

UNIVERSIDADE DO VALE DO ITAJAÍ

EMCT – ESCOLA DO MAR, CIÊNCIA E TECNOLOGIA

CIÊNCIA DA COMPUTAÇÃO – REDES DE COMPUTADORES II

PROF. MSc. FELIPE VIEL

GUSTAVO HENRIQUE STAHL MÜLLER

PAULO HENRIQUE ROHLING

**PROJETO DE REDE PARA UMA UNIVERSIDADE**

ITAJAÍ

2022

**SUMÁRIO**

[**1.** **INTRODUÇÃO** 2](#_Toc107685937)

[**2.** **DESENVOLVIMENTO** 3](#_Toc107685938)

[2.1. CONFIGURAÇÃO DOS ROTEADORES 3](#_Toc107685939)

[2.1.1. OSPF 4](#_Toc107685940)

[2.1.2. BGP 6](#_Toc107685941)

[2.2. SERVIÇO DE DHCP 8](#_Toc107685942)

[2.3. SERVIÇO DE DNS 10](#_Toc107685943)

[2.4. IMPLEMENTAÇÃO DO NAT 11](#_Toc107685944)

[2.5. DEFINIÇÃO DAS VLANS 12](#_Toc107685945)

[2.6. CONFIGURAÇÃO DO SNMP 12](#_Toc107685946)

[2.7. CONFIGURAÇÃO DO FIREWALL 12](#_Toc107685947)

[**3.** **CONCLUSÃO** 13](#_Toc107685948)

[**ANEXO A – TOPOLOGIA FINAL DA REDE** 10](#_Toc107685949)

[**ANEXO B – DIAGRAMA DE REDE** 11](#_Toc107685950)

[**ANEXO C – TABELAS DE CUSTOS** 12](#_Toc107685951)

1. **INTRODUÇÃO**

Este trabalho tem como objetivo desenvolver um projeto de rede que atenda às necessidades de uma universidade. Apresentaremos os equipamentos escolhidos, a forma como serão configurados e criaremos um orçamento para implementação da rede desenvolvida.

Esta universidade possui um departamento de Administração e outro de TI, que formam duas das sub-redes do projeto. Além destas, são necessárias outras duas sub-redes, uma para os visitantes e outra para os estudantes.

Toda a especificação da rede foi feita para comportar ao menos 100 computadores no total, sendo que 30 são destinados para a Administração e TI, 15 para visitantes e 55 para estudantes.

1. **DESENVOLVIMENTO**

Como foi pontuado na seção anterior, serão necessárias quatro sub-redes para este projeto de rede, logo, se faz necessária a definição das suas faixas de IP, bem como as máscaras utilizadas em cada uma delas. A Tabela 1 mostra as sub-redes criadas para cada departamento, bem como a definição de sua rede.

**Tabela 1 – Definição das sub-redes**

|  |  |  |  |
| --- | --- | --- | --- |
| **Departamento** | **Máscara de Sub-rede** | **Sub-rede** | **Default Gateway** |
| Administração | 255.255.255.0 | 192.168.0.X | 192.168.0.1 |
| TI | 255.255.255.0 | 192.168.1.X | 192.168.1.1 |
| Visitantes | 255.0.0.0 | 20.X.X.X | 20.0.0.1 |
| Estudantes | 255.0.0.0 | 10.X.X.X | 10.0.0.1 |

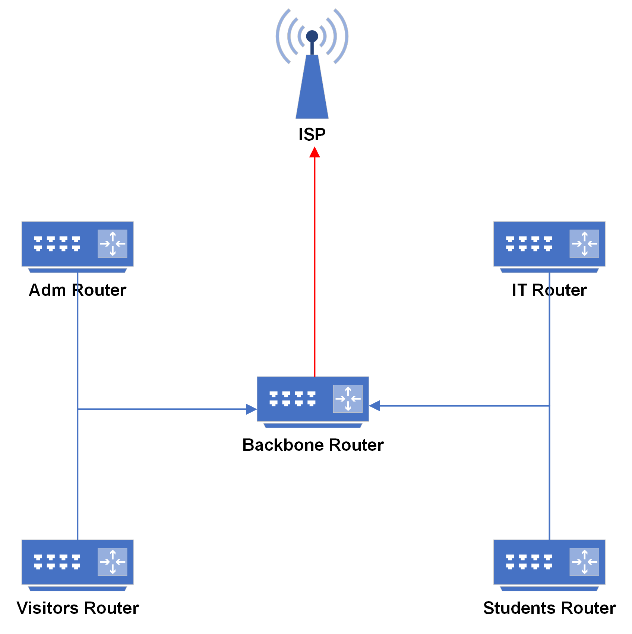
Fonte: Os autores.

* 1. CONFIGURAÇÃO DOS ROTEADORES

Para cada departamento descrito acima, foi destinado um roteador Cisco 2901, onde cada qual foi conectado à um roteador backbone através de cabos gigabit ethernet cat5e. No roteador central, foram adicionadas duas interfaces gigabit ethernet, pois o mesmo só possuía duas, além de uma interface óptica, responsável por receber uma fibra oriunda da ISP.

