Escola Secundária do Monte de Caparica

Redes de Comunicação

Módulo III – Redes de Computadores Avançado

Curso Técnico de Gestão e Programação de Sistemas Informáticos

(43 tempos)

Prof: Paulo Quaresma & Rosário Peixoto

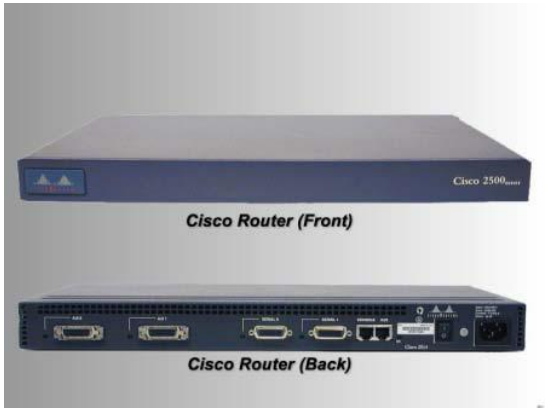
A camada Rede do modelo OSI

Introdução

- Computadores separados por distâncias de milhares de quilómetros comunicam em fracções de segundo.
- Todos os dias acedemos a páginas Web ou a servidores de jogos que se encontram do outro lado do planeta e tudo instantaneamente.
- Quem se encarrega de encaminhar os nossos pedidos pela rede?
- Como Funcionam as aplicações de rede?
- As respostas a estas questões e a muitas encontram-se neste módulo.

Camada de Rede do Modelo OSI

- A partir deste momento, entramos no domínio dos Router's e consequentemente das redes alargadas (WAN's).
- A comunicação na Internet depende fundamentalmente destes equipamentos.



Routers e Portos de Interface de Routers

- Nesta Camada (rede) imperam os routers.
- Este equipamento é responsável pelo encaminhamento dos pacotes entre diferentes redes.
- Muitas vezes denominados equipamentos L3 – Layer 3 ou simplesmente da camada 3.
- São em tudo semelhantes, em aspecto, a switchs embora estes últimos apenas funcionem na camada 2 – Layer 2 (L2).

Routers e Portos de Interface de Routers

- Os routers, representam os nós entre redes.
- São os equipamentos mais caros de uma rede, mas também os mais importantes.
- Em todo o mundo existem milhões interligados entre si, permitindo construir o que chamamos de Internet.
- Sem eles não seria possível comunicar entre computadores de redes diferentes.
- Actualmente, estamos prestes a esgotar os endereços IP disponíveis na Internet pelo uso do IPv.4

[1] **O** endereço IP versão 4 é constituído por 32 bits, isto é, por 4 bytes, cada um separado por um ponto e representado por um número decimal entre 0 e 255. Um exemplo : 192.168.1.1

Routers e Portos de Interface de Routers

- Nos anos 80, nunca se pensou que esta situação pudesse ocorrer, uma vez que o número de computadores existentes na época não era significativo.
- Na tentativa de contornar este problema, criou-se o NAT - *Network Address Translation*.
- Este protocolo é utilizado principalmente por routers e permite que uma rede privada tenha acesso à Internet (rede pública), isto é, no início do desenvolvimento das redes todos os pc's tinham um endereço IP fixo (pago) público.

Routers e Portos de Interface de Routers

- Desta forma, uma empresa com centenas de computadores na sua rede estaria a gastar igual número de IP's públicos para aceder à Internet.
- Com o aparecimento do NAT foi possível que redes privadas utilizassem IP´s de gama privada (ex. 10.0.0.12) e mesmo assim, pudessem aceder a uma rede pública (Internet) sem a necessidade de um IP público por computador.
- O esquema que se segue (figura 2), permite-nos compreender como funciona o protocolo NAT.

Routers e Portos de Interface de Routers

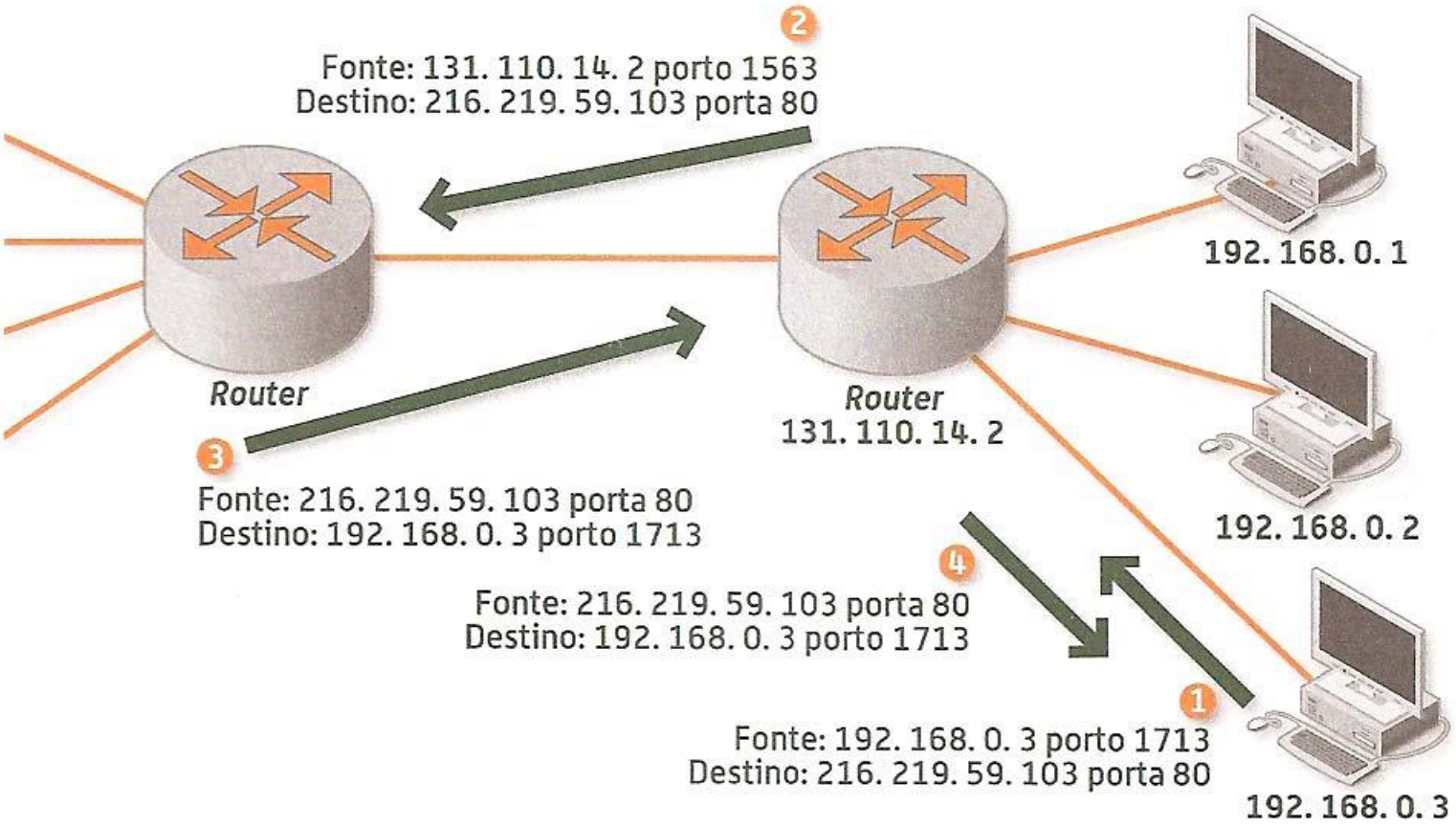


Figura 2 - Exemplo do funcionamento do protocolo NAT

Routers e Portos de Interface de Routers

- Neste exemplo, o computador com IP 192.168.0.3 tenta aceder a uma página de Internet (porta 80).
- Ao passar num router que utilize o protocolo NAT, este modifica os pacotes de dados substituindo o endereço IP privado por um válido na Internet (ex. 131.110.14.2).
- Desta forma, todos os computadores da rede podem utilizar apenas um endereço IP público para acederem à Internet, aumentando assim significativamente o número de IP's públicos livres na Internet.

