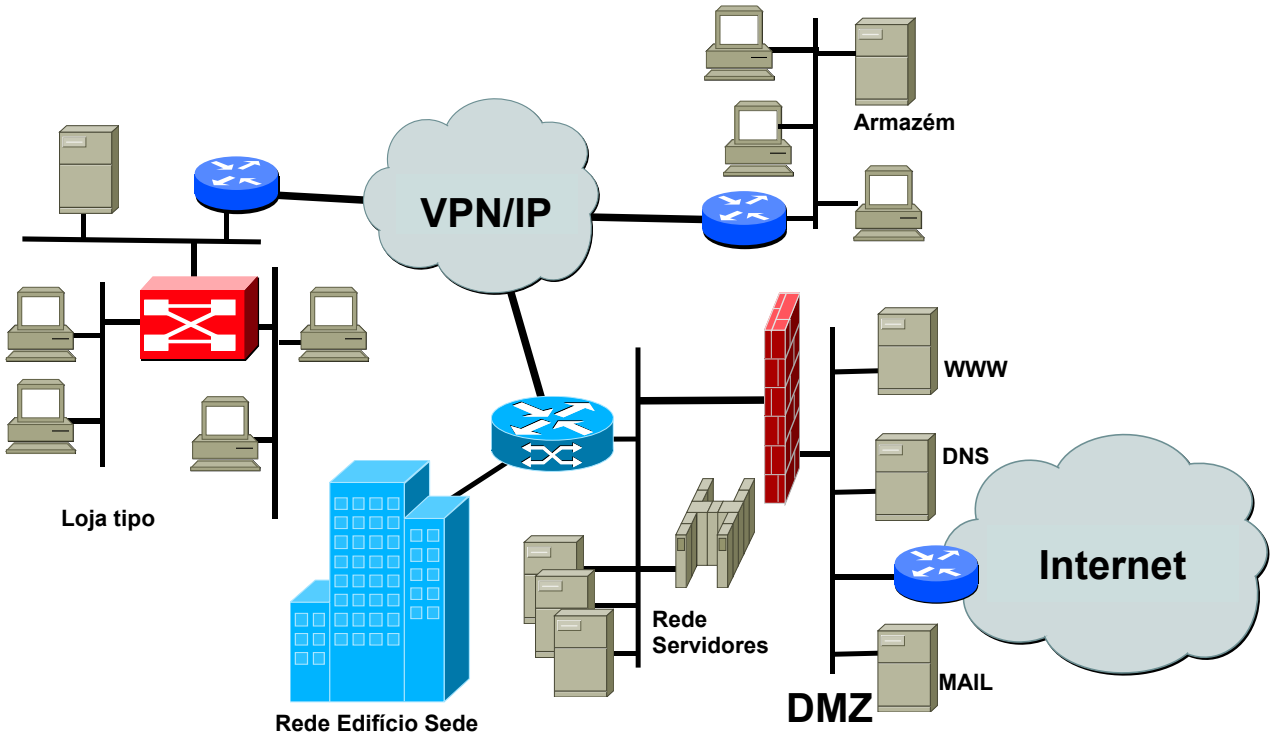
Endereçamento IP e Serviço DNS

Este trabalho tem por objetivo auxiliar a compreensão dos requisitos do endereçamento IP para uma rede empresarial, com várias redes locais de diferentes tamanhos e tecnologias. Depois deverá ser planeado e configurado o serviço de DNS para permitir a resolução de nomes distinta quando for feita a consulta a partir da rede interna (Intranet) ou do exterior (Internet), evitando a exposição dos endereços das redes internas.

Parte 1

Elabore o projeto do endereçamento IP necessário para a interligação das redes e dos sistemas da empresa QQUMA Lda.



As características principais da infraestrutura de rede da empresa são:

- Todos os serviços da rede são suportados na pilha de protocolos TCP/IP.
- As instalações da empresa estão interligadas por uma VPN/IP sobre MPLS.
- No edifício sede existe uma Ethernet, "Rede Servidores", que liga à *firewall* para o acesso ao exterior e ao router/switch de acesso à rede do edifício com cablagem estruturada (300 pontos de acesso). Os servidores nesta rede disponibilizam os serviços essenciais para a rede da empresa, tal como o servidor de DNS para a Intranet [ns.qquma.pt], o servidor de E-mail [mail.qquma.pt] e o servidor Web [www.qquma.pt].