O diagrama da Figura 1 ilustra a organização destas conexões. Note que a estrutura da ISP não foi definida, uma vez que não faz parte da rede a ser projetada.

**Figura 1 – Definição dos roteadores**



Fonte: Os autores.

Para que os roteadores possam se comunicar, é necessária a implementação de um protocolo de roteamento. Além disso, a comunicação entre o roteador central e o roteador da ISP só pode ser efetuada após a configuração de um protocolo de roteamento de borda.

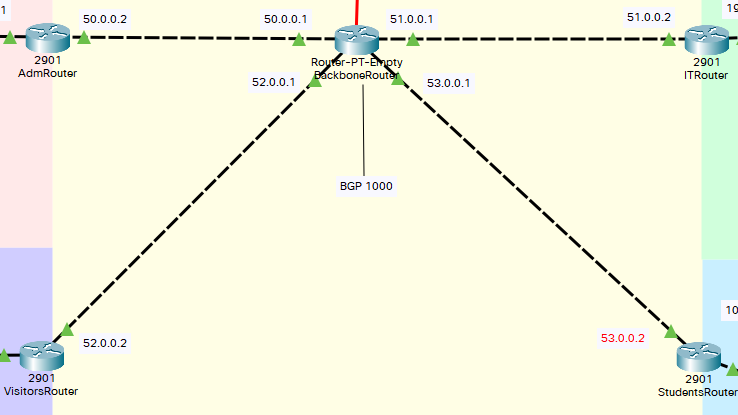
A seção a seguir explicará como foram feitas as implementações do OSPF e do BGP.

* + 1. OSPF

O OSPF (Open Shortest Path First) é um protocolo de roteamento intra-domínio responsável por gerenciar os caminhos entre roteadores. Para realizar tal atividade, este protocolo utiliza o algoritmo de Dijkstra para construir e manter uma tabela de roteamento contendo as rotas mais curtas para cada link da rede (diferentemente do RIP, que mantém todas as rotas possíveis).

Para que isto seja possível, cada conexão com o roteador central forma uma sub-rede nova, de forma que utilizaremos quatro sub-redes adicionais para esta configuração. As sub-redes são 50.X.X.X, 51.X.X.X, 52.X.X.X e 53.X.X.X, assim como ilustra a Figura 2.

**Figura 2 – Definição dos roteadores**



Fonte: Os autores.

Como pode ser visto no Anexo A, a definição do OSPF na topologia final possui cinco áreas, uma para cada departamento mais a área interna dos roteadores, sendo área 0 para interna, área 10 para administração, área 20 para TI, área 30 para visitantes e área 40 para estudantes.

A configuração destas áreas deve ser feita em todos os roteadores. Em suma, nós precisamos criar um processo do OSPF (será utilizado o mesmo processo para toda a configuração) e cadastrar as redes de cada uma das interfaces do roteador.

Iniciando pelo roteador da administração, temos duas interfaces que se conectam com duas sub-redes, a sub-rede da administração (192.168.0.X) e a sub-rede interna dos roteadores (50.X.X.X). Para cadastrar as duas sub-redes, precisamos acessar a configuração do OSPF através do comando ***router ospf 1***, seguido dos comandos para criar as sub-redes na tabela de roteamento do OSPF, que são eles: ***network 192.168.0.0 0.0.0.255 area 10*** e ***network 50.0.0.0 0.0.0.3 area 0.***

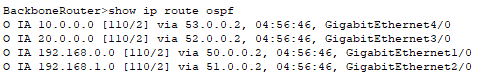
Para o roteador da TI, as duas interfaces se conectam com a sub-rede da TI (192.168.1.X) e a sub-rede interna dos roteadores (51.X.X.X). Novamente executa-se o comando ***router ospf 1***, seguido dos comandos ***network 192.168.1.0 0.0.0.255 area 20*** e ***network 51.0.0.0 0.0.0.3 area 0***, para a criação da nova área.

Para o roteador dos Visitantes, as duas interfaces se conectam com a sub-rede dos Visitantes (10.X.X.X) e a sub-rede interna dos roteadores (52.X.X.X). Novamente executa-se o comando ***router ospf 1***, seguido dos comandos ***network 10.0.0.0 0.0.0.255 area 30*** e ***network 52.0.0.0 0.0.0.3 area 0***, para a criação da nova área.

Para o roteador dos Estudantes, as duas interfaces se conectam com a sub-rede dos Estudantes (20.X.X.X) e a sub-rede interna dos roteadores (53.X.X.X). Novamente executa-se o comando ***router ospf 1***, seguido dos comandos ***network 20.0.0.0 0.0.0.255 area 40*** e ***network 53.0.0.0 0.0.0.3 area 0***, para a criação da nova área.

