Segundo Trabalho Prático de Redes de Computadores

Diego S. Cintra, Jainor Cunha

4 de dezembro de 2014

Sumário

Resumo

Nos foi proposta a implementação de um projeto de uma rede, distribuição de faixas IP, tabelas de roteamento e políticas de segurança para uma determinada empresa, através apenas de uma breve descrição dessa rede, utilizando do software Cisco Packet Tracer. A rede deve operar de maneira a permitir com que, dada algumas restrições, estações de uma determinada sub-rede possam se comunicar com as outras, e vice-versa. Também deve-se embutir, através ou do roteamento estático ou algum protocolo de roteamento, o balanceamento de carga entre os enlaces que conectam os dois estados aonde a empresa possui filiais. Essas requisições visam expandir nosso conhecimento a cerca das principais decisões de projeto a serem tomadas ao se projetar uma rede, bem como suas dificuldades.

1 Introdução

O cenário para implementação se dá a seguir. Uma empresa possui vários escritórios em São Paulo de Mato Grosso do Sul, e deseja interconectá-los com uma topologia de rede apropriada, que explicitaremos a seguir. Em São Paulo, temos o servidor HTTP e cinco máquinas de administração, bem como o link com a Internet. Em Campinas há 75 estações de trabalho e mais 25 sem fio. Santo André e São José possuem 50 estações cada, e eles estão conectados à SP via Fast Ethernet – em Campinas, a conexão se dá por fibra ótica. Já para Mato Grosso do Sul, temos duas máquinas administrativas mais os servidores de e-mail e FTP da empresa. Para Campo Grande, tem-se 40 estações, e em Três Lagoas temos 20 máquinas com um servidor local. Com base nessa topologia, foi-nos proposto a implementação de uma topologia de rede que se adequasse a tais requisições, além de definir as distribuições de faixas de endereço, tipos de roteamento e definições de políticas de segurança através do uso de firewalls. São esses tópicos que serão abordados ao longo desse relatório.

2 Desenvolvimento

Primeiramente, definimos qual seria a topologia em questão. Para facilitar a visualização e definição dessa, utilizamos o programa Cisco Packet Tracer, que é muito popular para desenvolvimento de projetos de redes. Em São Paulo, temos três divisões: Santo André, que contém 50 estações de trabalho; Campinas, que contém 75 estações mais 25 sem fio; e São José dos Campos, com 50 estações de trabalho, ficou encarregada de conter o servidor HTTP da empresa. O link com a Internet se dá a partir do roteador de São Paulo (ou seja, um roteador de borda do sistema autônomo). Já em Mato Grosso do Sul tem-se 40 estações em Campo Grande e em Três Lagoas temos 20 máquinas e um servidor local. Uma rede separada foi criada para armazenar o servidor de e-mail e 2 máquinas administrativas. No desenvolvimento do projeto, logicamente condensou-se a quantidade de máquinas existentes para cada divisão, utilizando o auxílio de uma nota que identifica quantos hosts estão sendo representados ali (como, por exemplo, a nota “x 24”, que representa 24 máquinas). Dois roteadores “principais”, representando os estados, foram alocados para realizar a comunicação entre todas as sub-redes da empresa; para cada sub-rede, um roteador também

foi definido. A internet foi representada com o elemento "Host exterior ao AS", sendo interligada via um roteador simples.

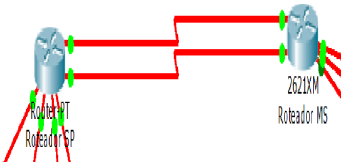
2.1 Sub-redes

Passado o projeto da rede, o próximo passo a ser realizado era o esquema de endereçamento IP para tal projeto. A faixa atribuída à empresa pelo Registro.br foi 200.10.120.0 com máscara 255.255.254.0, portanto a distribuição de endereços IP se deu da seguinte maneira:

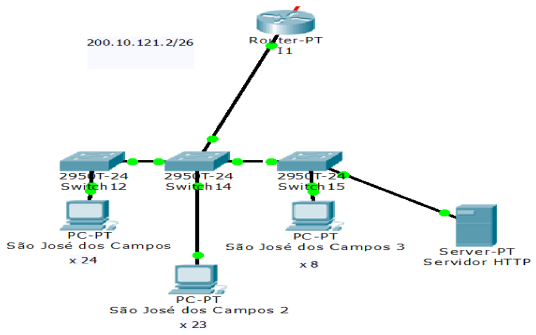
- A sub-rede 200.10.120.0 com máscara 255.255.255.128 foi atribuída a Campinas;
- A sub-rede 200.10.121.0 com máscara 255.255.255.192 foi atribuída a São José dos Campos;
- A sub-rede 200.10.121.64 com máscara 255.255.255.192 foi atribuída a Santo André;
- A sub-rede 200.10.120.248 com máscara 255.255.255.248 foi atribuída a zona que contém as duas máquinas administrativas e os servidores de e-mail e FTP da empresa;
- A sub-rede 200.10.121.128 com máscara 255.255.255.192 foi atribuída a Campo Grande e
- a sub-rede 200.10.121.224 com máscara 255.255.255.224 foi atribuída a Três Lagoas.

2.2 Roteadores

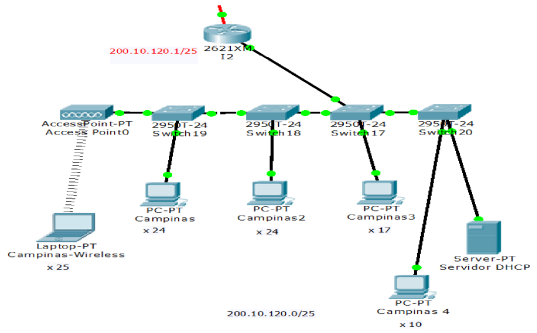
Entre os roteadores que interligam os dois estados, como requisitado na descrição do trabalho, definimos o endereço 200.10.120.222 com máscara 255.255.255.252 para a interface do roteador de SP que está conectado com o de MS (esse possuindo largura de banda de 1.544 Mbps), com endereço 200.10.120.221 e máscara 255.255.255.252. Visto que há dois enlaces seriais, para o segundo definimos os endereços 200.10.120.217 (do roteador de SP) e 200.10.121.218 (de MS) – conexão essa identificada com o *bandwidth* 512 Kbps -, todos com a máscara 255.255.255.252. Para a atribuição de endereços IP para os demais roteadores, denominamo-os todos com o prefixo "I", de intermediário. Antes de definirmos quais endereços foram atribuídos a quais roteadores, recomenda-se que o leitor abra o arquivo de projeto de rede enquanto realiza a leitura deste documento. A interligação entre os roteadores SP e MS se parece com isso:



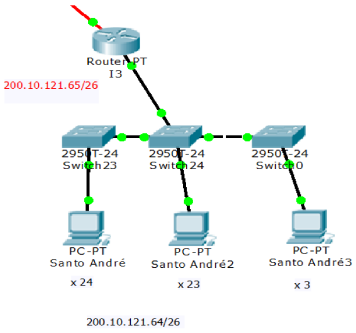
Para o roteador “I1”, definimos, para sua conexão com o roteador de São Paulo (via interface “serial 2/0”), o endereço 200.10.121.241 (com máscara, assim como requisitado na descrição desse trabalho, 255.255.255.252), aonde o último recebeu nessa interface o endereço 200.10.121.242. Para sua conexão com a sub-rede de São José dos Campos, a interface “fastEthernet 0/0” recebeu o endereço 200.10.121.2, com máscara 255.255.255.192. Endereços estáticos foram associados às máquinas dessa cidade, entretanto, é importante citar o endereço do servidor HTTP – 200.10.121.6. O roteador I1 se parece com isso:



