

Universidade do Minho
Licenciatura em Ciências da Computação
Sistemas de Comunicações e Redes
TP2: Protocolo IPv4 (Parte II – 2 aulas)

Endereçamento e Encaminhamento IP

1. Objetivos

Neste trabalho continua-se o estudo do protocolo IPv4 com ênfase no endereçamento e encaminhamento IP. Serão estudadas algumas das técnicas mais relevantes que foram propostas para aumentar a escalabilidade do protocolo IP, mitigar a exaustão dos endereços IPv4 e também reduzir os recursos de memória necessários nos *routers* para manter as tabelas de encaminhamento.

Das técnicas mais comuns, destacam-se:

- 1) *Classless InterDomain Routing*¹ (CIDR) - RFCs 1517, 1518, 1519, 1520
- 2) Subredes (*Subnetting*)
- 3) *Variable Length Subnet Masking*² (VLSM) - RFC 1009
- 4) Sumarização de Rotas (*Supernetting*)
- 5) Atribuição dinâmica de endereços usando o DHCP³
- 6) Utilização de endereços privados - RFC 1918

Relativamente à exaustão de endereços, as técnicas acima referidas apenas solucionam o problema no curto prazo. Uma solução para responder ao aumento significativo do número de endereços que se antevem necessários a médio e longo prazo é o uso progressivo do *Internet Protocol* versão 6 (IPv6).

2. Endereçamento e Encaminhamento IP

Recorda-se que um endereço IP identifica a interface de rede de um *host* numa determinada rede IP.

Originalmente, os endereços IP foram organizados em classes. Nesse esquema, o identificador de *host* e de rede estão pré-definidos. A classe A foi definida para redes de grande dimensão, a classe B para redes de média dimensão e a C para redes de pequena dimensão. A classe D é usada para comunicação em grupo (*multicast*) e a classe E é reservada. Atualmente, é usada a notação CIDR que, com auxílio de uma máscara de rede (*netmask*), permite determinar a parte do endereço IP que identifica a rede e o *host*.

Tomando como exemplo um endereço classe A 10.10.10.10, por defeito, a máscara de rede é sempre 255.0.0.0. Isto significa que o endereço de rede corresponde ao primeiro byte e o identificador de *host* aos três últimos bytes do endereço. Na notação CIDR especifica-se o número de bits (/n) usados para identificar o endereço de rede, e.g. 10.10.10.10/8, podendo o valor de /n variar. Assim, no esquema de endereçamento sem classes, a máscara de rede é variável e determinada de acordo com o valor /n.

1 Encaminhamento Inter-Domínio sem Classes

2 Máscaras de sub-rede de comprimento variável

3 *Dynamic Host Configuration Protocol*

Caso de estudo

No editor do CORE selecione em “Tools > IP addresses...” os endereços 192.168.0.0.

Considere que a organização REDES é constituída por quatro departamentos (*A, B, C, D*) e cada departamento possui um *router* de acesso à sua rede local. Estes *routers* de acesso (R_A , R_B , R_C e R_D) estão interligados entre si por ligações Ethernet a 1 Gbps, formando um anel. Por sua vez, existe um servidor (S_1) na rede do departamento *A* e, pelo menos, dois *PCs* por departamento, interligados ao *router* respetivo através de um *switch* (comutador). O servidor S_1 tem uma ligação a 1 Gbps e os *PCs* ligações a 100 Mbps. Considere apenas a existência de um *switch* por departamento. Modifique o endereço IP atribuído pelo CORE às placas de rede do departamento A de forma a pertencerem à rede 192.168.<nº do grupo>.0/24.

A conectividade IP externa da organização é assegurada através dum *router wireless* R_{ISP} de acesso ao ISP (*Internet Service Provider*), o qual está conetado diretamente (portanto, sem passar por nenhum *switch*) ao *router* R_A por uma ligação ponto-a-ponto a 1 Gbps, pertencente à rede 136.<nº do grupo>.254.254/16. O endereço IP da interface *wireless* do *router* R_{ISP} é 136.<nº do grupo+1>.254.254/16. (Nota: uma interface *wireless* é criada no *router* quando se liga este à *wireless* LAN (nuvem)).

Construa uma topologia CORE que reflita a rede local da organização. Para facilitar a visualização pode ocultar o endereçamento IPv6 (View > Show > IPv6 Addresses).