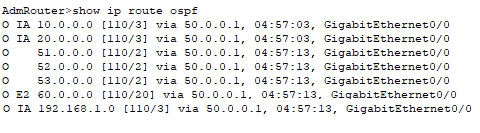
Com estas configurações feitas, podemos ver na Figura 3 que o roteador central já consegue enxergar as sub-redes. Na Figura 4, pode-se ver que o roteador da administração possui as sub-redes dos outros departamentos em sua tabela de roteamento, possibilitando a comunicação.

**Figura 3 – Tabela de roteamento do roteador central**



Fonte: Os autores.

**Figura 4 – Tabela de roteamento do roteador da administração**



Fonte: Os autores.

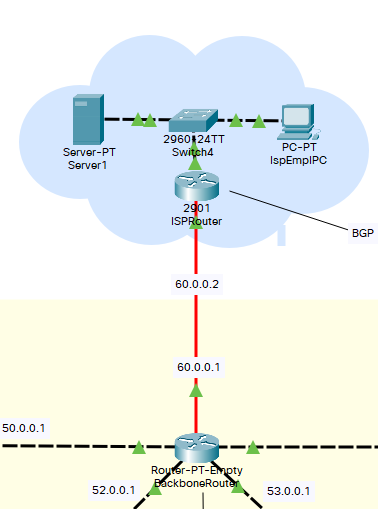
* + 1. BGP

O BGP (Border Gateway Protocol) é um protocolo de roteamento inter-domínio utilizado em roteadores de borda para que se comuniquem com outros AS. Ele é utilizado principalmente para que a ISP possa gerenciar as redes dos seus contratantes.

Da mesma forma que o OSPF, o BGP necessita que a conexão entre os roteadores forme uma nova sub-rede. Para esta conexão, foi utilizada a 60.X.X.X. Além disso, como a distância entre o roteador central e o roteador da ISP é grande, faz-se necessária a utilização de fibra óptica.

Para realizar os testes desta implementação, foi criada uma sub-rede para simular a ISP, como pode ser visto na Figura 5.

**Figura 5 – Conexão do roteador central com a ISP**



Fonte: Os autores.

Para dar início à configuração do BGP no roteador central, foi necessário definir um BGP ID para o roteador. Isto foi feito executando o comando ***router bgp 1000*** na CLI do roteador.

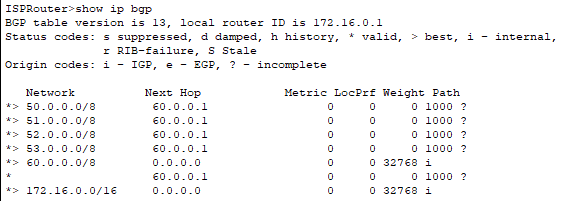
Em seguida, foi necessário cadastrar o roteador da ISP como um vizinho do roteador central através do comando ***neighbor 60.0.0.2 remote-as 1001***, seguido do comando ***redistribute connected***, utilizado para redistribuir as rotas recebidas.

Para fins de teste, estas configurações foram replicadas para o roteador daISP, fazendo a atribuição de outro ID BGP para ele, bem como o cadastro do roteador central como vizinho do mesmo.

Feito isto, o último passo necessário para que os dispositivos das duas redes possam se comunicar é redistribuir as rotas do OSPF nos roteadores da ISP, que foi feito aplicando os comandos ***redistribute bgp 1001 subnets*** e ***redistribute ospf 1 match external*** nos dois roteadores.

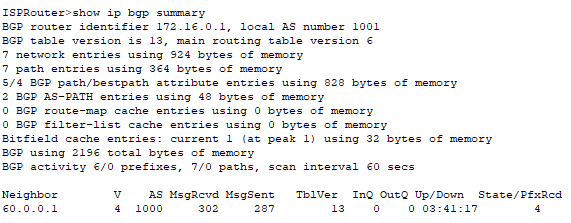
Após a realização destes passos, o sumário de vizinhos e as tabelas de rotas foram geradas e são mostradas nas Figuras 6 e 7. Já é possível notar que a configuração do BGP foi bem-sucedida e o roteador da ISP já pode visualizar a rede interna.

**Figura 6** – Sumário de vizinhos do roteador de borda da ISP



Fonte: Os autores.

**Figura 7** – Rotas geradas no roteador de borda da ISP



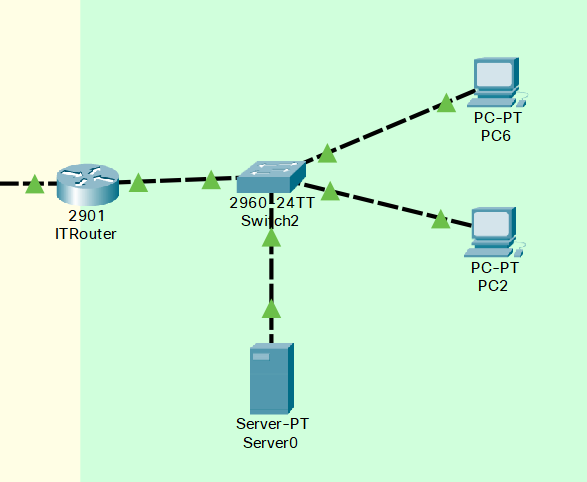
Fonte: Os autores.