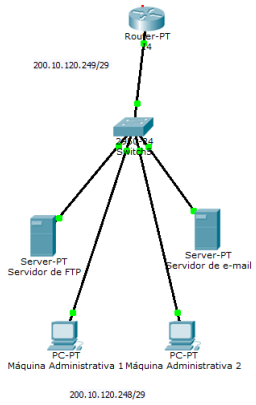
Em “I2”, a interface “fastEthernet 1/0”, que é conectada via fibra ótica, recebeu o endereço 200.10.120.198, que a interliga com o roteador de SP (com IP 200.10.120.197). Já para sua conexão com Campinas, a interface “fastEthernet 0/0” foi utilizada, com endereço definido como 200.10.120.1 e máscara 255.255.255.128. Nessa sub-rede, é importante notar que, devido à requisição de haverem pelo menos 25 estações de rede sem fio, utilizou-se de um access point para realizar-se essa conexão, e dado a natureza de estações wireless, um servidor DHCP foi implantado aqui, tendo definido em sua pool “serverPool” o gateway default 200.10.120.1, o endereço IP inicial como 200.10.120.75 e o número máximo de usuários como 50. O roteador I2 se parece com isso:



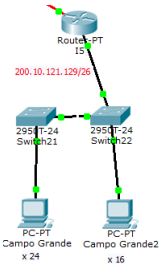
Na última das divisões de SP, temos “I3”, definido em sua interface com o roteador de São Paulo (através de “serial 2/0”) o endereço 200.10.120.202 (no fim deste enlace foi dado o IP 200.10.120.201). Para a sub-rede de Santo André utilizou-se do endereço 200.10.121.65, com máscara 255.255.255.192. O roteador I3 se parece com isso:



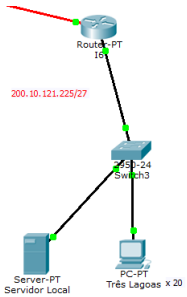
Para Mato Grosso do Sul, como havíamos previamente mencionado, decorreu-se da necessidade de definir uma sub-rede auxiliar, que conteria somente os servidores e as máquinas administrativas. Apesar de poder alocá-lo somente ao roteador de Mato Grosso do Sul, optamos por definir um roteador próprio a essa zona, por questões de padronização (visto que todas as outra máquinas também são segregadas por roteadores internos). O "I4" contém, em seu enlace com o roteador de MS (na interface "serial 2/0") o endereço 200.10.120.206, e o outro roteador ao fim do enlace recebeu 200.10.120.205. Na interface que o conecta a sub-rede que define a zona dos servidores, temos (via "fastEthernet 0/0") o endereço 200.10.120.249, com a mesma máscara da sub-rede (255.255.255.248). O roteador I4 se parece com isso:



Na cidade de Campo Grande encontramos o roteador "I5", conectado com o roteador de MS via "serial 2/0" e com endereço 200.10.120.210 (no fim do enlace tem-se o endereço 200.10.120.209). Para a interface que o conecta-o a sub-rede da cidade, o endereço 200.10.121.129 foi atribuído para "fastEthernet 0/0". O roteador I5 se parece com isso:



Por fim, em Três Lagoas, a conexão de "I6" com o roteador de MS é dada pelo endereço 200.10.120.214 e via "serial 2/0"; SP possui o IP 200.10.120.213. Para "fastEthernet 0/0", que o comunica com as estações de Três Lagoas, o endereço 200.10.121.225 foi atribuído. O roteador I6 se parece com isso:



2.3 Tabelas de Roteamento

Agora deve-se definir as tabelas de roteamento para cada um dos roteadores implantados. Por questões de simplicidade, todos os roteadores tiveram suas tabelas de roteamento preenchidas de maneira estática; de maneira a simplificar ainda mais, os roteadores I1, I2, I3, I4, I5 e I6 tiveram todos apenas duas entradas em suas tabelas: uma que permite com que o roteamento direto (isto é, entre o roteador e o host) seja realizado e a outra que define a rota padrão (default) de quaisquer pacotes que não sejam endereçados àquela rede. Para os roteadores I1, I2 e I3, essa rota definiu como próximo roteador o de SP, ao passo que I4, I5 e I6 tiveram definidos como próximo hop o roteador de Campo Grande.