Routers e Portos de Interface de Routers

- Mas como recebe um PC de uma rede privada a resposta da rede pública?
- No pacote de origem, enviado pelo IP 192.168.0.3, é indicado no cabeçalho que este se encontra no porto 1713 (valor aleatório) e tem como destino a porta 80 do IP 216.219.59.103 (da figura2).
- O router apenas modifica o cabeçalho no que respeita à origem do pacote, por exemplo, para porto 1563, IP 131.110.14.2 (IP do router), mantendo o cabeçalho de destino (ver bola laranja 2 da figura 2).
- Será agora a vez da estação de destino enviar a resposta de volta para a origem, isto é, para o porto 1563, IP 131.110.14.2 (bola laranja 3).

Routers e Portos de Interface de Routers

- Chegado o pacote de volta ao router, ele apenas confere a tabela NAT, previamente guardada em memória, para saber para que estação deve encaminhar o pacote.
- Assim, confere que para o porto 1563, IP 131.110.14.2, o cabeçalho do pacote deve ser modificado para o porto 1713, IP 192.168.0.3 para que chegue à estação correcta (bola laranja 4).
- De seguida, encontra-se a tabela NAT relativa a este exemplo.

Routers e Portos de Interface de Routers

Lado LAN	Lado WAN
131.110.14.2	192.168.0.3
Porto 1563	Porto 1713

Tabela 1 - Tabela NAT

Comunicação entre redes

- No ponto anterior explicou-se como as estações de uma rede privada acediam a uma rede pública, porém falta saber como os routers distinguem o tráfego que por eles passa.
- Cada router é dotado de memória.
- Esta varia de tamanho de router para router, tornando-se um parâmetro importante a ter em conta quando se adquire um.
- Nessa memória são armazenados endereços de forma estática ou dinâmica em forma de tabela.

Comunicação entre redes

- Em qualquer computador, através da consola do MS-DOS, é possível ter acesso à tabela de encaminhamento do nosso PC, que são em tudo semelhantes às existentes nos routers.
- Digitando **netstat –r** obtém-se algo similar à figura 3.

Comunicação entre redes

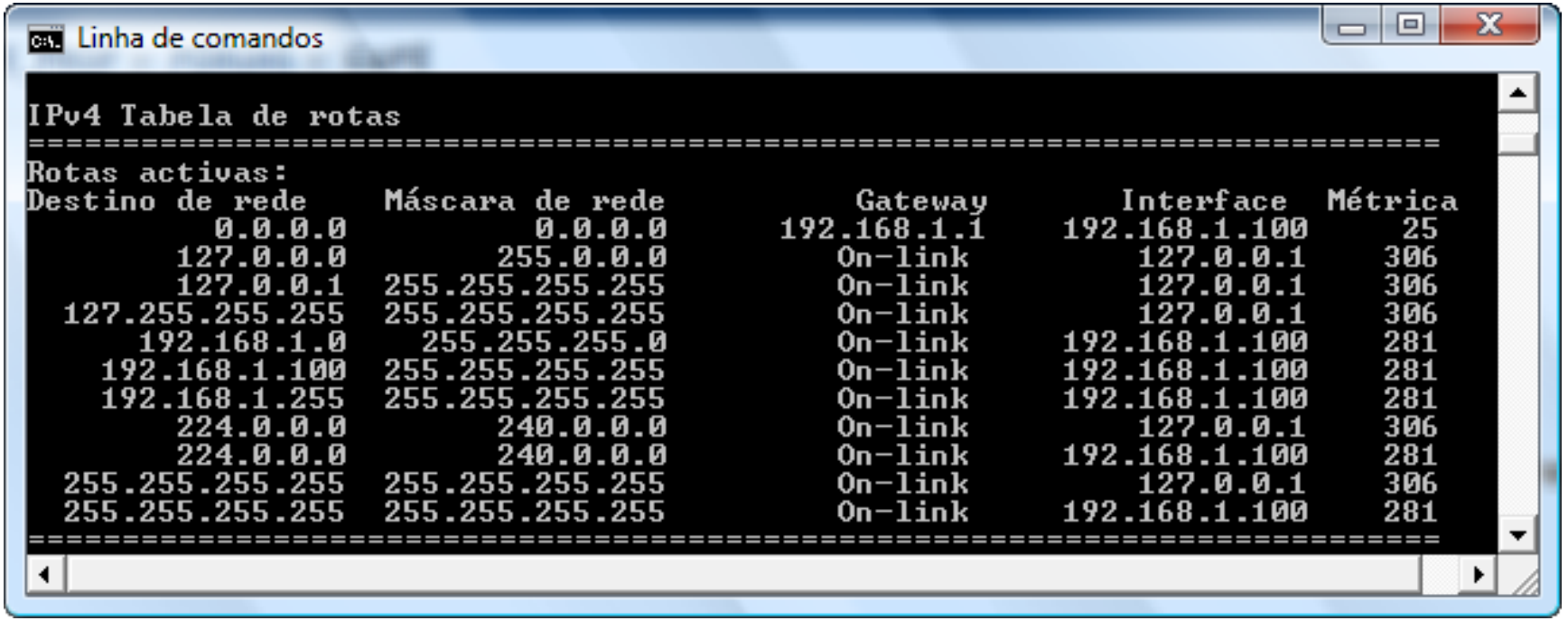


Figura 3- Tabela de encaminhamento gerada no MS-DOS com o comando netstat –r

Comunicação entre redes

- Dos endereços obtidos, alguns merecem a nossa atenção especial.
- O IP *gateway*, que neste caso é o 192.168.1.1, indica onde se encontra o router da nossa rede, que tem como função comunicar entre redes.
- Podemos ver a *gateway* como a ponte entre duas margens de um rio.
- Para atravessarmos de uma margem para a outra, em analogia com comunicarmos de uma rede para a outra, necessitamos de saber onde fica a ponte.
- É esta indicação que nos fornece a *gateway*, a saída da nossa rede.

Comunicação entre redes

- O IP 127.0.0.0 serve para a comunicação com o próprio computador (*localhost*).
- Qualquer pacote enviado para este endereço ficará no próprio computador e será tratado como se fosse um pacote recebido pela rede (*loopback*).
- O IP 0.0.0.0 serve para encaminhar pacotes para a *gateway* quando o IP de destino não consta na tabela de encaminhamento, isto é, quando o endereço não consegue ser resolvido dentro da própria rede.
- É a rota a seguir por defeito (*default*).

Comunicação entre redes

- O endereço IP 224.0.0.0 é o endereço reservado para o *multicast* e finalmente o endereço 255.255.255.255 é reservado para *broadcast*.
- Quando um PC de uma rede privada tenta aceder à Internet esse pedido percorre a rede até chegar a um router.
- Este vai conferir a sua tabela e ao verificar que o pedido não pode ser satisfeito dentro da rede, encaminha-o para o seu hierárquico superior, neste caso o servidor *ISP*, e assim sucessivamente até que se encontre o destino (ou não).
- A solicitação do pedido fica guardada no router para que este possa receber a resposta e reencaminhá-la para a estação que o emitiu.

Comunicação entre redes

Proposta de Trabalho

No computador, abra a consola do MS-DOS no Windows e digite o comando ***netstat-r***. Verifique as semelhanças entre o resultado e a tabela de encaminhamento mostrada anteriormente. Qual a sua *gateway*?

Conceitos de ARP e tabelas ARP

- ARP – *Address Resolution Protocol* é a forma de associar um endereço físico (*MAC Address*) a um endereço virtual (IP).
- Quando apenas é conhecido o endereço virtual de uma estação e se pretende saber o endereço físico (MAC) da mesma é utilizado o protocolo ARP.

- Este, através do envio de uma mensagem em *broadcast* – *Quem é a estação com o IP xxx.xxx.xxx.xxx ?* – recebe a resposta da estação com o IP solicitado (*em unicast*) onde consta o *Mac Address*, permitindo assim a comunicação entre as duas máquinas.(Ver figura 4).