* 1. SERVIÇO DE DHCP

Como é de conhecimento geral, a atribuição estática de endereços IP para os dispositivos da rede é completamente inviável. Logo, é necessário utilizar o DHCP (Dynamic Host Configuration Protocol) para fazer a atribuição dinamicamente assim que o dispositivo se conectar à uma das sub-redes pré-determinadas.

Para isso, foi inserido na rede um servidor próprio para a universidade, uma vez que poderemos reaproveitá-lo para a hospedagem do site institucional, que será feito na próxima seção. Na Figura 8, mostra-se a rede da TI com o servidor conectado à um switch, junto com outros dois computadores para testar.

**Figura 8** – Inserção do novo servidor na rede de TI



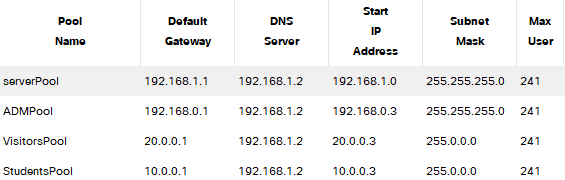
Fonte: Os autores.

Quando um novo dispositivo se conecta à uma sub-rede e ainda não possui um endereço IP, não há como ele saber para onde enviar uma requisição DHCP. Por isso, por padrão, essa requisição é feita em broadcast, ou seja, o pacote é enviado para todos os dispositivos da rede e somente um link que provê o serviço de DHCP a aceita.

Com isso em mente, é necessário fazer com que o servidor possa fornecer endereços IP para todos os quatro departamentos, ou seja, ele deve ser capaz de atribuir endereços 192.168.0.X, 192.168.1.X, 10.X.X.X e 20.X.X.X. Para isso, é preciso cadastrar pools de endereços para cada sub-rede, que foi feito da forma como é mostrada na Figura 9.

Nota-se que o número máximo de usuários para todas as sub-redes é de 241, o valor padrão. Este valor não foi alterado pelo simples fato de que a rede não precisa suportar mais de 100 computadores.

**Figura 9** – Definição das pools de IP no serviço DHCP



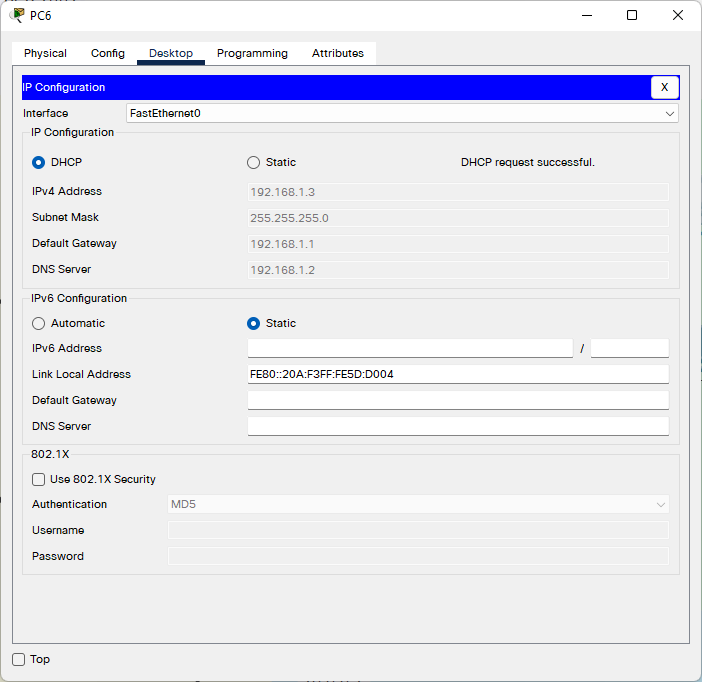
Fonte: Os autores.

Após configurar o serviço DHCP, os computadores conectados à sub-rede de TI já recebem um endereço IP dinamicamente, como mostra a Figura 10. No entanto, as outras sub-redes não conseguem alcançar o servidor, pois os roteadores de cada sub-rede, ao receber um pacote em broadcast, não o propagam externamente.

Para resolver este problema, é necessário que cada roteador cadastre um endereço de helper. Este é um endereço de um link da rede responsável por lidar com alguma requisição quando o roteador está prestes a descarta-la. Para criar este redirecionamento, basta executar o comando ***ip helper-address 192.168.1.2*** na CLI de cada roteador da rede (exceto o central). O endereço IP 192.168.1.2 pertence ao servidor previamente configurado.

