



Atividade Avaliativa de Redes de Computadores

Samuel de Oliveira Ribeiro

1. Roteamento estático consiste em utilizar uma rota pré definida e configurada manualmente pelo administrador da rede. Esta forma de roteamento tem problemas quando há uma alteração na topologia da rede, caso isso ocorra o administrador deverá avaliar novamente toda a rede e redefini-las se necessário.

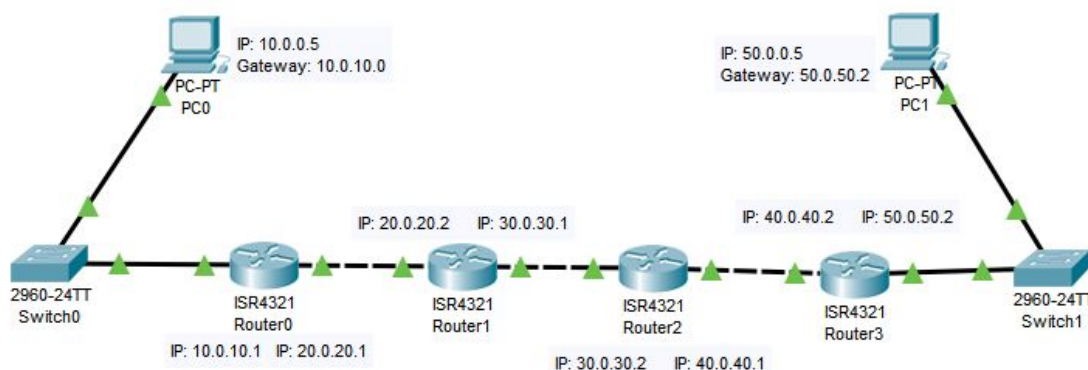


Figura 01: Comunicação entre o PC0 e PC1 por meio de roteamento estático.

Na figura 01 mostra uma topologia de rede com roteamento estático definido para haver a comunicação entre o Pc0 e o Pc1, da forma que foi definido há a comunicação de envio e recepção de pacotes. Para que este roteamento estático seja definido foi definido os endereços IP para cada roteador sendo que cada interface ligada a outro roteador estão numa mesma sub-rede, para assim manter uma conexão, além de ser definido os endereços IPs para o Pc0 e o Pc1 com o endereço IP do “seu” roteador como Gateway.

```
Gateway of last resort is not set

S   10.0.0.0/8 [1/0] via 20.0.20.1
S   20.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C   20.0.0.0/8 is directly connected, GigabitEthernet0/0/0
L   20.0.20.2/32 is directly connected, GigabitEthernet0/0/0
S   30.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C   30.0.0.0/8 is directly connected, GigabitEthernet0/0/1
L   30.0.30.1/32 is directly connected, GigabitEthernet0/0/1
S   50.0.0.0/8 [1/0] via 30.0.30.2

Router#
```

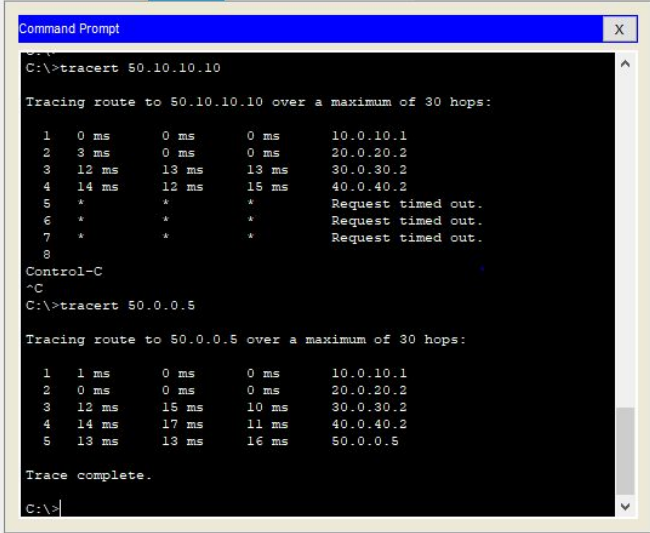
Figura 02: Rotas definidas no roteador 01.

