40	VLAN Telefones	10.3.4.1/24	f0/22-29
VLAN 50	VLAN Wifi	10.3.5.1/24	f0/30-37
VLAN 60	VLAN Câmeras	10.3.6.1/24	f0/38-40

19. Etherchannel

O protocolo é um protocolo de Link Aggregation, usado para alta disponibilidade e uma tolerância a falhas dentro da sua rede, neste projeto utilizamos esse protocolo entre os switches de camada 2 para que nenhuma das VLANs fique sem comunicação com a rede, ele foi configurado da mesma forma para todas a unidades, da seguinte maneira:

```
!
interface FastEthernet0/20
 switchport mode trunk
 channel-group 1 mode active
!
interface FastEthernet0/21
 switchport mode trunk
 channel-group 1 mode active
!
```

```
S1P#show etherchannel
                Channel-group listing:
                ----------------------

Group: 1
----------
Group state = L2
Ports: 2 Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol:   LACP
```

20. HSRP

O protocolo HSRP, Hot Standby Router Protocol, é um dentre vários protocolos que garante uma alta disponibilidade e uma tolerância a falhas dentro da sua rede, ele é configurado entre 2 ou mais roteadores.

Nesse projeto o HSRP esta presente nos 2 roteadores, R1 e R2 de cada unidade, além de trazer redundância para a interfaces eles tem o mesmo objetivo entre as VLANs dentro de nossa rede.

Foi configurado o endereço virtual 10.X.100.254, variando esse endereço conforme a unidade que estamos. Esse endereço é conhecido pelos 2 roteadores e caso haja falha nos links eles decidiram qual roteador assumira como principal até que o problema seja resolvido.

```
GigabitEthernet0/0 - Group 1
  State is Active
    12 state changes, last state change 01:30:37
  Virtual IP address is 10.1.100.254
  Active virtual MAC address is 0000.0C07.AC01
    Local virtual MAC address is 0000.0C07.AC01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.164 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 250 (configured 250)
  Group name is hsrp-Gig0/0-1 (default)
```

20.2 Teste de Falhas

Os testes foram feitos desligando e ligando a interfaces que ligam os 2 roteadores, temos R1 como principal tendo a prioridade de 250 quando desligamos o

```
R1P(config-if)#
 %HSRP-6-STATECHANGE: GigabitEthernet0/0 Grp 1 state Active -> Init

%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to down
```

link, aparece a seguinte mensagem:

Enquanto no R2 aparece a seguinte mensagem:
Informando que agora ele é o roteador que esta ativo e não mais em modo standby.

```
%HSRP-6-STATECHANGE: GigabitEthernet0/0 Grp 1 state Speak -> Standby

%HSRP-6-STATECHANGE: GigabitEthernet0/0 Grp 1 state Standby -> Active
```

21. PVST

O PVST, Per VLAN Spanning Tree, é um protocolo também voltado para melhora da performance da rede, sempre aplicado em switches, utilizando redundância na rede é um protocolo que elimina loops de camada 2, e é possível a configuração de prioridade entre as VLANs e as mensagens a ela associada.