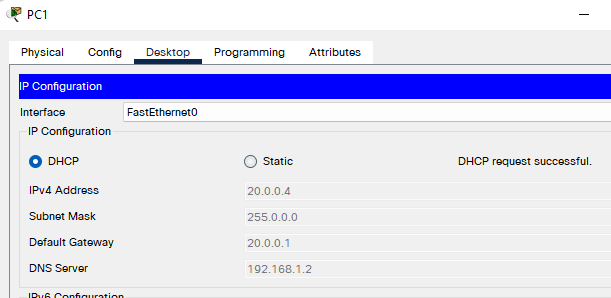
Depois de realizar esta última configuração, um dispositivo conectado à sub-rede de visitantes, por exemplo, já pôde receber um endereço IP dinamicamente, como é mostrado na Figura 11.

**Figura 10** – Requisição DHCP da TI completada com sucesso



Fonte: Os autores.

**Figura 11** – Requisição DHCP de um visitante completada com sucesso



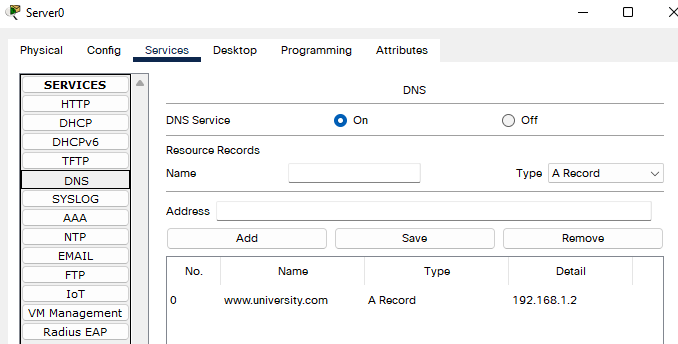
Fonte: Os autores.

* 1. SERVIÇO DE DNS

A universidade possui um site institucional hospedado neste mesmo servidor. Logo, para que os dispositivos conectados às sub-redes possam acessá-lo mais facilmente, faz-se necessária a implementação de um serviço de DNS também.

Como é mostrado na Figura 12, sua configuração é bem simples, basta definir um endereço para o website, que será o ***www.university.com***, e especificar o endereço IP para qual ele aponta, que é o próprio endereço do servidor.

**Figura 12** – Definição do endereço DNS

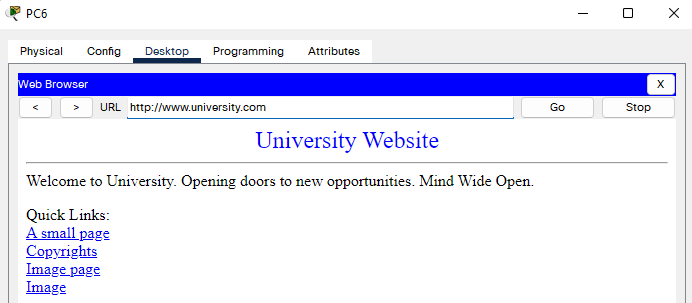


Fonte: Os autores.

Já que possuímos um serviço de DHCP ativo, podemos fazer com que todos os dispositivos que receberem um endereço IP também recebam um endereço de DNS. Isso já foi feito na seção anterior, como pode ser visto na Figura 9.

Feita esta configuração, qualquer dispositivo conectado a qualquer sub-rede pode acessar o website ilustrado na Figura 13 através de um navegador.

**Figura 13** – Página institucional



Fonte: Os autores.

* 1. IMPLEMENTAÇÃO DO NAT

A configuração do NAT foi feita no roteador central para que os endereços IPs da parte interna da rede sejam mascarados durante a comunicação. Para isso, foi necessário criar uma pool de endereços para o NAT, que é feito através do comando ***ip nat pool natpool 172.16.0.1 172.16.0.254 netmask 255.255.0.0***, onde definimos a faixa de endereços IP públicos (aqui simulado com a rede da ISP).

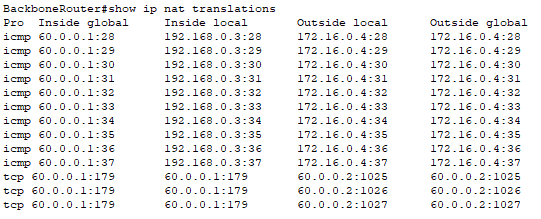
Depois disso, precisamos criar uma access-list para permitir que os endereçamentos para as sub-redes sejam traduzidos. Isto é feito através dos comandos ***access-list 10 permit 192.168.0.0 0.0.0.255***, ***access-list 20 permit 192.168.1.0 0.0.0.255***, ***access-list 30 permit 10.0.0.0 0.0.0.255*** e ***access-list 40 permit 20.0.0.0 0.0.0.255***.

Agora, é preciso fazer com que o NAT utilize estas listas na pool de endereços através dos comandos ***ip nat inside source list X pool natpool***, onde X é o ID de cada uma das access-list.