Até então esta rede funciona de forma não estática, para isso ocorrer foi definido, para cada roteador, qual será a interface de destino ao receber um pacote com determinado IP dentro a máscara de rede especificada. A Figura 02 mostra duas definições de rotas, a primeira é a rota *10.0.0.0/8 via 20.0.20.1*, ou seja, todos pacotes destinados para um endereço IP iniciado em '10' serão direcionados para a interface 20.0.20.1 que é a interface do roteador 0. O processo inverso é feito para a transmissão no sentido contrário, sendo todos os pacotes destinados para um IP iniciado em '50' serão direcionados para a interface de rede 30.0.30.2.

2. Traceroute é uma ferramenta de diagnóstico que rastreia a rota de um pacote através de uma rede de computadores que utiliza os protocolos IP e o ICMP. O dispositivo envia uma sequência de datagramas de Protocolo UDP para um endereço de porta inválido no host remoto.

Seu funcionamento está baseado no uso do campo Time to Live (TTL) do cabeçalho IP destinado a limitar o tempo de vida dele. Este valor é decrementado a cada vez que o pacote é encaminhado por um roteador. Ao atingir o valor zero o pacote é descartado e o originador é alertado por uma mensagem ICMP *TIME_EXCEEDED*. Através da manipulação do campo TTL de uma série de datagramas UDP é possível receber esta mensagem de cada um dos roteadores no caminho do pacote.

Outras três mensagens de UDP são agora enviadas, cada uma com o valor de TTL definido como 2, que faz com que o segundo roteador retorne ICMP *TIME_EXCEEDED*. Este processo continua até que os pacotes realmente alcancem o outro destino. Desde que estes datagramas estão tentando alcançar uma porta inválida no host de destino, os mensagens inalcançáveis da porta ICMP são retornados, indicando uma porta inalcançável; este sinais de evento o programa Traceroute que está terminado.



```
Command Prompt
C:\>tracert 50.10.10.10

Tracing route to 50.10.10.10 over a maximum of 30 hops:

  0  0 ms    0 ms    0 ms    10.0.10.1
  1  3 ms    0 ms    0 ms    20.0.20.2
  2 12 ms   13 ms   13 ms    30.0.30.2
  3 14 ms   12 ms   15 ms    40.0.40.2
  4 *      *      *      Request timed out.
  5 *      *      *      Request timed out.
  6 *      *      *      Request timed out.
  7 *      *      *      Request timed out.
  8
Control-C
^C
C:\>tracert 50.0.0.5

Tracing route to 50.0.0.5 over a maximum of 30 hops:

  0  1 ms    0 ms    0 ms    10.0.10.1
  1  0 ms    0 ms    0 ms    20.0.20.2
  2 12 ms   15 ms   10 ms    30.0.30.2
  3 14 ms   17 ms   11 ms    40.0.40.2
  4 13 ms   13 ms   16 ms    50.0.0.5

Trace complete.

C:\>
```

Figura 03: Rotas geradas pelo comando tracert na rede apresentada na Figura 01.

Na figura 02 foi feito um teste do comando tracert no CPT. No primeiro teste foi utilizado um IP existente na rede, sendo assim o envio de pacotes foi finalizado quando o IP destino foi atingido com TTL igual a 1. Já no segundo teste foi utilizado um IP inexistente na rede (Figura 01), sendo assim os pacotes iriam parar de ser transmitido quando atingisse o limite de 30 hops (Foi enviado 30 pacotes com TTL iniciando de 1 e terminando em 30, sempre enviando o pacote de forma incremental, este valor é variável). Cada saída do comando refere-se aos endereços dos roteadores da rota que foi definida anteriormente.

3. A Tradução de Endereço de Rede ou NAT refere-se a um processo específico que envolve remapear um único endereço IP em outro endereço IP, através da alteração das informações de rede e informações de endereço encontradas no cabeçalho IP dos pacotes de dados. As redes locais têm vários endereços IP privados que pertencem a dispositivos específicos na rede, através de um sistema NAT esses endereços privados são traduzidos em um endereço IP público quando são enviadas solicitações de saída dos dispositivos de rede para a Internet. Um processo inverso ocorre quando os dados recebidos, geralmente como uma resposta a solicitações específicas, são enviados para uma rede local. Neste caso, o NAT altera o endereço IP público para o endereço IP privado do dispositivo específico para o qual o pacote de dados é direcionado. O endereço IP público é usado repetidamente pelo roteador que conecta os computadores à Internet.