- 1) Atenda aos endereços IP atribuídos automaticamente pelo CORE aos diversos equipamentos da topologia.
 - a. Indique que endereços IP e máscaras de rede foram atribuídos pelo CORE a cada equipamento. Para simplificar, pode incluir uma imagem que ilustre de forma clara a topologia definida e o endereçamento usado.
 - b. Tratam-se de endereços públicos ou privados? Porquê?
 - c. Porque razão o CORE não atribui um endereço IP aos *switches*? Faz sentido na prática um *switch* ter um endereço IP? Justifique.
- 2) Para o *router* R_A e o servidor S_1 do departamento A:
 - a. Execute o comando *netstat -rn* por forma a poder consultar a tabela de encaminhamento unicast (IPv4). Inclua no seu relatório as tabelas de encaminhamento obtidas. Interprete as várias entradas de cada tabela. Se necessário, consulte o manual respetivo (*man netstat*).
 - b. Diga, justificando, se está a ser usado encaminhamento estático ou dinâmico (sugestão: analise os processos que estão a correr em cada sistema (*hosts, routers*) usando, por exemplo, o comando *ps -ax*).
 - c. Escolha um *PC* da organização REDES que esteja o mais distante possível em termos de saltos IP do servidor S_1 . Recorrendo apenas ao comando *traceroute -I*, responda às seguintes questões, justificando:
 - i. Existe conectividade IP desse *PC* para o servidor S_1 ? A quantos saltos IP está o *PC* selecionado do servidor S_1 ?
 - ii. As rotas dos pacotes ICMP *echo reply* são as mesmas, mas em sentido inverso, das rotas dos pacotes ICMP *echo request* trocadas entre esse *PC* e o servidor S_1 ? (Sugestão: trace a rota de S_1 para o *PC* selecionado).
 - d. Admita que, por questões administrativas, a rota por defeito (0.0.0.0 ou *default*) deve ser retirada definitivamente da tabela de encaminhamento do servidor S_1 localizado no departamento A. Use o comando *route delete* para o efeito. Se necessário, consulte o manual respetivo (*man route*). Que implicações tem esta medida para os utilizadores da organização REDES que acedem ao servidor. Justifique.

- e. Adicione as rotas estáticas necessárias para restaurar a conectividade para o servidor S_1 , por forma a contornar a restrição imposta na alínea anterior. Utilize para o efeito o comando *route add* e registre os comandos que usou.
- f. Teste a nova política de encaminhamento garantindo que o servidor está novamente acessível, utilizando para o efeito o comando *ping*. Registe a nova tabela de encaminhamento do servidor S_1 .
- g. Apague nas tabelas de encaminhamento dos *routers* R_A , R_B , R_C e R_D a rede a que pertence a interface *wireless* do *router* R_{ISP} . Usando rotas por defeito, altere as tabelas de encaminhamento dos equipamentos da organização REDES de forma a possibilitar aos seus utilizadores o acesso genérico à Internet através do *router* R_{ISP} .
 - i. Apresente as novas tabelas de encaminhamento.
 - ii. Teste a solução verificando a conectividade entre um *PC* de cada departamento e a interface *wireless* do *router* R_{ISP} (basta usar um *PC* por departamento).

3. Definição de Sub-redes

Por forma a minimizar a falta de endereços IPv4 é comum a utilização de sub-redes. Além disso, a definição de sub-redes permite uma melhor organização do espaço de endereçamento das redes em questão.

Para definir endereços de sub-rede é necessário usar a parte prevista para endereçamento de *host*, não sendo possível alterar o endereço de rede original. Recordase que o *subnetting*, ao recorrer ao espaço de endereçamento para *host*, implica que possam ser endereçados menos *hosts*.

Considere a topologia definida anteriormente. Assuma que o endereçamento entre os *routers* se mantém inalterado. Contudo, o endereçamento em cada departamento deve ser redefinido.

- 1) Considere que dispõe apenas do endereço de rede IP 150.XX.80.0/20, em que XX é o decimal correspondendo ao seu número de grupo (GXX). Defina um novo esquema de endereçamento para as redes dos departamentos (mantendo as redes de acesso e central (*core*) inalteradas) e atribua endereços às interfaces dos vários sistemas envolvidos. Assuma que todos os endereços de sub-redes são usáveis. Deve justificar as opções usadas.
- 2) Qual a máscara de rede que usou (em formato decimal)? Quantos *hosts* IP pode interligar no máximo em cada departamento? Quantos prefixos de sub-rede ficam disponíveis para uso futuro? Justifique.
- 3) Garanta e verifique que conectividade IP entre as várias redes locais da organização REDES é mantida. Explique como procedeu.

Bibliografia

Internetworking - Protocolo IP (Notas de Apoio das Aulas Teóricas).
Internet Protocol (IP): <https://www.rfc-editor.org/rfc/rfc791>.

Relatório do trabalho

O relatório final deve incluir apenas:

- título e identificação do grupo;
- uma secção "Questões e Respostas" relativas ao enunciado acima (formato: transcrição da questão, resposta, ...);
- uma secção de "Conclusões" que autoavaleie (de forma completa) os resultados da aprendizagem decorrentes das várias vertentes estudadas no trabalho.

O relatório deve seguir preferencialmente o formato LNCS (Springer, existem *templates .tex* e *.docx*) e ser submetido obrigatoriamente na plataforma de ensino com o nome SCR-TP2-Gxx.pdf (por exemplo, SCR-TP2-G112.pdf para o grupo G112) até final do dia previsto para a conclusão do trabalho.