Por fim, com os endereçamentos configurados, só é necessário definir no roteador central quais interfaces são internas e qual interface é externa. Para o nosso caso, utilizaremos o comando ***ip nat inside*** para todas as interfaces, exceto a que se conecta com o roteador da ISP, para a qual será utilizada o comando ***ip nat outside***.

Após todos estes passos e alguns pings entre os computadores da administração e da ISP, podemos ver na Figura 14 que o roteador já começa a popular a tabela de traduções.

**Figura 14** – Página institucional



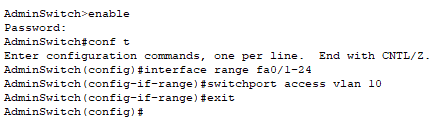
Fonte: Os autores.

* 1. DEFINIÇÃO DAS VLANS

No total foram criadas 4 VLANs, uma para cada departamento da universidade. Nenhuma porta trunk foi utilizada, apenas portas de acesso. A configuração foi realizada em todos os switches da rede, de acordo com o departamento em que cada switch está. Interfaces do switch de administração receberam o ID de VLAN 10, interfaces do switch de TI receberam o ID de VLAN 20, interfaces do switch de visitantes receberam o ID de VLAN 30 e interfaces dos switches de estudantes receberam o ID de VLAN 40.

O uso destas VLANs ainda permite que computadores que estão em diferentes departamentos se comuniquem.

**Figura 15** – Configuração da VLAN 10 no switch do departamento de administração.



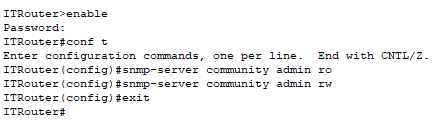
Fonte: Os autores.

* 1. CONFIGURAÇÃO DO SNMP

Todas os roteadores e switches da rede podem ser gerenciados com o protocolo SNMP. A string de comunidade usada em todas as entidades é *admin*, mas na vida real é boa prática que diferentes roteadores/switches usem diferentes strings.

Como a terceira versão do SNMP usa uma combinação de usuário e senha para autenticação, a nossa rede (como está) permite somente o uso da primeira ou segunda versão do SNMP.

**Figura 16** – Ativação do SNMP no roteador da TI.

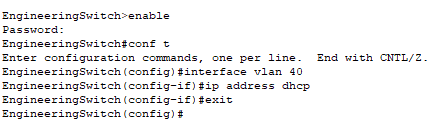


Fonte: Os autores.

Para que a configuração do SNMP funcionasse em switches, precisamos criar uma interface virtual que possuísse um endereço IP. Essa interface recebe o seu endereço IP, máscara e gateway através do DHCP previamente configurado. A interface criada é configurada para estar na mesma VLAN que o switch está.

Esse processo foi executado em cada um dos switches da rede.

**Figura 17** – Configuração de IP no switch de engenharia do departamento de estudantes.

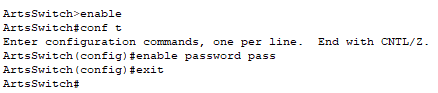


Fonte: Os autores.

* 1. CONFIGURAÇÃO DO FIREWALL

A primeira medida de proteção (e a mais simples) foi criar uma senha para executar o comando *enable* em switches e roteadores. A senha usada em todas as entidades foi *pass*, mas diferentes senhas poderiam ser usadas para diferentes entidades:

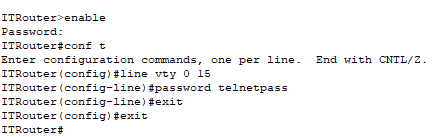
**Figura 18** – Criação de senha para o comando *enable* no switch do andar de Artes do departamento de estudantes.



Fonte: Os autores.

Uma senha foi criada em todas as linhas usadas para conexões Telnet em todos os roteadores e switches da rede. A senha usada foi *telnetpass*:

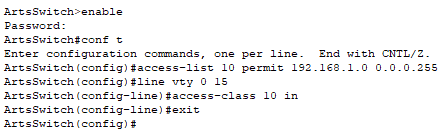
**Figura 19** – Criação de uma senha para todas as linhas usadas para conexões Telnet.



Fonte: Os autores.

Uma lista de acesso padrão de ID 10 foi criada em todos os roteadores e switches para somente aceitar requisições Telnet de endereços IPs que pertencem ao departamento de TI (ou seja, que possuem endereços IPs que casam com o padrão 192.168.1.0/24):

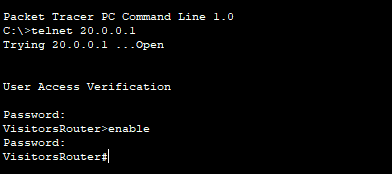
**Figura 20** – Criação da lista de acesso para requisições Telnet no switch do andar de Artes do departamento de estudantes.



Fonte: Os autores.