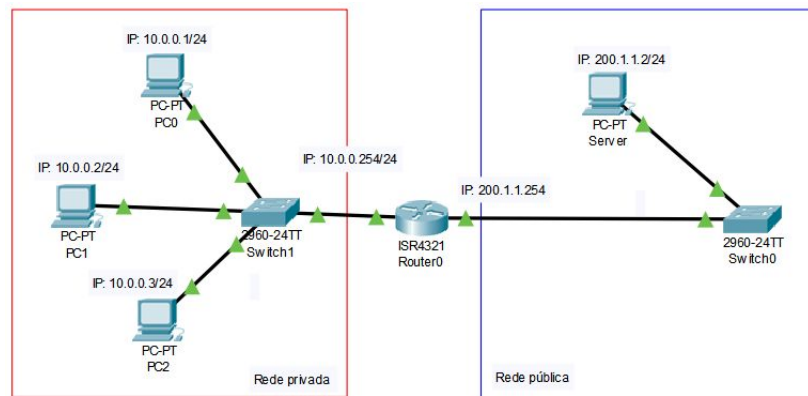


Figura 04: Topologia de rede com o funcionamento do NAT ativo.

Como proposto será configurado o roteador da figura 04 para que ele realize o NAT, possibilitando que haja uma comunicação entre o host0 (10.0.0.0/24) e o server (200.1.1.1) por meio do roteador (200.1.1.254) configurado com o NAT. Já com os endereços IPs configurados corretamente e a topologia de rede definida é feito a configuração do protocolo NAT. No terminal CLI do roteador deve ser configurada a interface de rede Gigabit/Ethernet0/0/0 com apresentados na tabela 01 a seguir.

Comando	Descrição dos comandos
<i>Enable</i>	Muda do modo usuário para o modo de configuração global
<i>configure terminal</i>	Muda do modo privilegiado para o modo de configuração global
<i>ip nat inside source list 1 interface GigabitEthernet0/0/0 overload:</i>	Configura o nat para ser ativo na porta GigabitEthernet0/0/0
<i>access-list 1 permit any</i>	lista de acesso que permite ou nega endereços que utilizarão o processo de nat onde:
<i>interface GigabitEthernet0/0/0</i>	Entra no modo de configuração de interface específica do roteador
<i>ip nat inside</i>	indica de esta interface será uma interface interna no processo de nat
<i>exit</i>	Encerra o modo de configuração
<i>interface GigabitEthernet0/0/1</i>	Modo de configuração da interface de saída
<i>ip nat outside</i>	Indica que a interface selecionada será uma interface externa no processo de nat

Tabela 01: Comandos utilizados para configuração do NAT no Router 0 da figura 04.

Após a execução destes comandos, o nat já estará configurado na rede. As figuras 05 e 06 mostram respectivamente o comando ping entre o host0 e servidor (citados anteriormente) e a execução do comando *sh ip nat translation* que mostra as traduções ativas na tabela nat. Inicialmente a tabela NAT estava vazia, após ser utilizado o comando ping foi feito a tradução dos IPs e o mesmo ficou guardado em cache na tabela conforme mostra a figura 06.

```

Command Prompt

Packet Tracer PC Command Line 1.0
C:\>
C:\>
C:\>ping 200.1.1.2

Pinging 200.1.1.2 with 32 bytes of data:

Reply from 200.1.1.2: bytes=32 time=6ms TTL=127
Reply from 200.1.1.2: bytes=32 time<1ms TTL=127
Reply from 200.1.1.2: bytes=32 time<1ms TTL=127
Reply from 200.1.1.2: bytes=32 time<1ms TTL=127

Ping statistics for 200.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 6ms, Average = 1ms

C:\>

```

Figura 05: Resultado do comando ping entre PC0 e o Server segunda figura 04.

```

Router#
Router#sh ip nat translation
Router#
Router#sh ip nat translation
Pro  Inside global      Inside local      Outside local      Outside global
icmp 10.0.0.254:10       10.0.0.1:10       200.1.1.2:10       200.1.1.2:10
icmp 10.0.0.254:11       10.0.0.1:11       200.1.1.2:11       200.1.1.2:11
icmp 10.0.0.254:12       10.0.0.1:12       200.1.1.2:12       200.1.1.2:12
icmp 10.0.0.254:9        10.0.0.1:9        200.1.1.2:9        200.1.1.2:9

Router#
Router#

```

Figura 06: Tabela nat do roteador segundo a topologia de rede da figura 04.