Nessa configuração estamos utilizando o S1 como Root Bridge do PVST

Configurações no Switch 1

```
S1P#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0040.0B8B.BE9C
              Cost        38
              Port        24(FastEthernet0/24)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     00E0.F7AD.5AE3
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/24           Root FWD 19        128.24   P2p
Gi0/1            Desg FWD 4         128.25   P2p
Gi0/2            Desg FWD 4         128.26   P2p

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    24586
              Address     00E0.F7AD.5AE3
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24586  (priority 24576 sys-id-ext 10)
              Address     00E0.F7AD.5AE3
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Gi0/1            Desg FWD 4         128.25   P2p

VLAN0020
  Spanning tree enabled protocol ieee
  Root ID     Priority    24596
              Address     00E0.F7AD.5AE3
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24596  (priority 24576 sys-id-ext 20)
              Address     00E0.F7AD.5AE3
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Gi0/1            Desg FWD 4         128.25   P2p
```

```
VLAN0030
  Spanning tree enabled protocol ieee
  Root ID     Priority    24606
              Address     00E0.F7AD.5AE3
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24606  (priority 24576 sys-id-ext 30)
              Address     00E0.F7AD.5AE3
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi0/1            Desg FWD 4         128.25   P2p

VLAN0040
  Spanning tree enabled protocol ieee
  Root ID     Priority    24616
              Address     00E0.F7AD.5AE3
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24616  (priority 24576 sys-id-ext 40)
              Address     00E0.F7AD.5AE3
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi0/1            Desg FWD 4         128.25   P2p

VLAN0050
  Spanning tree enabled protocol ieee
  Root ID     Priority    24626
              Address     00E0.F7AD.5AE3
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24626  (priority 24576 sys-id-ext 50)
              Address     00E0.F7AD.5AE3
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi0/1            Desg FWD 4         128.25   P2p

VLAN0060
  Spanning tree enabled protocol ieee
  Root ID     Priority    24636
              Address     00E0.F7AD.5AE3
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24636  (priority 24576 sys-id-ext 60)
              Address     00E0.F7AD.5AE3
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20
```

22. Tabela de ligação das Interfaces nos equipamentos

Para simular a rede em funcionamento foi necessário recriar esse projeto em uma escala reduzida e implementar todas as configurações e registrar elas para provar que está se comportando como esperado, nessa sessão teremos as tabelas de ligação das Interfaces nos equipamentos.

Tabela de endereçamento das interfaces

Unidade	PERDIZES

Equipamento	Interface	IP	Masc.
R1	g0/1.10	10.1.1.1	255.255.255.0
	g0/1.20	10.1.2.1	
	g0/1.30	10.1.3.1	
	g0/2.40	10.1.4.1	
	g0/2.50	10.1.5.1	
	g0/2.60	10.1.6.1	
	g1/0	10.1.100.1	
	g1/1	10.1.100.2	
R2	g0/1.10	10.1.1.1	255.255.255.0
	g0/1.20	10.1.2.1	
	g0/1.30	10.1.3.1	
	g0/2.40	10.1.4.1	
	g0/2.50	10.1.5.1	
	g0/2.60	10.1.6.1	
	g1/0	10.1.100.3	
	g1/1	10.1.100.4	
F1	g0/1	10.1.100.5	255.255.255.0
	g0/2	10.1.100.6	
	g0/3	10.1.100.7	
	g0/4	10.1.100.8	
F2	g0/1	10.1.100.9	255.255.255.0
	g0/2	10.1.100.10	
	g0/3	10.1.100.11	

Unidade	TATUAPÉ

Equipamento	Interface	IP	Masc.
R1	g0/1.10	10.2.1.1	255.255.255.0
	g0/1.20	10.2.2.1	
	g0/1.30	10.2.3.1	
	g0/2.40	10.2.4.1	
	g0/2.50	10.2.5.1	
	g0/2.60	10.2.6.1	
	g1/0	10.2.100.1	
	g1/1	10.2.100.2	
R2	g0/1.10	10.2.1.1	255.255.255.0
	g0/1.20	10.2.2.1	
	g0/1.30	10.2.3.1	
	g0/2.40	10.2.4.1	
	g0/2.50	10.2.5.1	
	g0/2.60	10.2.6.1	
	g1/0	10.2.100.3	
	g1/1	10.2.100.4	
F1	g0/1	10.2.100.5	255.255.255.0
	g0/2	10.2.100.6	
	g0/3	10.2.100.7	
	g0/4	10.2.100.8	
F2	g0/1	10.2.100.9	255.255.255.0
	g0/2	10.2.100.10	
	g0/3	10.2.100.11	