Conceitos de ARP e tabelas ARP

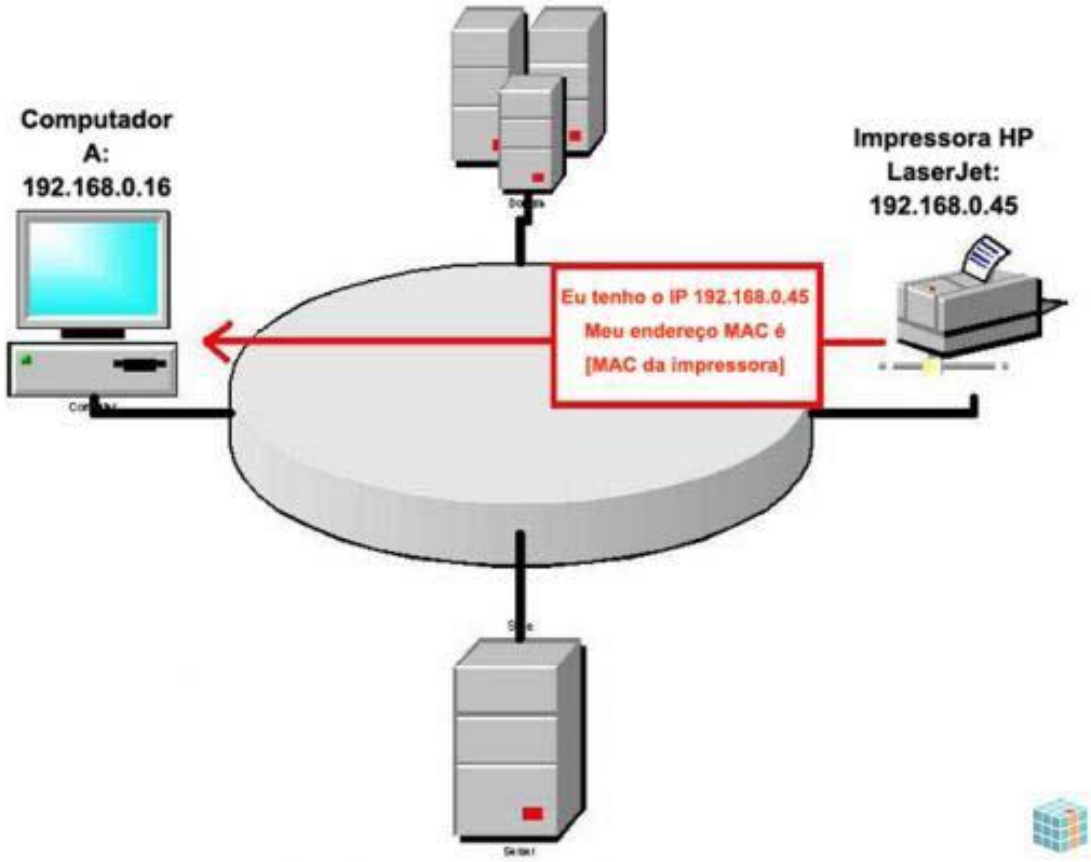


Figura 4 - Exemplo de um envio de mensagem Broadcast e recepção da resposta em Unicast

Conceitos de ARP e tabelas ARP

- Como se viu anteriormente (no módulo 2), as mensagens em *Broadcast* podem baixar o rendimento de uma rede, já que causam congestionamentos ou mesmo *Broadcast Storms*.
- Para que as estações não necessitem de estar constantemente a enviar mensagens em *Broadcast*, guardam em forma de tabela os IP's e respectivos Mac Address acedidos, bem como os das estações que lhe acederam recentemente.
- As linhas da tabela serão gradualmente apagadas ao fim de dois minutos, sempre que não se verificar comunicação entre os respectivos computadores.
- Assim, antes de transmitir a estação verifica se o computador com que pretende comunicar já se encontra na tabela.

Conceitos de ARP e tabelas ARP

- Se assim for, retira o Mac respectivo da tabela e comunica em *unicast*, caso contrário, envia uma mensagem em *broadcast* (*ARP Request*).
- O Protocolo ARP é utilizado nas seguintes situações:
  - Quando duas estações estão na mesma rede e pretendem comunicar entre si (sem aceder a routers) (PC-PC);
  - Quando duas estações estão em redes diferentes e têm de aceder a um *router/gateway* para comunicar entre si (PC-Router);
  - Quando um Router tem de encaminhar um pacote de dados para um computador através de outro Router (Router-Router);
  - Quando um Router tem de encaminhar um pacote de dados para uma estação na sua rede (Router-PC).

Conceitos de ARP e tabelas ARP

Proposta de Trabalho

No computador, abra a consola do MS-DOS no Windows e digite ***arp -a*** para ter acesso à tabela arp do seu computador. Analise-a.

Rotas Estáticas e Dinâmicas

- Os routers guardam os registos dos seus conhecidos (outros routers) em forma de tabela associando-os a um caminho (rotas).
- Como são construídas essas tabelas?
- Em que se baseia o router para as determinar?
- Estas são questões que surgem automaticamente.
- Um router tem dois tipos de rotas associadas a endereços, como se mostra de seguida.

Rotas estáticas

- Inseridas manualmente (implica pessoal especializado) através de comandos de administração para gerir a tabela de encaminhamento.

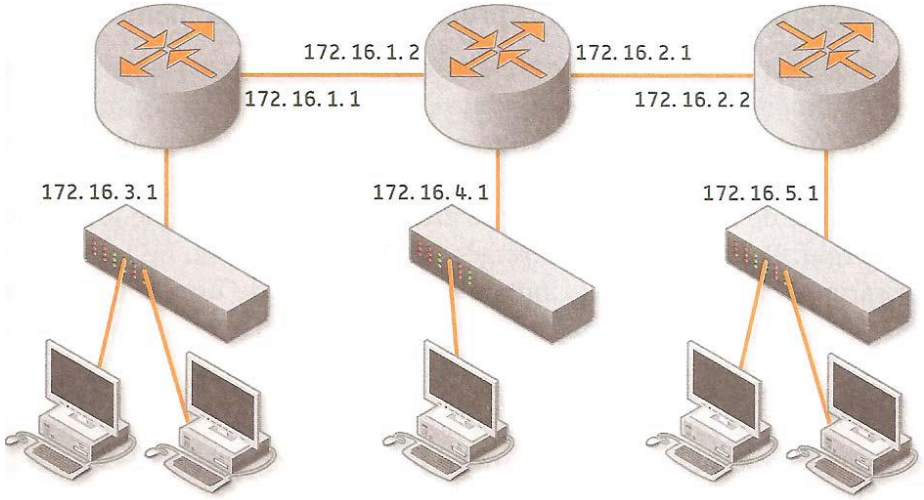


Figura 5 - Configuração de rotas estáticas

Rotas estáticas

- No caso de se configurarem os routers da figura 5 com rotas estáticas, quando um computador da rede 172.16.3.0 quiser comunicar com um da rede 172.16.4.0 sabe que tem de encaminhar o pedido para a interface 172.16.1.2 para que o próximo router resolva.
- No entanto, se houvesse um outro caminho (melhor), que não o existente na figura, que ligasse o router 1 ao router 2 ele continuaria a encaminhar os pacotes pela mesma interface visto este endereçamento ser estático.

Rotas estáticas

- Este tipo de endereçamento apresenta vantagens e desvantagens

Vantagens	Desvantagens
Maior segurança, uma vez que existe apenas um caminho de entrada/saída da rede;	Sem redundância ou tolerância a falhas – no caso de um link falhar, perde-se a comunicação por completo, já que o router não irá tentar descobrir um caminho alternativo;
Processamento da informação no router mais rápido.	Em redes de grandes dimensões torna-se impraticável configurar todas as rotas manualmente.

Tabela - Vantagens e desvantagens do encaminhamento estático

Rotas Dinâmicas

- Em vez da inserção manual, a tabela de encaminhamento será preenchida dinamicamente com base em **protocolos de encaminhamento**.
- Usa-se essencialmente para redes com mudanças frequentes de topologia ou de grandes dimensões.
- O preenchimento será então baseado em **Métricas** que podem variar entre:

Rotas Dinâmicas

- Número de saltos (*hops*);
- Atraso (*delay*);
- Custo dos caminhos – Valor atribuído arbitrariamente pelo administrador da rede;
- Largura de banda – velocidade de transmissão;
- Congestionamento;
- Fiabilidade.

Rotas Dinâmicas

- Contudo, os routers não analisam todas estas métricas em simultâneo.
- Existem para isso algoritmos que suportam os protocolos de encaminhamento e podem usar apenas uma ou mais métricas.
- À semelhança das rotas estáticas existem vantagens e desvantagens na utilização das rotas dinâmicas que são apresentadas na tabela seguinte.