Vantagens do uso do NAT:

- Ela ajuda a mitigar o esgotamento do espaço de endereçamento IP público global.
- Aumenta o nível de segurança ao ocultar o esquema de endereçamento e a topologia da rede interna.

Desvantagens do uso do NAT:

- Os protocolos de túnel se tornam complicados à medida que o NAT altera os valores nos cabeçalhos dos pacotes, o que afetará as verificações de integridade desses protocolos.
- Uma vez que os endereços internos estão escondidos atrás de um único endereço publicamente acessível, seria impossível para um host externo iniciar a comunicação com um host interno sem uma configuração especial no firewall para permitir isso.

4. Uma sub-rede é uma subdivisão lógica de uma rede IP. A subdivisão de uma rede grande em redes menores resulta num tráfego de rede reduzido e uma melhor performance de rede. Foi definido na rede presente na figura 07 endereços IPs e máscaras de rede para os computadores da mesma para que os seguintes critérios sejam cumpridos: há uma sub-rede vermelha; Há sub-rede azul; não há troca de pacotes entre as sub-redes; todos os PCs podem trocar pacotes com o roteador.

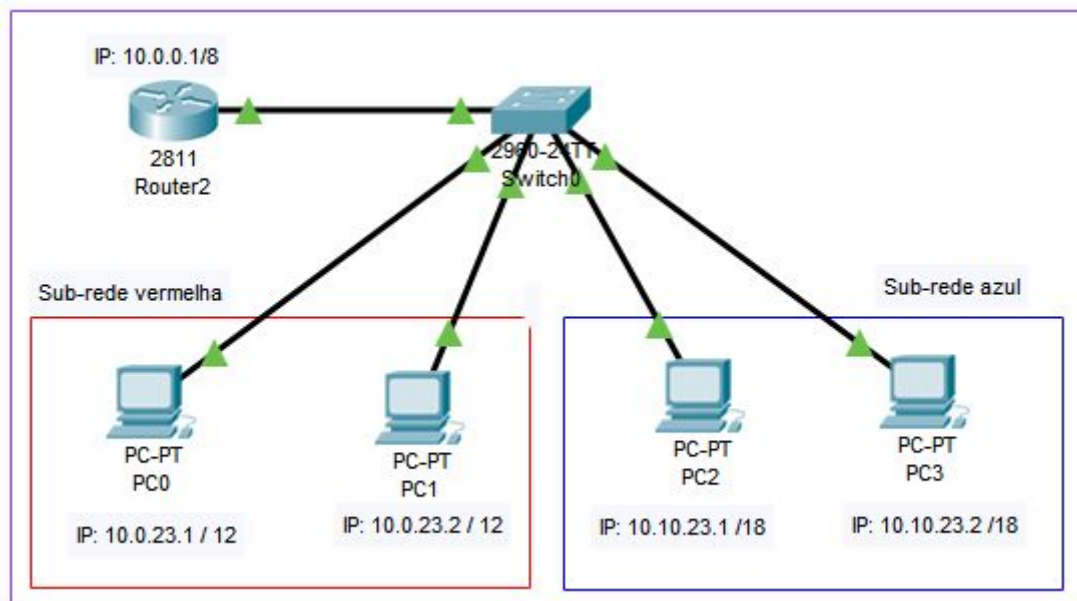


Figura 07: Topologia de rede com uma sub-rede Vermelha e outra sub-rede Azul.

As figuras 08, 09 e 10 mostram respectivamente a resposta do comando ping entre o PC0 e PC1, PC 0 e Router 2 e PC0 e PC2. Como podemos observar foi estabelecido a conexão entre computadores na mesma sub-rede e com o roteador além de não ser possível estabelecer conexão entre PCs em sub-redes diferentes. Isso foi possível por meio da alteração das máscaras de sub-rede. Uma máscara de sub-rede, é um número de 32 bits usado em um IP para separar a parte correspondente à rede pública, à sub-rede e aos hosts.

```
Packet Tracer PC Command Line 1.0
C:\>ping 10.0.23.2

Pinging 10.0.23.2 with 32 bytes of data:

Reply from 10.0.23.2: bytes=32 time<1ms TTL=128
Reply from 10.0.23.2: bytes=32 time<1ms TTL=128
Reply from 10.0.23.2: bytes=32 time<1ms TTL=128
Reply from 10.0.23.2: bytes=32 time=3ms TTL=128

Ping statistics for 10.0.23.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 0ms
```