Unidade	BELA VISTA

Equipamento	Interface	IP	Masc.
R1	g0/1.10	10.3.1.1	255.255.255.0
	g0/1.20	10.3.2.1	
	g0/1.30	10.3.3.1	
	g0/2.40	10.3.4.1	
	g0/2.50	10.3.5.1	
	g0/2.60	10.3.6.1	
	g1/0	10.3.100.1	
	g1/1	10.3.100.2	
R2	g0/1.10	10.3.1.1	255.255.255.0
	g0/1.20	10.3.2.1	
	g0/1.30	10.3.3.1	
	g0/2.40	10.3.4.1	
	g0/2.50	10.3.5.1	
	g0/2.60	10.3.6.1	
	g1/0	10.3.100.3	
	g1/1	10.3.100.4	
F1	g0/1	10.3.100.5	255.255.255.0
	g0/2	10.3.100.6	
	g0/3	10.3.100.7	
	g0/4	10.3.100.8	
F2	g0/1	10.3.100.9	255.255.255.0
	g0/2	10.3.100.10	
	g0/3	10.3.100.11	

23. Equipamentos

Para esse projeto, foi escolhido equipamentos que suportassem a capacidade de tráfico de dados necessária, equipamentos com alta segurança e equipamentos de fácil instalação, manutenção e gerenciamento.

A infraestrutura é baseada em 4 principais equipamentos, o firewall que é responsável por filtrar todo conteúdo do tráfico de dados, sendo ele de dentro para fora da rede ou de fora para dentro. O roteador, responsável por fazer a comunicação entre as diferentes sub-redes e pela comunicação com a internet.

O switch é responsável por ligar fisicamente os equipamentos e possibilitar a comunicação deles com os outros equipamentos, e por fim o access point, responsável pela conexão wi-fi tanto dos funcionários quanto dos visitantes.

A maioria dos equipamentos escolhidos são da Cisco, empresa de referência em equipamentos para infraestrutura de rede, o único equipamento que não é da Cisco é o firewall, é da Netgate, marca de referência em security gateways e a qual tenho vivência diária do funcionamento e configurações.

23.1 Firewall

O firewall que será utilizado é o SG-5100 da Netgate, ele contém 6 interfaces para conexão, sendo uma porta WAN, uma LAN e 4 portas opcionais, podendo configurá-las como WAN ou LAN.

Foi escolhido esse modelo devido seus recursos de segurança, e por principalmente conter o recurso de IPS/IDS, muito importante contra ataques e fundamental para segurança da sua rede.

Ele contém uma interface de configuração clara, objetiva e completa, tendo acesso por um WebGUI.

23.2 Roteador

O roteador escolhido foi o NCS 540 Small Density, N540X-6Z18G-SYS-A, um roteador básico, oferece uma plataforma de roteamento de acesso segura e altamente disponível para provedores de serviços. Os fatores de forma fixos e modulares suportam automação e programação avançadas para fornecer 5G, PHY remoto, Carrier Ethernet e FTTx.

Conta com uma fonte redundante, e 24 portas, sendo 18x 1G SFP+, 6x 1G/10G SFP+ para fazer a comunicação e gestão de toda a rede.

23.3 Switch

O WS-C2960-48TC-L é um dos switches Cisco Catalyst 2960 Series. Contendo 48 portas, esta série oferece suporte para voz, vídeo, dados e acesso altamente seguro, também oferece um gerenciamento escalonável conforme as necessidades de negócio.

Os recursos comuns estão incluídos: Segurança aprimorada incluindo Cisco TrustSec para fornecer autenticação, controle de acesso e administração de política de segurança, opções de desempenho Multiple Fast ou Gigabit Ethernet, Cisco EnergyWise para gerenciamento de energia, gerenciamento de rede escalável.

23.4 Access Point

O UniFi AC Lite AP apresenta a mais recente tecnologia Wi-Fi 802.11ac em um design industrial refinado e é ideal para implantação econômica de redes sem fio de alto desempenho.

24. Tabela de Custo dos equipamentos

A tabela a seguir representa uma estimativa de preço dos produtos, uma vez que são importados, podem ter seus valores alterados.