- Existem três lojas com a configuração igual à loja tipo apresentada. Em cada loja existe um router de acesso ao qual está ligado um comutador Ethernet 10/100 Mb/s que disponibiliza duas VLANs para clientes com o máximo de 24 e 16 estações ligadas, respetivamente. Para os serviços de rede locais, tal como a gestão do domínio do DNS para a loja e o proxy HTTP, existe um servidor que é visto nas duas VLANs e deverá ser reconhecido pelos nomes [ns.lojaX.qquma.pt] e [proxy.lojaX.qquma.pt].
- Há um armazém com um router de acesso e uma rede local Ethernet, com um único domínio de colisões, à qual estão ligadas 17 estações e um servidor local [armazem.qquma.pt], que tem configurado um servidor cache do serviço DNS e que reencaminha todos os pedidos para o servidor principal localizado no edifício sede.
- Para as comunicações diretas com o exterior, portanto a montante da *firewall* e com ligação direta à Internet, existe uma zona desmilitarizada da rede, a DMZ. Nesta rede estão instalados os únicos servidores visíveis do exterior: DNS, E-mail e Web, sendo reconhecidos pelos nomes [ns.qquma.pt], [mail.qquma.pt] e [www.qquma.pt], respetivamente.

Para resolver o problema de endereçamento foi-lhe atribuído o seguinte bloco de endereços:

192.168/21 para a Intranet e **20.49.51.160/28** para a DMZ.

1. Projete o esquema de endereçamento da rede da empresa, usando do bloco de endereços acima, apenas os blocos de endereços com o tamanho necessário para cada rede. Justifique.
2. Apresente os vários endereços (identificação da rede e *broadcast*) e as respetivas máscaras para cada uma das redes.
3. Atribua endereços aos servidores indicados e às *gateways* de cada rede local. As boas práticas recomendam que os servidores tenham os endereços mais baixos da rede, por exemplo o mais baixo será o servidor de DNS, e a *gateway* o mais alto (antes do *broadcast*).
4. Assumindo a atribuição de endereços que fez anteriormente, configure na sua bancada uma topologia de rede que represente a rede de servidores do edifício sede, as redes de uma loja e a do armazém.

Parte 2

Configure o serviço de DNS para a empresa QQUMA Lda, com o domínio qquma.pt.

1. Identifique nos sistemas Unix que tem disponíveis a localização dos programas associados e necessários para a instalação e configuração do *daemon* "named".
2. Caso não exista, crie o diretório /var/named e coloque aí todos os ficheiros de configuração e dados do named.
3. Configure uma solução de "*split DNS*" com um servidor primário para o domínio qquma.pt na Intranet e o outro será o que estará disponível para a Internet com a informação dos serviços/servidores da DMZ (configure o servidor de DNS da Intranet para fazer *forward* para o servidor de DNS externo com conectividade à Internet, ou alternativamente configure um servidor com "vistas").
4. Configure para o subdomínio das redes da loja o respetivo servidor DNS e coloque o servidor DNS do domínio da empresa como servidor secundário (*slave*) deste.
5. Na rede do armazém configure o servidor de cache de DNS previsto.
6. Os servidores DNS da Intranet fazem *forward* para o servidor da empresa no edifício sede.
7. Nenhum IP das redes Intranet deverá ter conectividade à Internet, apenas terá a rede DMZ. Por isso, para a implementação deste cenário em cada bancada, deverá ser feito NAT da rede 20.49.51.160/28 para a rede do laboratório. A rede 192.168/21 não deverá ter conetividade externa.
8. Active a geração de logs do BIND no(s) servidor(es) e teste as configurações. Apresente o extrato do log demonstrativo do bom funcionamento das configurações.

Exemplo de configuração do NAT:

```
router#conf terminal
router(config)#int fa0/0
router(config-if)#description outside access interface
router(config-if)#ip nat outside
router(config-if)#int fa0/1.10
router(config-if)#description inside access interface
router(config-subif)#ip nat inside
router(config-if)#int fa0/1.20
router(config-if)#description inside access interface
router(config-subif)#ip nat inside
router(config-if)#int fa0/1.30
router(config-if)#description inside access interface
router(config-subif)#ip nat inside
router(config-subif)#exit

router# conf terminal
! Include the VLAN10 IP network
router(config)#access-list 1 permit 172.16.1.0 0.0.0.255
! Include the VLAN20 IP network
router(config)#access-list 1 permit 172.16.2.64 0.0.0.31
! Include the VLAN30 IP network
router(config)#access-list 1 permit 172.16.2.192 0.0.0.15
router(config)#ip nat inside source list 1 interface fa0/0 overload
```

Material de Consulta:

- Comer, Douglas E., *Internetworking with TCP/IP, Vol I*
- http://www.isc.org
- Páginas do Manual *online* do Linux (locais ou http://www.linuxdoc.org)
- RFCs.