Rotas Dinâmicas

Vantagens	Desvantagens
Garante redundância e tolerância a falhas;	Falta de controlo nas rotas escolhidas (tarefa do protocolo de encaminhamento);
Boa aplicabilidade para redes de grandes dimensões;	Processamento da informação no router mais lento devido aos cálculos impostos pelo protocolo de encaminhamento;

Tabela - Vantagens e desvantagens do encaminhamento dinâmico

Algoritmos e protocolos de encaminhamento

- Os algoritmos e protocolos de encaminhamento, apenas se aplicam a endereçamento dinâmico.
- Neste ponto abordam-se as formas como os routers de uma rede comunicam entre si e trocam informações, bem como conseguem, face a alterações na rede, permitir a convergência da mesma.
- Na gíria das redes é usual ouvir-se dizer frequentemente que uma rede convergiu.
- Pode definir-se convergência como o intervalo de tempo necessário para que os routers tomem conhecimento de uma alteração na rede e recalculem as rotas para a nova topologia.

Algoritmos e protocolos de encaminhamento

- Os factores que influenciam o tempo de convergência são:
  - A distância em saltos do router ao ponto de mudança;
  - O número de routers que usam protocolos dinâmicos de encaminhamento;
  - Largura de banda e congestionamento nos links;
  - Capacidade de processamento do router;
  - Protocolo de encaminhamento utilizado.
- Neste ponto abordam-se dois algoritmos e respectivos protocolos associados: *Distance Vector* (RIP) e *Link-State* (OSPF).

Distance Vector (DV) ou Algoritmo do Vector Distâncias

- Cada router tem uma tabela que contém as redes (routers) a ele ligadas directamente e as distâncias associadas.
- Todos os routers da rede trocam as suas tabelas, constituídas por um vector **(V,D)** [onde V identifica o destino e D a distância até ao destino], com os seus routers vizinhos da seguinte forma:
  - Espera a mudança na distância até a um certo destino (geralmente hops) ou do final do temporizador;
  - Recalcula a tabela de encaminhamento;
  - Se a distância for menor para algum destino, notifica (apenas) os vizinhos.

Distance Vector (DV) ou Algoritmo do Vector Distâncias

- A descoberta da rede é feita através do algoritmo do vector das distâncias ou de Bellman-Ford.
- O algoritmo foi descoberto por dois matemáticos americanos Richard E. Bellman [1920-1984] e Lester Randolph Ford, Jr. [1927-] e consiste em calcular o caminho mais curto entre dois pontos.
- A sua aplicabilidade em redes foi deveras importante sendo ainda largamente utilizado em alguns protocolos.

Distance Vector (DV) ou Algoritmo do Vector Distâncias (2)

- O algoritmo apresenta as seguintes características:
  - **Iterativo**: através da informação recebida dos vizinhos consegue calcular a sua tabela;
  - **Assíncrono**: os routers não enviam a informação em simultâneo;
  - **Distribuído**: cada router comunica apenas com os seus vizinhos diretos.

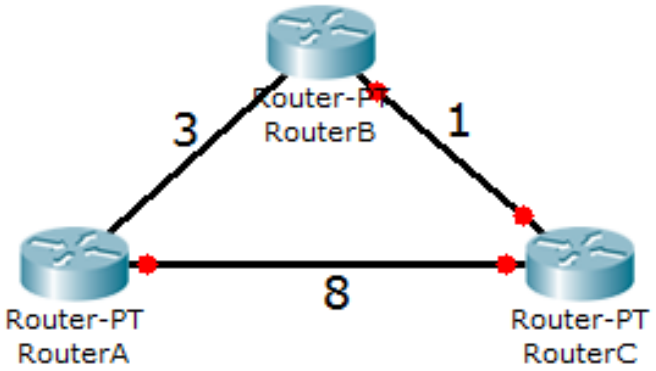
Distance Vector (DV) ou Algoritmo do Vector Distâncias

Exercício Resolvido

- Para uma melhor compreensão de como os routers aplicam este algoritmo apresenta-se o seguinte exercício:

Exercício Resolvido

- A partir da figura, obtenha as tabelas de encaminhamento finais de cada router, usando o algoritmo de vector distâncias



Distance Vector (DV) ou Algoritmo do Vector Distâncias

Exercício Resolvido

Resolução:

Na 1ª Iteração cada router verifica a que distância está dos outros, preenchendo apenas a linha correspondente ao seu próprio router (ver tabela seguinte).

1ª Iteração Router A

De **Para**

	A	B	C
A	0	3	8
B	∞	∞	∞
C	∞	∞	∞

1ª Iteração Router B

De **Para**

	A	B	C
A	∞	∞	∞
B	3	0	1
C	∞	∞	∞

1ª Iteração Router C

De **Para**

	A	B	C
A	∞	∞	∞
B	∞	∞	∞
C	8	1	0

Distance Vector (DV) ou Algoritmo do Vector Distâncias

Exercício Resolvido

Na 2ª Iteração, os routers vizinhos trocam as tabelas entre si recebendo dados que lhes permitem preencher as linhas que anteriormente estavam a infinito. Simultaneamente, as linhas preenchidas na 1ª Iteração são recalculadas com base nos novos valores. No caso de existirem custos mais baixos, esses passam a ser os novos valores da tabela (alterações assinaladas a vermelho).

2ª Iteração Router A

De \ Para

	A	B	C
A	0	3	4
B	3	0	1
C	8	1	0

2ª Iteração Router B

De \ Para

	A	B	C
A	0	3	8
B	3	0	1
C	8	1	0

2ª Iteração Router C

De \ Para

	A	B	C
A	0	3	8
B	3	1	0
C	4	1	0

Distance Vector (DV) ou Algoritmo do Vector Distâncias

Exercício Resolvido

Finalmente, na 3ª Iteração voltam a trocar as tabelas e os custos mais baixos são aplicados às tabelas que ainda têm custos mais elevados para atingir certos destinos.

3ª Iteração Router A

De \ Para	A	B	C
A	0	3	4
B	3	0	1
C	4	1	0

3ª Iteração Router B

De \ Para	A	B	C
A	0	3	4
B	3	0	1
C	4	1	0

3ª Iteração Router C

De \ Para	A	B	C
A	0	3	4
B	3	1	0
C	4	1	0

As tabelas anteriores (3ª Iteração) são as tabelas finais resultantes do exercício.

Distance Vector (DV) ou Algoritmo do Vector Distâncias

- Através do que se referiu sobre este algoritmo e do que foi observado ao longo do exercício, podemos agora apresentar algumas vantagens e desvantagens do mesmo.

Vantagens	Desvantagens
Fácil de Implementar;	Mensagens de actualização podem ser muito extensas (a tabela de encaminhamento é enviada na totalidade mesmo que só um custo se altere);
O Cálculo da tabela de routing é pouco complexo, pelo que não necessita de grande capacidade de processamento do router.	As mudanças propagam-se lentamente entre routers, podendo existir routers com informação incorrecta e esta ser propagada pela rede;
	O algoritmo pode não convergir e é lento quando converge.

Tabela - Vantagens e desvantagens do algoritmo VD

Protocolo de encaminhamento dinâmico RIP

- O RIP – *Routing Information Protocol* – foi usado pela primeira vez em 1969 (embora uma versão diferente das existentes hoje em dia) no projecto ARPANET.
- Existem dois tipos de RIP actualmente: **RIP v1** e **RIP v2** .
- Este protocolo (tanto v.1 como v.2) usa o algoritmo do vector das distâncias de Bellman-Ford.
- O RIP apenas deve ser usado em pequenas redes, devido ao seu problema de convergência (lenta) e limite de saltos.

Protocolo de encaminhamento dinâmico RIP

- Como vimos anteriormente, o algoritmo do vector das distâncias baseava-se em *hop count* (conta os saltos até ao destino).
- No RIP, a escolha dos caminhos é baseada apenas no número de saltos até ao destino.
- Isto torna-o fácil de implementar e o router onde é implementado não tem de ter grande capacidade de processamento.

Protocolo de encaminhamento dinâmico RIP

- Desta forma, quando um router recebe a tabela de um router vizinho a indicar que é possível alcançar a rede X com um número de saltos N, significa que ele pode alcançar a mesma rede X com um número de saltos N+1, se for pelo router que lhe enviou a mensagem (iterativo).