Intuitivamente, sabe-se que a maior quantidade de entradas de tabela de roteamento ficou entre os roteadores de São Paulo e Mato Grosso do Sul. Para facilitar ao leitor, vamos definir as tabelas desses abaixo, tendo como endereço de destino o IP para qual o datagrama está sendo encaminhado, a máscara associada, o próximo gateway e qual das interfaces faz o encaminhamento. Comecemos pelo roteador de SP:

Endereço de Destino	Máscara Associada	Próximo *Gateway*	Interface
200.10.120.248	255.255.255.248	200.10.120.221	Serial 8/0
200.10.121.224	255.255.255.224	200.10.120.221	Serial 8/0
200.10.121.128	255.255.255.192	200.10.120.218	Serial 3/0
200.10.121.0	255.255.255.192	200.10.121.241	Serial 6/0
200.10.120.0	255.255.255.128	200.10.120.198	Fast 4/0
200.10.121.64	255.255.255.192	200.10.120.202	Serial 2/0
0.0.0.0	0.0.0.0	200.10.121.194	Serial 7/0

Para o roteador de MS, tem-se:

Endereço de Destino	Máscara Associada	Próximo *Gateway*	Interface
200.10.120.248	255.255.255.248	200.10.120.206	Serial 1/0
200.10.121.224	255.255.255.224	200.10.120.214	Serial 1/1
200.10.121.64	255.255.255.192	200.10.120.217	Serial 1/3
200.10.121.128	255.255.255.192	200.10.120.210	Serial 1/2
200.10.121.0	255.255.255.192	200.10.120.217	Serial 1/3
200.10.120.0	255.255.255.128	200.10.120.217	Serial 1/3
0.0.0.0	0.0.0.0	200.10.120.217	Serial 1/3

2.4 Políticas de Segurança

Após a definição das tabelas de roteamento, o próximo passo foi definir quais roteadores teriam atribuídas as políticas de segurança definidas pela a empresa, que são parafraseadas a seguir:

- Usuários da rede Laboratório de Três Lagoas não podem acessar qualquer outra rede onde tenha servidores;
- Somente os usuários do Laboratório podem acessar seu servidor local;
- Usuários da rede de Santo André e São José não podem acessar o servidor FTP que está em MS;
- Usuários de todas as redes (exceto Lab) podem acessar o servidor de correio que está em MS;
- Somente os usuários de SP e suas divisões, podem acessar o servidor HTTP.

Para a realização de tais políticas, adotamos a utilização das ACLs estendidas, introduzidas no Cisco IOS Software Release 8.3, cuja sintaxe é definida abaixo:

access-list *<número da lista>* {deny | permit} [*protocolo da camada de rede ou transporte:* ip|udp|tcp|...] [*endereço da origem*] [*endereço de destino*] [*nº da porta* ou opções]

Com isso, alguns roteadores foram selecionados para cobrir as restrições supracitadas. Como o roteador "I6" se localiza como o primeiro hop da rede de Três Lagoas, ficou delegado a ele a filtragem de pacotes para impedir com que outras estações de diferentes redes tivessem acesso ao servidor local e garantir

com que as estações daí só pudessem se comunicar com as sub-redes de Campo Grande e Santo André, que são as únicas que não possuem servidores (o acesso a redes com servidores é bloqueado às máquinas de Três Lagoas). Portanto, criamos uma access-list de identificador 121 para a interface serial 2/0, com os seguintes comandos:

1. 121 permit ip 200.10.121.224 0.0.0.31 200.10.121.128
2. access-list 121 permit ip 200.10.121.224 0.0.0.31 200.10.121.64
3. access-list 121 deny ip 200.10.121.226 0.0.0.0 200.10.120.0 0.0
4. access-list 121 permit ip 200.10.121.226 0.0.0.0 any
5. access-list 121 deny ip 200.10.121.224 0.0.0.31 200.10.120.0 0.0.1.255
6. interface s 2/0
7. ip access-group 121 out

Isso garantiu com que Três Lagoas só pudesse se comunicar com redes que não possuam servidores. Para negar o acesso de qualquer outra estação ao servidor local, na interface "fastEthernet 0/0", definiu-se a seguinte sequência de comandos:

1. access-list 114 deny ip 200.10.120.0 0.0.1.255 200.10.121.226 0.0.0.0
2. access-list 114 permit ip any 200.10.121.224 0.0.0.31
3. interface f 0/0
4. ip access-group 114 out