Equipamento	**Quantidade**	**Valor**
Firewall	1	R$ 5.300,00
Roteador	1	R$ 10.000,00
Switch	1	R$ 5.600,00
Access Point	2	R$ 1.400,00
		R$ 22.300,00

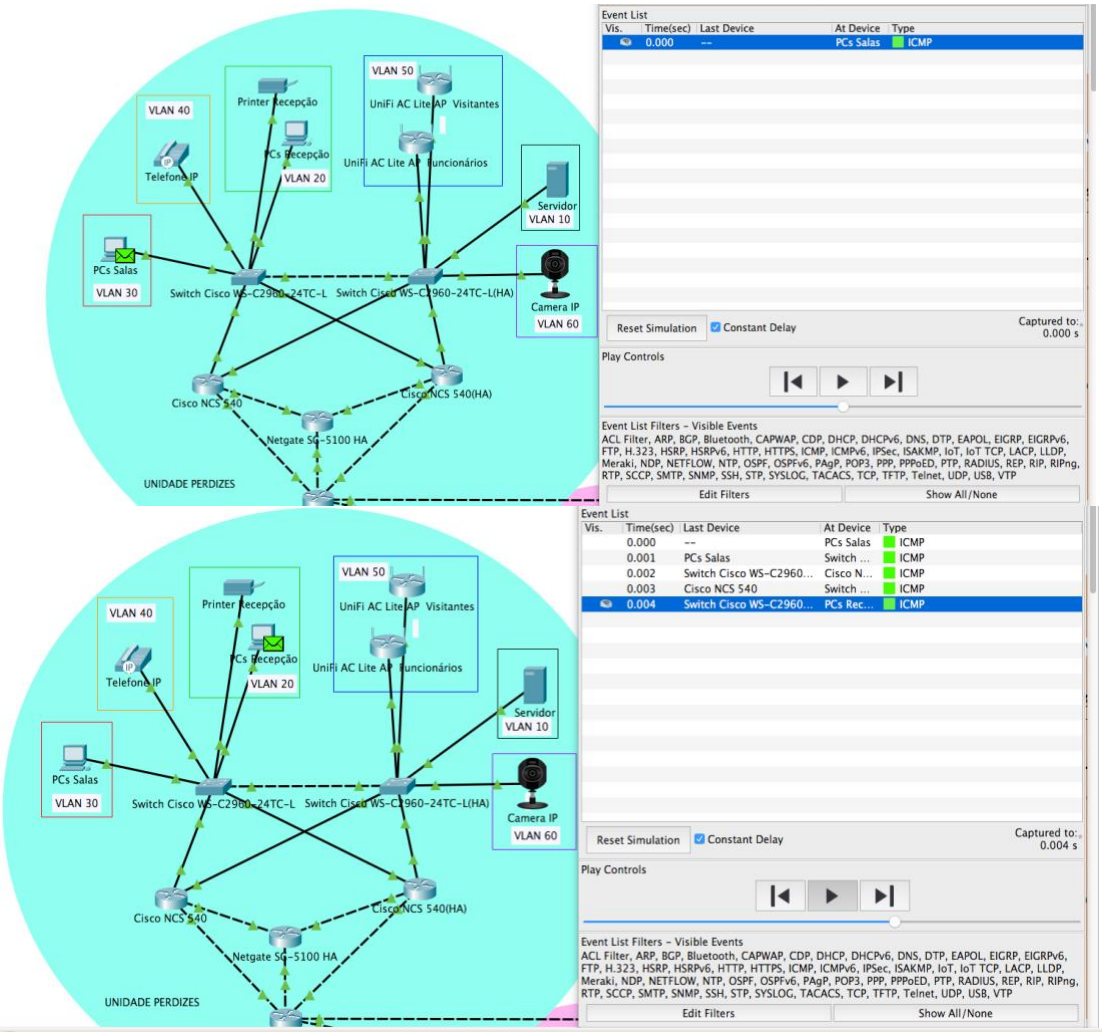
24.2 Tabela de Custo com Alta Disponibilidade

Equipamento	**Quantidade**	**Valor**
Firewall	2	R$ 10.600,00
Roteador	2	R$ 20.000,00
Switch	2	R$ 11.200,00
Access Point	2	R$ 1.400,00
		R$ 43.200,00

É importante ressaltar que as unidades foram usadas apenas como uma referência, desde plantas até quantidade dos dispositivos.