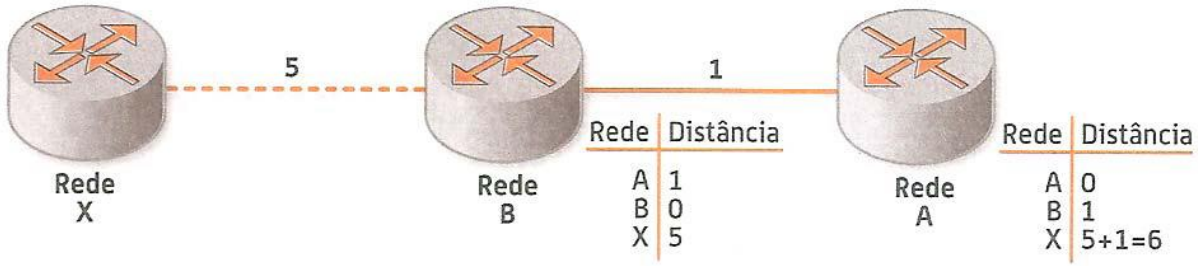


Figura 6 - Contagem de HOPs no RIP

Protocolo de encaminhamento dinâmico RIP

- No entanto, ao escolher as rotas apenas baseado no número de saltos até ao destino (métrica utilizada) pode estar a pôr de parte alternativas melhores.

- Por exemplo, um destino pode encontrar-se a uma distância de 6 saltos através de uma linha de 10Mbps e a 10 saltos através de uma linha de 1Gbps.

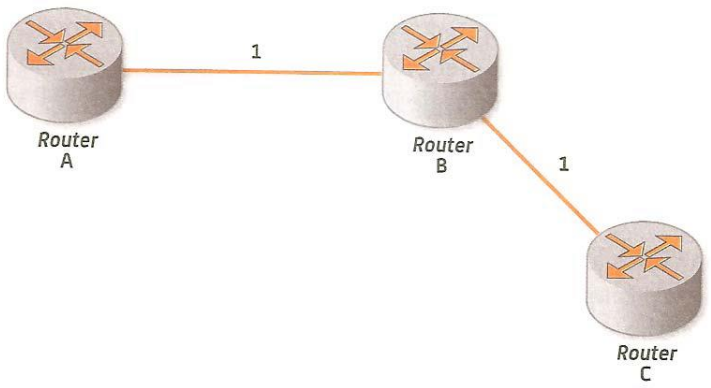
- O RIP escolhia a primeira alternativa embora a segunda fosse a melhor a nível de largura de banda.
- Este factor bem como o congestionamento, fiabilidade e outros não têm peso na decisão para a escolha dos melhores caminhos.

Protocolo de encaminhamento dinâmico RIP

- Neste protocolo de 30 em 30 segundos cada router envia para os seus vizinhos as atualizações.
- Um router que não receba informação do outro router (vizinho) durante 90 segundos marca essa rede como inacessível.
- Ao fim de 3 minutos sem "dar notícias" os routers vizinhos apagam a linha da tabela de routing que continha essa rede.
- Entretanto, durante esses períodos de espera o que acontece se existirem alterações na topologia de rede?
- Muito provavelmente ***loops***.
- Este é outro dos problemas do RIP, a sua incapacidade de detectar loops na rede.
- A lentidão com que converge aliada à falta de sincronismo dos nós propicia a formação de loops são um problema grave.

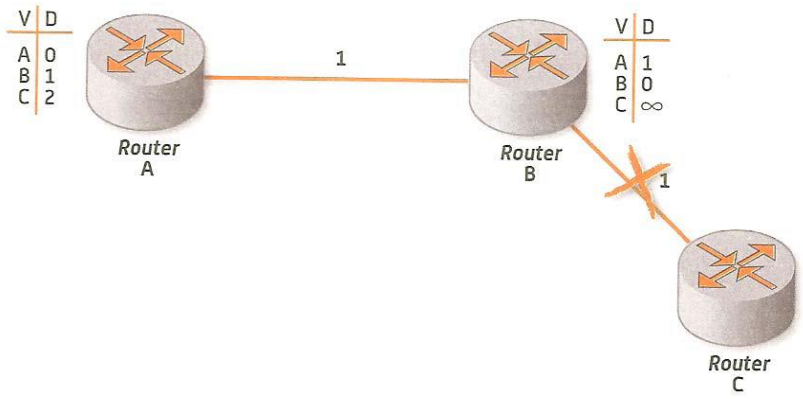
Protocolo de encaminhamento dinâmico RIP

- Quando os pacotes de dados são continuamente encaminhados através de um ciclo infinito, em vez de encaminhados para o destino esperado.
- Vejamos um exemplo:



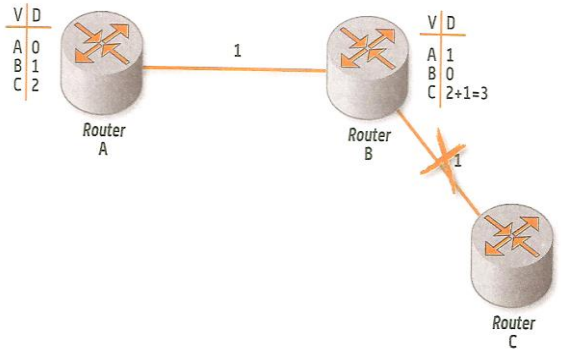
Protocolo de encaminhamento dinâmico RIP

- Imaginem que um router A comunica com C através de B.
- Entretanto o link entre B e C cai (ver figura 8).
- O router B altera o valor do número de saltos para C, na sua tabela, para infinito (valor quando o destino não se encontra acessível).



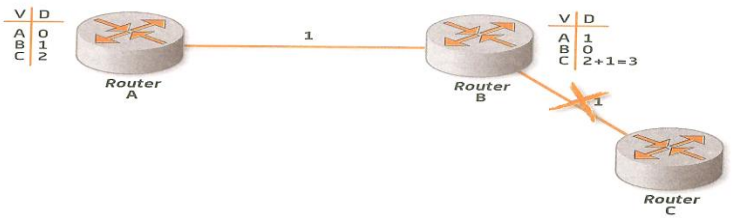
Protocolo de encaminhamento dinâmico RIP

- Até aqui tudo bem.
- No entanto, imaginem que A ainda não recebeu nenhuma actualização por parte de B relativamente ao router C e envia a sua tabela para B (devido à comunicação ser assíncrona).
- O router B compara o número de saltos que A lhe deu para chegar a C com o valor que tem na sua tabela, que neste caso é infinito.
- Como esse número é menor ele atualiza a sua tabela para chegar a C (2+1) porque acha que A encontrou outro caminho para lá chegar (ver figura 9).



Protocolo de encaminhamento dinâmico RIP

- Supondo que nesse momento o router A tenta enviar um pacote de dados para C, envia-o através de B, pensando que ainda pode fazer o trajeto A-B-C.
- Chegado esse pacote a B, ele envia-o para A, já que o caminho para C continua em baixo.
- Quando esta informação chega de novo a A ele continua a ter na sua tabela que o caminho para C é por B.
- Assim, pensando que o router B teve de alterar o caminho para C por algum motivo, atualiza a sua tabela com a nova distância que recebeu de B (3) adicionando uma unidade (salto a dar entre A e B).



Protocolo de encaminhamento dinâmico RIP

- A próxima atualização será por parte de A (temporizador de 30 segundos) que irá atualizar a tabela de B (4+1) novamente e assim sucessivamente criando-se um loop infinito.
- Como é possível solucionar esse problema?
- Para "tentar resolver" o problema da contagem para o infinito, introduziu-se um limite de número de saltos máximos possíveis.
- Estipulou-se 16 saltos (infinito).
- Assim, o loop somente se prolonga até aos 16 saltos onde o nó será removido da tabela de encaminhamento.
- Contudo, outro problema emergiu devido a este limite.
- Se por um lado, se resolveu o problema da contagem para infinito, por outro lado, limitou-se a distância entre routers a 15 saltos. Se após uma alteração na rede, um destino ficar a mais de 15 saltos deixa de ser atingível.

Protocolo de encaminhamento dinâmico RIP

- Diz-se nestes casos que a rede não teve capacidade para convergir.
- Todavia, a solução dos 16 saltos não evita que o loop se mantenha, por vezes, bastante tempo (pode demorar alguns minutos) sendo possível perder-se informação de encaminhamento relativa a outras redes.
- A resposta a este problema residia então no período de latência entre actualizações.
- Para não ser necessário esperar os 30 segundos de actualização periódica criou-se outra técnica chamada *Triggered Updates*.
- A implementação desta técnica permitia que, imediatamente após a alteração de uma métrica num router, a informação seguisse para os routers vizinhos.
- No entanto, tem de ser usada com cuidado pois em alguns casos existe a possibilidade de se criarem **broadcast storms**

Protocolo de encaminhamento dinâmico RIP

- Na tentativa de evitar as Broadcast Storms e os loops desenvolveu-se ainda outra técnica denominada de *Split Horizon*.
- O protocolo de RIP v.1 foi o primeiro a utilizá-lo.
- Este protocolo garante que os routers não anunciam as rotas através das interfaces por onde as aprenderam.
- Assim, no exemplo anterior, se A actualizasse B antes de B atualizar A não haveria problema pois este não mencionaria o custo de C a B já que aprendeu essa rota através do próprio.
- Na próxima atualização, B comunicaria a A que C estava inacessível.