Figura 08: comando ping entre PC0 e PC1


```

C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Reply from 10.0.0.1: bytes=32 time=1ms TTL=255
Reply from 10.0.0.1: bytes=32 time=3ms TTL=255
Reply from 10.0.0.1: bytes=32 time=2ms TTL=255
Reply from 10.0.0.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 1ms

```

Figura 09: comando ping entre PC0 e Router 2.

```

C:\>ping 10.10.23.1

Pinging 10.10.23.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.10.23.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>

```

Figura 10: comando ping entre PC0 e PC2.

O roteador está com máscara de rede 255.0.0.0 (8 bits), sendo assim todas as suas sub-redes devem ter uma máscara com valor superior ou igual a 8 bits. Para a sub-rede vermelha foi definido uma máscara de sub-rede 255.240.0.0 (12 bits) e para a sub-rede azul foi definido máscara de sub-rede 255.255.192.0 (18 bits). Dessa forma a sub-rede vermelha só envia pacotes para uma rede com máscara X (menor que 12 bits) e que o endereço IP desta máscara X seja igual (Por exemplo, aplicando a máscara do router ao PC 0 os primeiro 8 bits são iguais, sendo assim há uma comunicação entre os mesmos).

O mesmo ocorre para a sub-rede azul. Quando se trata da comunicação entre a sub-rede vermelha e a sub-rede azul não é possível haver trocas de pacotes pois no 12º bit os endereços IPs se diferem e como a menor máscara entre eles é /12 haveria comunicação caso até o 12º bit os IPs fossem iguais, mas não é o que ocorre na rede definida.

5. OSPF é um protocolo de roteamento (Feito para redes com protocolo IP) do tipo link-state, que envia avisos sobre o estado da conexão (link-state advertisements, LSA) a todos os outros roteadores em uma mesma área hierárquica. Informações sobre interfaces ligadas, métrica usada e outras variáveis são incluídas nas LSAs. Ao mesmo tempo em que o roteador OSPF acumula informações sobre o estado do link, ele usa o algoritmo SPF para calcular a menor rota para cada nó.

O algoritmo SPF, mais conhecido com algoritmo de Dijkstra, que visa buscar um caminho mais curto entre os routers da rede com base em algumas métricas definidas. Por ser um protocolo do tipo link-state, o OSPF difere-se do RIP e do IGRP, que são protocolos de roteamento baseados em vetores de distância. Os roteadores que trabalham com algoritmos de vetor de distância, a cada atualização, enviam toda ou parte de suas tabelas de roteamento para seus vizinhos.

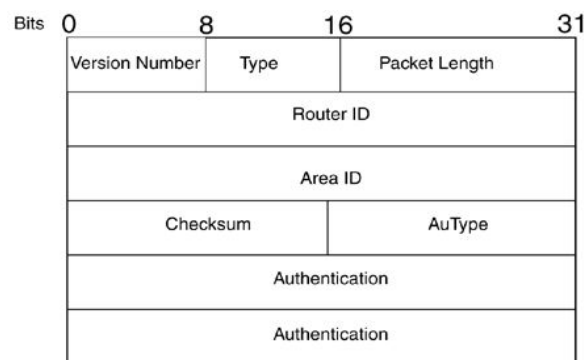


Figura 11: Cabeçalho dos pacotes OSPF.

A Figura 11 contém cabeçalho do protocolo OSPF de 24 octetos definido pela RFC 2328. Sendo eles:

- Versão: Identifica a versão de OSPF utilizada.
- Tipo: Identifica o pacote OSPF como um dos seguinte:
 - i. Hello
 - ii. Database Description
 - iii. Link State Request
 - iv. Link State Update
 - v. Link State Acknowledgment
- Tamanho do pacote: Tamanho do pacote incluindo tamanho deste cabeçalho.
- ID do roteador: Identifica a origem do pacote.
- ID da área: Identifica a que área o pacote pertence. Cada pacote tem apenas uma área associada.
- Checksum: Campo para verificar se houve alterações na transmissão do pacote.
- Tipo de autenticação: Informações sobre a autenticação.
- Dados: Contém informações encapsuladas de camadas superiores

Uma topologia de rede pode ser feita de forma hierárquica, sendo a maior entidade desta topologia nomeada de sistema autônomo (AS), este sistema autônomo é uma coleção de

redes sob uma mesma “administração” e que tem uma estratégia de roteamento comum (Similar a uma vlan). O OSPF é um protocolo de roteamento intra-AS (interior gateway). Um AS pode ser dividido em diversas áreas dentro de uma mesma topologia, essas áreas são formadas por grupos de redes adjacentes e host ligados (Roteadores de borda podem participar de múltiplas áreas).