25. Teste de Comunicação dentro da Rede

Para o teste de conexão, fizemos a comunicação entre os dispositivos da VLAN 30, VLAN das Salas, com a VLAN 20, VLAN da Recepção, simulando um envio de e-mail, ou algum formulário do dia a dia.



Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PCs Salas	ICMP
	0.001	PCs Salas	Switch ...	ICMP
	0.002	Switch Cisco WS-C2960...	Cisco N...	ICMP
	0.003	Cisco NCS 540	Switch ...	ICMP
	0.004	Switch Cisco WS-C2960...	PCs Rec...	ICMP
	0.005	PCs Recepção	Switch ...	ICMP
	0.006	Switch Cisco WS-C2960...	Cisco N...	ICMP
	0.007	Cisco NCS 540	Switch ...	ICMP
	0.008	Switch Cisco WS-C2960...	PCs Salas	ICMP

26. Referências Bibliográficas

- BRITO, Samuel. VPN Site-to-Site no Firewall Cisco ASA do Packet Tracer. Blog LabCisco, 2018. Disponível em:<http://labcisco.blogspot.com/2016/05/vpn-siteto-site-no-firewall-cisco-asa.html>. Acesso em: 20 de mar. De 2021

- Quantidade de hosts e sub-rede. Cisco, 2005. Disponível em:< https://www.cisco.com/c/pt_br/support/docs/ip/routing-information-protocolrip/13790-8.html>. Acesso em 20 de mar. 2021

- MEIRELES, Adriano. Capítulo 3: Entendendo o endereçamento IP. Hardware.com.br, 2006. Disponível em:< https://www.hardware.com.br/livros/linux-redes/capitulo-entendendoenderecamento.html#:~:text=Cada%20grupo%20de%208%20bits,o%20host%20 dentro%20da%20rede.>. Acesso em 21 de mar. 2021

- BORGES, Cihco. DHCP ou Servidor?. Clube do Hardware, 2012. Disponível em:< https://www.clubedohardware.com.br/topic/968639-dhcp-do-servidor-oudo-roteador/>. Acesso em: 25 de mar. De 2021

- How to Configure Standard ACL for Cisco Packet Tracer - CCNA Tutorial Youtube, 2019. Disponível em:< https://www.youtube.com/watch?v=4PCLROZv4uo>. Acesso em 26 de mar. 2021

- BATTISTI, Júlio. Tutorial de TCP/IP – Parte 20 – NAT – Network Address Translation. Linhadecódigo. Disponível em:< http://www.linhadecodigo.com.br/artigo/795/tutorial-de-tcp_ip-parte-20-natnetwork-address-translation.aspx#:~:text=Por%20padr%C3%A3o%2C%20o%20NAT%20utiliza,endere%C3%A7amento%2C%20nas%20configura%C3%A7%C3%B5es%20do%20NAT.>Acesso em 26 de mar. 2021.

- Recursos e funcionalidade do HSRP protocol , cisco.com, 2021. Disponível em:<https://www.cisco.com/c/pt_br/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.html>.Acesso em 20 jun. de 2021.

- Spanning-tree root bridge configuration, NetworkLessons.com, 2021. Disponível em:< https://networklessons.com/spanning-tree/spanning-tree-root-bridge-configuration>. Acesso em 26 de jun. de 2021

Manual Firewall Netgate SG-5100

- https://docs.netgate.com/pfsense/en/latest/solutions/sg-5100/index.html

Manual Roteador Cisco NCS 540 Small Density

- https://www.cisco.com/c/en/us/products/collateral/routers/network-convergencesystem-500-series-routers/datasheet-c78-744713.html

Manual Switch Cisco WS-C2960-48TC-L

- https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-plusseries-switches/data_sheet_c78-728003.html

Manual Access Point UAP-AC-LITE

- https://dl.ubnt.com/datasheets/unifi/UniFi_AC_APs_DS.pdf