Protocolo de encaminhamento dinâmico RIP

- Assim, o router A teria de escolher outro caminho para chegar a C (caso existisse).
- Esta técnica é porém falível pois não evita loop quando eles são independentes e ocorrem em mais de duas máquinas em simultâneo.

RIP v.1	RIP v.2
Envio de mensagens por broadcast - Interrompem todas as máquinas (mesmo que não tenham RIP);	Envio em multicast 224.0.0.0;
Não existe autenticação das mensagens;	Autenticação das mensagens (maior segurança);
Suporte muito incompleto a máscaras de rede.	Campo para indicar máscara de rede com suporte para máscaras estáticas e variáveis (sub-redes).

Protocolo de encaminhamento dinâmico RIP

- Na versão 2 do protocolo RIP, usa-se outra técnica denominada de *Split Horizon With Reverse* que em vez de omitir as rotas aprendidas através de uma certa interface, inclui essa rota nas trocas de informação, mas colocando o seu valor em 16 (infinito).
- Desta forma, muito dificilmente há probabilidade de ocorrer um loop na rede.

Algoritmo de encaminhamento Link-State ou estado da ligação

- Em 1959, Edsger Dijkstra (1930-2002), cientista alemão, concebeu um algoritmo, que consistia em calcular o caminho mais curto entre dois pontos (porém mais eficiente do que o algoritmo de Bellman-Ford).
- Mais tarde, este algoritmo veio a revelar-se de extrema importância nas redes de comunicação, mais propriamente no que diz respeito a protocolos de encaminhamento baseados em Link-State.

Algoritmo de encaminhamento Link-State ou estado da ligação

- Os protocolos do tipo Link-State mantêm uma tabela de informação topológica muito mais complexa que os Distance Vector (DV).
- Cada router tem a informação completa (tabela de encaminhamento única) sobre a topologia da rede e não apenas as dos seus vizinhos, como no DV.
- Desta forma, cada router calcula de forma independente os caminhos mais curtos pelo algoritmo de Dijkstra, pelo que o algoritmo converge sempre.
- Apenas as alterações são enviadas entre routers e não a tabela toda como no DV, por outro lado estas são comunicadas imediatamente quando existe uma mudança nos custos da rede.
- Como se baseia em custos, torna-se muito flexível, podendo ser aplicadas diferentes métricas conforme o que o administrador da rede pretender.

Algoritmo de encaminhamento Link-State ou estado da ligação

- Este algoritmo, à semelhança do DV, apresenta vantagens e desvantagens, como se pode verificar na tabela abaixo.

Vantagens	Desvantagens
O algoritmo converge rapidamente;	Muito complexo;
É imune a ciclos;	Utiliza muitos recursos (CPU, Memória).
Cada router tem informação completa sobre a topologia da rede.	

Tabela - Vantagens e desvantagens do Link State

Protocolo de encaminhamento dinâmico OSPF

- O protocolo Open Shortest Path First (OSPF) foi desenvolvido para substituir o RIP.
- Ao contrário da versão 2 do RIP, que veio colmatar algumas falhas da anterior versão, este protocolo segue ideias completamente diferentes para a realização do encaminhamento dinâmico.
- O ponto forte do OSPF é permitir em áreas (autónomas).
- Cada área é independente das restantes.
- Logo, o que se passa dentro de uma área não é propagado para as outras (a não ser na situação em que o router de uma área queira comunicar com o router de outra área).

Protocolo de encaminhamento dinâmico OSPF

- É importante saber que um sistema configurado com OSFP tem de contar com pelo menos uma área, denominada área de Backbone (Área 0.0.0.0 ou Área 0).
- Dentro de cada área existem routers com funções diferentes:
  - **Routers internos:** são os que se encontram em áreas que não a de backbone e realizam apenas encaminhamento de pacotes dentro da sua área, sem conhecimento da topologia das restantes áreas.

Protocolo de encaminhamento dinâmico OSPF

- **Routers de fronteira de área:** são router que pertencem a uma área qualquer mas também á de Backbone. Têm conhecimento da topologia da sua área e da de Backbone.
- **Router de Backbone:** todos os routers que se encontram na área de backbone.
- **Routers de fronteira de sistemas autónomos:** routers que estão situados na periferia de um sistema autónomo e que trocam informações de rotas com routers de outros sistemas autónomos.

Protocolo de encaminhamento dinâmico OSPF

- A área de Backbone é a responsável pelo encaminhamento entre áreas.
- Por exemplo, quando um router da área 1 pretende comunicar com um router da área 2, terá de passar obrigatoriamente pela área de Backbone (**encaminhamento hierárquico**).
- A transferência entre uma área e a área de Backbone é assegurada através dos routers de fronteira de área.

Protocolo de encaminhamento dinâmico OSPF

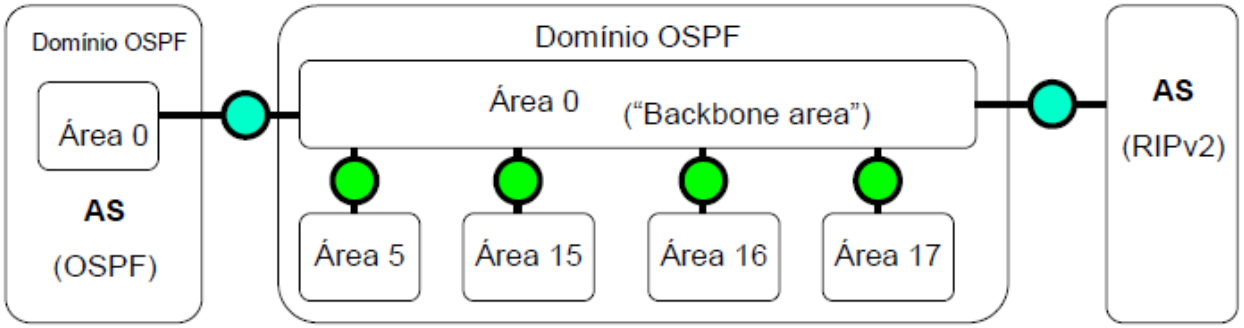


Figura 11 - Exemplo de uma rede OSPF

- O protocolo OSPF é um protocolo link-state, cada "router" tenta identificar os routers vizinhos, recorrendo a broadcast e multicast.
- Depois divulga a lista de vizinhos aos restantes routers.
- Cada "router" monitoriza o estado dos "routers" vizinhos, sempre que se produz alguma alteração repete a divulgação.
- As transações OSPF usam diretamente o protocolo IP, não recorrem ao protocolo UDP.

Endereçamento

- O endereço IP é o equivalente ao nosso bilhete de identidade, porem serve para identificar equipamentos (computadores, routers, pda's, etc.)
- Um IP é constituído por 32 bits, isto é, 4 X 8 bits (4 octetos) separados por pontos x.x.x.x.
- Os valores de x são números decimais entre 0 e 255, visto que 2^8=256.
- Existem apenas dois tipos de redes.
- A rede pública e as redes privadas.
- A rede pública, ou Internet, conta com a maior parte dos IP's ficando uma pequena gama de IP's disponíveis para as redes privadas.
- Estes são identificadores únicos, pelo que não podem existir IP's iguais na mesma rede, seja ela pública ou privada.

Classes de endereços

- Originalmente, o espaço do endereço IP foi dividido em poucas estruturas de tamanho fixo chamados classes de endereço.
- Os endereços IP estão divididos em 5 Classes:
  - Classe A (Rede de muito grande dimensão)
  - Classe B (Redes de grande dimensão)
  - Classe C (Redes de média e pequena dimensão)
  - Classe D (Endereços de Multicast)
  - Classe E (Endereços para futura utilização)
  - Endereços Reservados

Classes de endereços

- As três principais são a classe A, classe B e classe C.
- Examinando os primeiros bits de um endereço, o software do IP consegue determinar rapidamente qual a classe, e logo, a estrutura do endereço.
- ***Classe A*: 1.0.0.0 – 126.0.0.0**
  - *Os endereços da classe A são utilizados para segmentos de rede que possuem um grande número de computadores.*
  - O primeiro octeto, que designa a rede, varia entre 1 e 126, ou seja, prevê 126 redes distintas.
  - Cada rede pode ter até 16777214 computadores.
  - No total, a classe A prevê assim 2.113.928.964 equipamentos diferentes.