Os roteadores OSPF criam um banco de dados de topologia de todos os links dentro de sua área e todos os roteadores dentro de uma área terão um banco de dados de topologia idêntico. As atualizações de roteamento entre esses roteadores conterão apenas informações sobre links locais para suas áreas. Limitar o banco de dados de topologia para incluir apenas a área local economiza largura de banda e reduz as cargas da CPU. Para o OSPF funcionar a área 0 deve estar definida para que a mesma seja a área “Backbone”. Na figura 11 a área 0 é o “Backbone” do sistema.

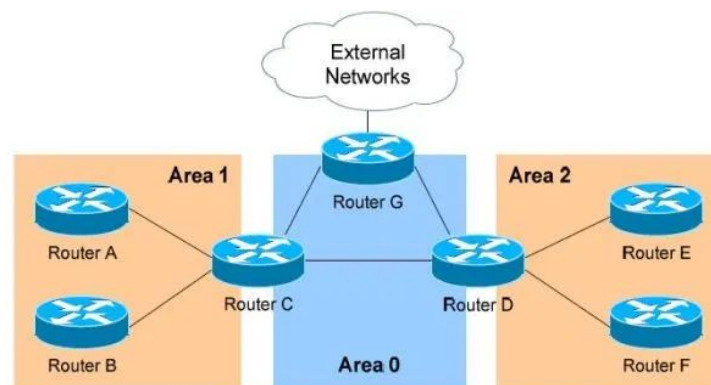


Figura 12: Exemplo de uma topologia de rede utilizando OSPF.

Conforme a figura 12, os roteadores A e B pertencem totalmente a área 1, enquanto enquanto os roteadores E e F pertencem totalmente à área 2. Esses são conhecidos como roteadores internos. O roteador C pertence à área 0 e à área 1, portanto é um roteador de área de borda (ABR). Por ter uma interface na Área 0, também pode ser considerado um roteador de backbone. O mesmo pode ser dito para o roteador D, pois pertence às áreas 0 e 2. Já o roteador G é um roteador de borda de sistema autônomo (ASBR).

Quando o OSPF é ativado todos os roteadores irão gerar pacote LSA, que contém o status dos links FastEthernet (Todos os roteadores da mesma área receberam o pacote). Os roteadores de área de borda de uma rede gerarão LSAs de resumo contendo informações de custos para alcançar a rede de forma que as áreas que o mesmo faz conexão receber pacotes um do outro. Já o ASBR gerarão LSAs que contém rotas para as redes externas da AS (Todos os roteadores recebem este pacote). Os pacotes são enviados na rede quando ocorre uma alteração na mesma ou em intervalos periódicos de 30 minutos.

6. Foi implementado um modelo de rede com OSPF ativo em seus host. Para ativar o OSPF foi preciso, para cada roteador definir suas networks (são as interfaces de rede) juntamente com a área do OSPF que cada interface pertencerá. Este exemplo modelado há apenas uma área com todos os roteadores totalmente pertencentes a ela, sendo assim não há ABR e nem ASBR.