Antes da regra ser criada, qualquer computador poderia obter acesso remoto à qualquer roteador ou switch da rede, desde que soubesse a senha do comando *enable* e a senha Telnet, como mostra a figura:

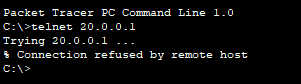
**Figura 21** – Computador do departamento de visitantes obtendo acesso ao roteador de visitantes.



Fonte: Os autores.

Após a lista de acesso ser criada e configurada, qualquer tentaiva de conexão Telnet que não tenha o departamento de TI como origem é recusada pelo roteador/switch:

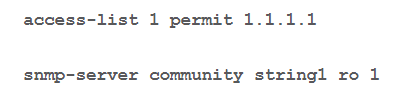
**Figura 22** – Computador do departamento de visitantes tendo o acesso Telnet negado pelo roteador de visitantes.



Fonte: Os autores.

Por último, também tentamos criar uma lista de acesso que proíbe requisições SNMP que não vieram do departamento de TI. Usamos como referência uma documentação da Cisco que ensinava à aplicar listas de acesso com o SNMP:

**Figura 23** – Criação e configuração de uma lista de acesso para requisições SNMP.



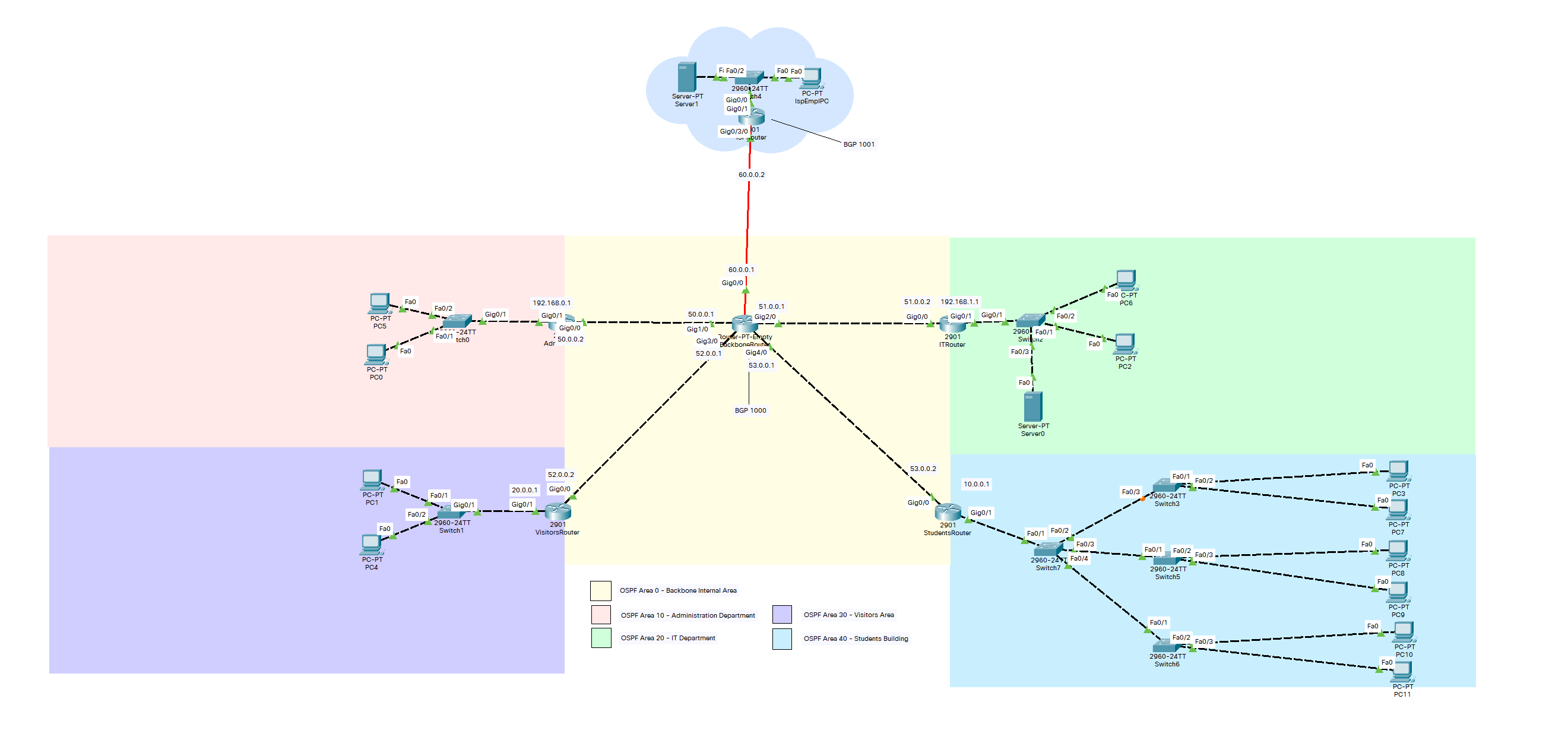
Fonte: Protegendo o Protocolo de Gerenciamento de Rede Simples - Cisco. Acessível em https://www.cisco.com/c/pt\_br/support/docs/ip/simple-network-management-protocol-snmp/20370-snmpsecurity-20370.html.