A próxima restrição era a de bloquear o acesso de quem está em São José dos Campos e Santo André ao servidor FTP de MS. Portanto, para os roteadores I1 e I3 foram implementadas Access Control Lists (com identificadores 106 e 105, respectivamente) que garantem que o acesso de qualquer estação contida na sub-rede em questão não possa se comunicar com tal servidor. Abaixo, a implementação das ACLs, para I3 e I1, respectivamente:

1. access-list 105 deny ip any 200.10.120.251 0.0.0.0
2. access-list 105 permit ip any any
3. interface s 2/0
4. ip access-group 105 out
5. access-list 106 permit ip 200.10.121.6 0.0.0.65 any
6. access-list 106 deny ip any 200.10.120.251 0.0.0.0
7. access-list 106 permit ip any any
8. interface s 2/0
9. ip access-group 106 out

A penúltima regra explicita que todos, com exceção das estações de Três Lagoas, podem acessar o servidor de e-mail. Dado que somente uma sub-rede deve ser excluída (visto que ninguém pode se comunicar com o servidor local de Três Lagoas também), em I4 definiu-se a restrição de acesso de qualquer estação daí para a sub-rede dos servidores, dada pelos comandos abaixo:

1. access-list 107 deny ip 200.10.121.224 0.0.0.31 200.10.120.253 0.0.0.0
2. access-list 107 deny ip 200.10.121.224 0.0.0.31 200.10.120.251 0.0.0.0
3. access-list 107 permit ip any any
4. interface s 2/0
5. ip access-group 107 out

Por fim, a última regra estabelece que somente os usuários de São Paulo podem acesssar o servidor HTTP. Contido pela sub-rede do roteador I1, logicamente foi a esse que se atribuiu a responsabilidade de filtrar pacotes de MS que indevidamente tentassem accessar o servidor Web:

1. access-list 108 deny ip 200.10.120.248 0.0.0.7 200.10.121.6 0.0.0.0
2. access-list 108 deny ip 200.10.121.128 0.0.0.63 200.10.121.6 0.0.0.0
3. access-list 108 deny ip 200.10.121.224 0.0.0.31 200.10.121.6 0.0.0.0
4. access-list 108 deny ip 200.10.121.193 0.0.0.3 200.10.121.6 0.0.0.0
5. access-list 108 permit ip any any
6. interface s 2/0
7. ip access-group 108 in

Após isto, todos os passos requeridos por essa empresa foram cumpridos.

3 Experimentos e Resultados

Sendo uma rede bastante simplificada, as definições de projeto, distribuição de endereços IP, roteamento e regras de filtragem puderam ser feitas logo de imediato. O software utilizado na simulação do projeto por vezes nos enganou, devido a seu realismo na simulação definir, quase sempre, falhas na primeira vez que hosts tentam se comunicar; porém, logo esse realismo pôde ser entendido. Alguns problemas, a princípio, foram encontrados na comunicação entre as duas redes de diferentes estados, devido a uma má distribuição das faixas de IP. Porém, após o reajuste desses endereços, o roteamento agiu de maneira correta, e as ACLs foram rapidamente implementadas logo em seguida, funcionando de maneira correta e funcional.

4 Conclusão

Após a realização desse trabalho, pudemos entender um pouco mais como se dá a implementação de uma topologia de rede, desde seu alicerce – tomando decisões de projeto adequadas – até a implementação de tabelas de roteamento e filtros de acesso. Pudemos também entender melhor quais são as principais dificuldades envolvidas nesse processo.

Fomos capazes de abstrair, no desenvolvimento desse trabalho, sobre a construção de uma topologia de rede e definição de endereços IP e o quanto de cuidado devemos ter ao implementar tais requisições. Após seu término, estamos aptos, na medida do possível, a projetar uma topologia de rede através apenas de informações fornecidas.

5 Referências

- Firewalls. (2014) - Slide disponível no EAD da disciplina de Redes de Computadores
- Configuração de ACLs. (2014) - Slide disponível no EAD da disciplina de Redes de Computadores