Classes de endereços

- **Classe B: 128.1.0.0 – 191.255.0.0**
  - *A classe B está determinada para redes de alcance (número de computadores do segmento) médio e grande.*
  - O primeiro octeto varia entre os valores 128 e191, enquanto o segundo octeto varia entre 0 e 255.
  - Prevê 16.384 segmentos de rede, com 65.534 computadores por segmento.
- **Classe C: 192.0.1.0 – 223.255.255.0**
  - *Os endereços da classe C são utilizados para redes pequenas o para redes locais, LANs.*
  - O primeiro octeto varia entre 192 e 223, o que permite 2.097.152 segmentos de rede, com 254 computadores por segmento.

Classes de endereços

- ***Classe D*: (endereço multicast): 224.0.0.0-239.255.255.255**
  - *As redes da classe D são utilizadas para multicast e broacast.*
- ***Classe E*: (endereço especial reservado): 240.0.0.0-247.255.255.255**
  - *A classe E está reservada para uso futuro, pelo que não está disponível.*

Classes de endereços

- Nem todos os endereços possíveis são válidos para atribuição a hosts, mas as regras de atribuição são simples:

Figura 12- Endereços IP válidos

Classes de endereços

- Mesmo sendo tantos os endereços IP possíveis, não chegam todos para atribuição a todos os computadores do mundo que estão ligados à Internet sem haver repetições;
  - Existem várias soluções para ultrapassar esse problema, e uma delas é importante que conheças: os endereços IP privados;
  - A ideia é simples: há uma gama de endereços em cada classe que os routers não encaminham. Assim, uma rede local – que, para ter acesso à Internet, deve ter um router dedicado ou um computador que faça esse papel, incluindo um servidor NAT (Network Address Translation – norma que permite que os endereços IP não sejam vistos pela Internet) – pode ver atribuídos aos seus hosts endereços dessas gamas;

Classes de endereços

São endereços grátis – já que os outros, denominados públicos, pagam-se bem caros – que podem ser atribuídos livremente nas redes locais. Essas gamas de endereços constam da seguinte tabela:

CLASSE	GAMA DE ENDEREÇOS
A	10.X.X.X
B	172.16.X.X - 172.31.X.X
C	192.168.0.X - 192.168.255.X

Figura 13 - Gama de endereços privados

IP´S FIXOS E DINÂMICOS

- O router contém uma tabela com todos os IP´s dos computadores.
- Esta tabela é armazenada de forma estática ou dinâmica.
- Na estática, o router tem todos os endereços IP´s da rede já determinados;
- Na dinâmica, os endereços IP são atribuídos de acordo com o pedido.
- No caso do endereçamento dinâmico, utiliza-se um protocolo chamado DHCP (Dynamic Host Configuration Protocol – Protocolo de Configuração Dinâmica de Máquina);
- Sempre que um cliente solicitar um endereço IP, o servidor DHCP disponibilizará um endereço válido que não esteja a ser utilizado nesse momento.
- Quando o cliente terminar a sua sessão, o IP será libertado

MASCARA DE SUB-REDE

- Ao configurar o protocolo TCP/IP, seja qual for o sistema operativo usado, além do endereço IP é preciso fornecer também a máscara de sub-rede (*subnet mask*).
- Ao contrário do endereço IP, que é formado por valores entre 0 e 255, a máscara de sub-rede é formada apenas por dois valores: 0 e 255, como em 255.255.0.0 ou 255.0.0.0,
  - onde um valor 255 indica a parte do endereço IP referente à rede,
  - e um valor 0 indica a parte endereço IP referente ao host.

MASCARA DE SUB-REDE

- A máscara de rede-padrão acompanha a classe de endereço IP:

Classe do endereço IP	Bits da máscara de sub-rede				Máscara padrão de sub-rede
Classe A	11111111	00000000	00000000	00000000	255.0.0.0
Classe B	11111111	11111111	00000000	00000000	255.255.0.0
Classe C	11111111	11111111	11111111	00000000	255.255.255.0

Figura 14 - Máscaras de sub-rede

MASCARA DE SUB-REDE

- Mas afinal para que servem as máscaras de sub-rede?
- Apesar de as máscaras-padrão acompanharem a classe de endereço IP, é possível "mascarar" um endereço IP, mudando as faixas do endereço que serão usadas para endereçar a rede e para o host.
- O termo máscara de sub-rede é muito apropriado neste caso, pois a "máscara" é usada apenas dentro da sub-rede.

MASCARA DE SUB-REDE

- Veja-se por exemplo, o endereço 208.137.106.103.
- Por ser um endereço da classe C, a sua máscara-padrão seria 255.255.255.0, indicando que o último octeto se refere ao host, e os restantes à rede.
- Porém, se mantivéssemos o mesmo endereço, mas alterássemos a máscara para 255.255.0.0 apenas os dois primeiros octetos (208.137) continuariam a representar a rede, enquanto que o host passaria a ser definido pelos dois últimos (e não apenas o último).

MASCARA DE SUB-REDE

Ex. de endereço IP	Máscara de sub-rede	Parte referente à rede	Parte referente ao *host*
208.137.106.103	255.255.255.0 (padrão)	208.137.106.	103
208.137.106.103	255.255.0.0	208.137.	106.103
208.137.106.103	255.0.0.0	208.	137.106.103

Figura 15 - Máscaras de sub-rede

- Nota que 208.137.106.103 com máscara 255.255.255.0 é diferente de 208.137.106.103 com máscara 255.255.0.0;
- enquanto no 1° caso temos o host 103 dentro da rede 208.137.106,
- no 2° caso temos o host 106.103 dentro da rede 208.137.

MASCARA DE SUB-REDE

- Dentro de uma mesma sub-rede, todos os hosts deverão ser configurados com a mesma máscara de sub-rede; caso contrário, poderão não conseguir comunicar, pois farão o router pensar que estão em redes distintas.
- Se, por exemplo, houver dois computadores na mesma sub-rede, configurados com os endereços 200.133.103.1 e 200.133.103.2 mas configurados com máscaras diferentes, 255.255.255.0 para o 1° e 255.255.0.0 para o 2°, teremos um erro de configuração.

MASCARA DE SUB-REDE

Proposta de Trabalho

Verifique se os dois IP's 200.18.102.79/28 e 200.18.102.81/28 se encontram na mesma sub-rede

PROTOCOLO ARP

- Protocolos como o IP trabalham acima de protocolos como o Ethernet, que é da segunda camada do modelo OSI.
- Portanto, podemos – e temos, na quase generalidade das redes locais – ter TCP/IP sobre Ethernet.
- Também já sabes que, numa rede TCP/IP os hosts são identificados por endereços IP e, nas redes Ethernet, por endereços físicos, os MAC addresses.
- A questão que se coloca agora é óbvia: quando dois hosts querem comunicar por TCP/IP, mas estão numa rede em que os adaptadores são Ethernet, como resolver o problema da identificação.
- Por outras palavras, como é que um dado host que quer enviar algo para o computador com endereço IP 192.168.4.7, sabe qual o seu endereço físico para o identificar de facto ao nível da transmissão dos bits?