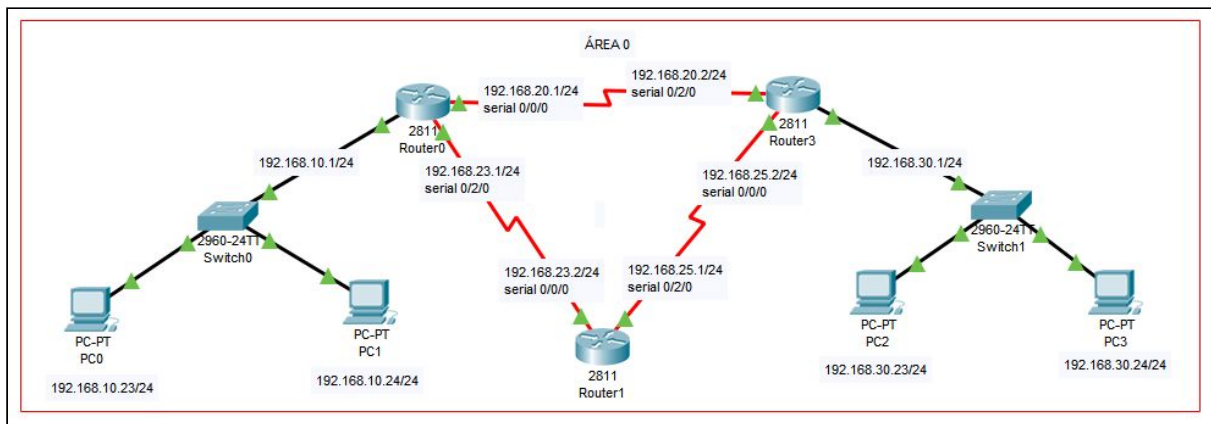


Figura 13: Topologia de rede com protocolo OSPF ativo.

Comando	Descrição dos comandos
<i>Enable</i>	Muda do modo usuário para o modo de configuração global
<i>configure terminal</i>	Muda do modo privilegiado para o modo de configuração global
<i>router ospf 1</i>	Ativa protocolo OSPF
<i>network 192.168.10.0 0.0.0.255 area 0</i>	Define a interface de rede 192.168.10.0/24 na area 0
<i>network 192.168.20.0 0.0.0.255 area 0</i>	Define a interface de rede 192.168.10.0/24 na area 0
<i>network 192.168.23.0 0.0.0.255 area 0</i>	Define a interface de rede 192.168.10.0/24 na area 0
<i>copy running-config startup-config</i>	Salvando alterações na configuração.

Tabela 02: Comandos utilizados para configuração do OSPF no Router0 da figura 13.

Para definir as configurações do OSPF na topologia de rede da figura 13 foi preciso, para cada roteador, definir qual área cada interface de rede estará. A tabela 02 exemplifica esta configuração para o Router0: Primeiro deve-se acessar o terminal CLI do roteador no CPT; em seguida é habilitado modo de configuração mudando também os privilégios do usuário; é ativado o protocolo OSPF e em seguida é definido as áreas de cada interface de rede; ao finalizar deve salvar as alterações no roteador e repetir o processo para os demais roteadores.

Event List				
Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC1	ICMP
	0.001	PC1	Switch0	ICMP
	0.002	Switch0	Router0	ICMP
	0.003	Router0	Router3	ICMP
	0.004	Router3	Switch1	ICMP
	0.005	Switch1	PC3	ICMP
	0.006	PC3	Switch1	ICMP
	0.007	Switch1	Router3	ICMP
	0.008	Router3	Router0	ICMP
	0.009	Router0	Switch0	ICMP
	0.010	Switch0	PC1	ICMP
	0.236	--	Router1	OSPF
	0.237	Router1	Router0	OSPF
	0.346	--	Router1	OSPF
	0.347	Router1	Router3	OSPF

Figura 14: Simulação de envio de pacotes entre PC1 e PC3 segundo topologia da figura 13.

At Device: Router0 Source: Router1 Destination: 224.0.0.5	
In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer 3: IP Header Src. IP: 192.168.23.2, Dest. IP: 224.0.0.5 OSPF HELLO	Layer3
Layer 2: HDLC Frame HDLC	Layer2
Layer 1: Port Serial0/2/0	Layer1

Figura 15: Informação enviada pelo OSPF contido no Layer 3 - In Layers.

Quando um pacote termina de ser transmitido o protocolo OSPF é ativado em todos os roteadores, como todos os eles estão numa mesma área eles iram enviar e receber pacotes LSA do tipo “HELLO” (Figura 15) para manter a conexão estabelecida com seus vizinhos e também poder identificar se todos os outros roteadores ainda estão funcionando na rede. Cada roteador envia periodicamente um LSA para fornecer informação as adjacências de um roteador ou para informar aos outros quando o estado de um roteador se altera.

Comparando as adjacências estabelecidas com os link states, roteadores com falhas podem ser detectados rapidamente, e a topologia da rede pode ser alterada apropriadamente. Com a base topológica gerada por meio dos LSAs, cada roteador calcula uma árvore de menores rotas, com ele próprio como raiz. A árvore de menores rotas, por sua vez, torna-se a tabela de roteamento.