Porém, os comandos que foram documentados pela Cisco simplesmente não funcionam atualmente no Packet Tracer. Após pesquisar mais sobre, descobrimos que vários outros usuários estão com o mesmo problema. Supostamente, os comandos funcionam em roteadores e switches Cisco reais, mas não no Packet Tracer.

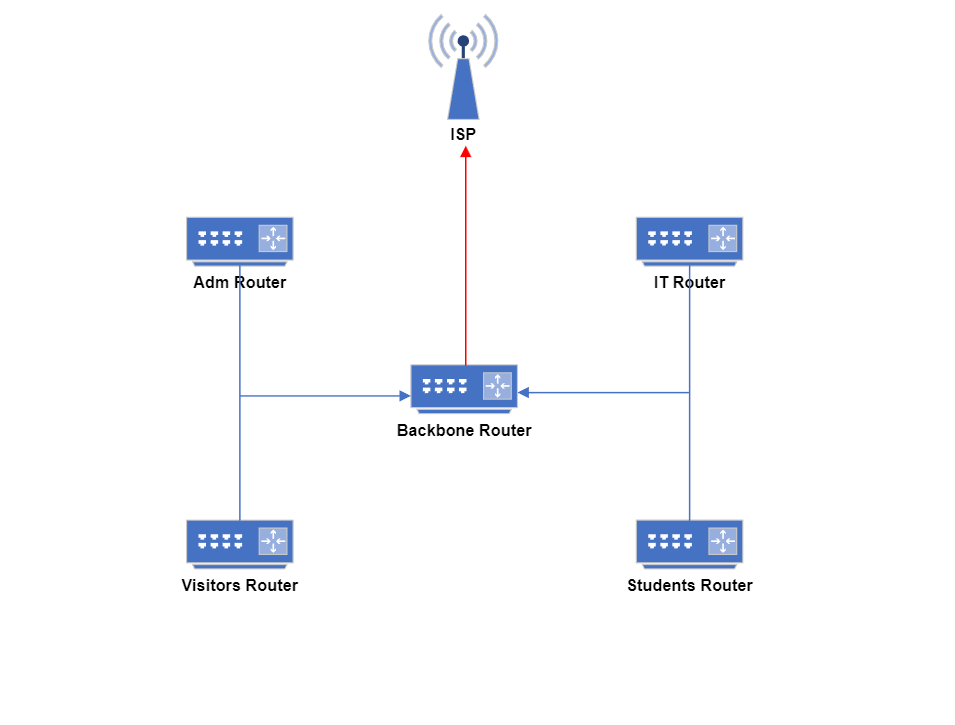
1. **CONCLUSÃO**

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed ut purus rutrum, tempus erat nec, ullamcorper est. Proin ut lacinia augue, interdum pharetra mi. Class aptent taciti sociosqu ad litora.

# **ANEXO A – TOPOLOGIA FINAL DA REDE**



# **ANEXO B – DIAGRAMA DE REDE**



<https://univali-my.sharepoint.com/:u:/g/personal/rohling_edu_univali_br/EY_tf6wTtOlMtg_DWKFIweMBlN97IcjNEkXq3LcLTQisxQ>

# **ANEXO C – TABELAS DE CUSTOS**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Dispositivos** | **Referência** | **Quantidade** | **Preço Unitário** | **Total Parcial** |
| Roteador Cisco 2901 | https://www.encurtador.com.br/joHQX | 5 | R$ 3.584,50 | R$ 17.922,50 |
| Módulo 1GE-SFP-CU (Gigabit Ethernet e Fiber) | https://www.encurtador.com.br/cnFI0 | 2 | R$ 692,50 | R$ 1.385,00 |
| Cabo de Rede Cat5e (vendido por metro) | https://www.encurtador.com.br/lmIU4 | X | R$ 2,65 |  |
| Servidor HP ML30 16GB | 1TB | https://www.encurtador.com.br/dopEN | 1 | R$ 7.040,00 | R$ 7.040,00 |
|  |  |  |  |  |
|  |  |  |  |  |
| **TOTAL** | | | | **R$ 0,00** |

|  |  |  |
| --- | --- | --- |
| **Serviços** | **Referência** | **Custo** |
| Custo de implementação (por hora) (\*) |  | R$ 60,00 por hora (para cada integrante)  R$ 120,00 \* 160 horas  **R$ 19.200,00** |
| Funcionário: Analista de Suporte de Rede | https://www.vagas.com.br/cargo/analista-de-suporte-de-rede | **R$ 3.136,00 / mês** |
| Internet (1Gbps) | https://unifique.com.br/para-empresas/internet-fibra-optica-empresarial | **R$ 399,90 / mês** |
|  |  |  |

*(\*) Considerou-se uma jornada de trabalho de 8 horas diárias, 5 dias por semana, durante 4 semanas.*