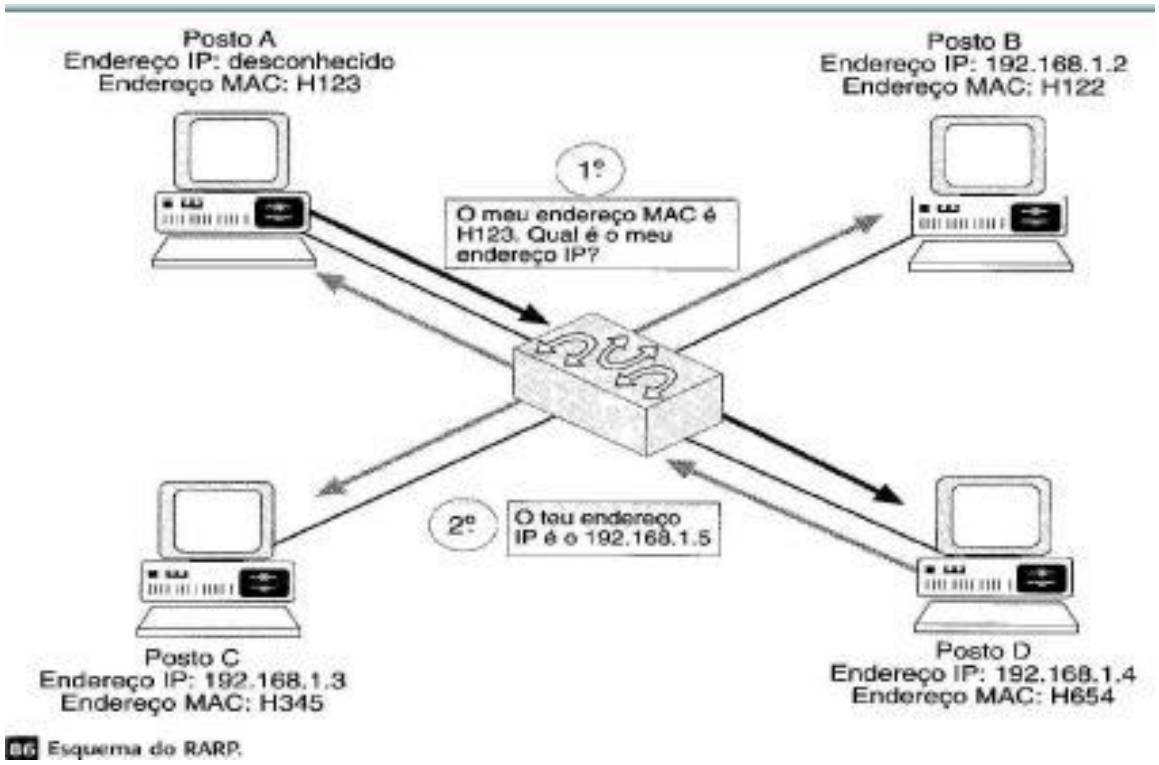
PROTOCOLO ARP

- A resposta está no **ARP** (Address Resolution Protocol) que funciona deste modo:
- quem pretende saber o endereço físico de um host cujo IP conhece, envia um pedido de broadcast para a rede do tipo "Está por aí o host com endereço IP ×. ×. ×. ×?
- Se sim, por favor responda com o seu endereço MAC".
- A resposta permitirá ao emissor endereçar devidamente a mensagem e adaptá-la ao protocolo de baixo nível em que o receptor trabalha.

PROTOCOLO RARP

- Nas redes locais, sobretudo as que têm acesso à Internet, têm normalmente um gateway que lhes dá acesso ao exterior.
- Esse gateway rapidamente fica a conhecer os endereços IP dos computadores que tem na sua rede, ou porque o administrador da rede lhe forneceu a lista ou porque ele tomou nota dos endereços à medida que os foi conhecendo.
- Então, quando um host não se lembra do seu IP, pode perguntá-lo ao seu gateway recorrendo ao protocolo RARP (Reverse ARP).

PROTOCOLO RARP



86 Esquema do RARP.

Figura 16 - Protocolo Reverse ARP

Camada de Transporte do modelo OSI

Objectivo da camada 4

- A camada de transporte é a primeira camada ponto a ponto no modelo OSI, ou seja, o protocolo da camada de transporte é conhecido e trocado entre os *hosts* de origem e de destino da camada, sendo totalmente transparente para a sub-rede de comunicação.
- A função básica dessa camada é aceitar dados da camada de sessão, dividi-los em unidades menores caso necessário, passar essas unidades para a camada de rede e assegurar que todas as unidades cheguem correctamente ao destino.

Objectivo da camada 4

- A camada de transporte oferece à camada superior (sessão) serviços de entrega de dados sem erros, em sequência, sem duplicação ou perda de informação, este é o tipo de serviço mais popular da camada de transporte.
- Contudo, existem outros possíveis tipos de serviço, como o utilizado para mensagens isoladas sem garantia sobre a ordem de entrega e o envio de mensagens em *broadcast*.
- O tipo de serviço a ser usado é determinado quando a conexão é estabelecida.

PROTOCOLO TCP

- O protocolo TCP (Transport Control Protocol) é responsável pelo controlo do fluxo de dados na rede; recebe os dados da camada de rede (IP) e ordena-os, verificando se chegaram todos correctamente.
- Como já referido, as aplicações enviam dados a ser transmitidos pela rede ao protocolo TCP através de canais virtuais de comunicação chamadas portas.
- As portas mais usadas são as apresentadas na tabela seguinte:

PROTOCOLO TCP

PORTA	APLICAÇÃO
15	Netstat
20	FTP (dados)
21	FTP (controlo)
23	Telnet
25	SMTP
43	Whois
80	HTTP

PROTOCOLO TCP

- O protocolo TCP é endereçado pelo nº de IP e o número de porta.
- É desta forma que as aplicações podem "conversar" (na camada de transporte) sem que os dados sejam trocados entre elas.
- Ao receber um pacote de dados, o protocolo TCP envia uma mensagem de confirmação à máquina transmissora, chamada *acknowledge* ou, simplesmente ack.
- Se a confirmação não for recebida após um determinado intervalo de tempo, os dados serão retransmitidos novamente pelo protocolo TCP.

PROTOCOLO TCP

- As características fundamentais do TCP são:
  - Orientado à conexão - A aplicação envia um pedido de conexão para o destino e usa a conexão para transferir dados.
  - Ponto a ponto - uma conexão TCP é estabelecida entre dois pontos.
  - Confiabilidade - O TCP usa várias técnicas para proporcionar uma entrega confiável dos pacotes de dados, que é a grande vantagem que tem em relação ao UDP, e motivo do seu uso extensivo nas redes de computadores. O TCP permite a recuperação de pacotes perdidos, a eliminação de pacotes duplicados, a recuperação de dados corrompidos, e pode recuperar a ligação em caso de problemas no sistema e na rede.

PROTOCOLO TCP

- Full duplex - É possível a transferência simultânea em ambas direcções (cliente - servidor) durante toda a sessão.
- Handshake - Mecanismo de estabelecimento e finalização de conexão a três e quatro tempos, respectivamente, o que permite a autenticação e encerramento de uma sessão completa. O TCP garante que, no final da conexão, todos os pacotes foram bem recebidos.
- Entrega ordenada - A aplicação faz a entrega ao TCP de blocos de dados com um tamanho arbitrário num fluxo (ou stream) de dados, tipicamente em octetos. O TCP parte estes dados em segmentos de tamanho especificado pelo valor MTU. Porém, a circulação dos pacotes ao longo da rede (utilizando um protocolo de encaminhamento, na camada inferior, como o IP) pode fazer com que os pacotes não cheguem ordenados. O TCP garante a reconstrução do *stream* no destinatário mediante os números de sequência.

PROTOCOLO TCP

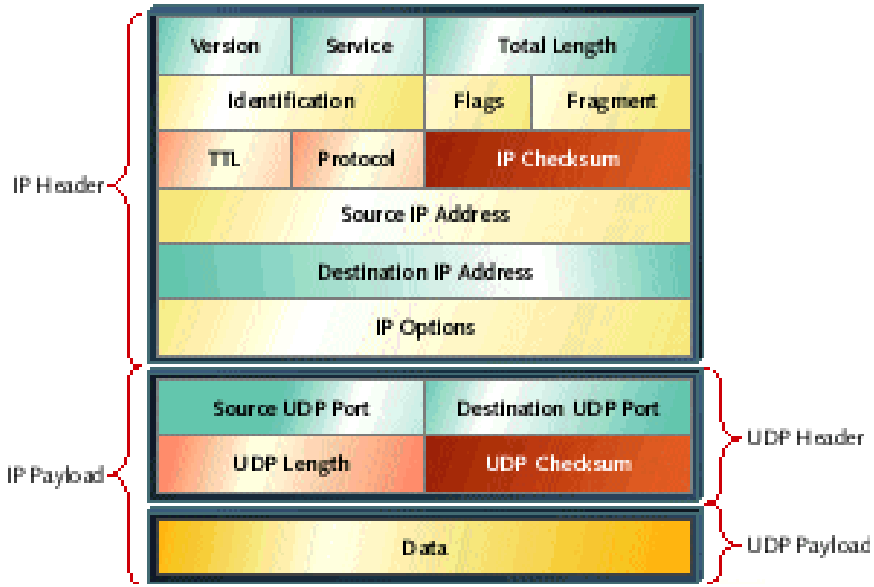
- Controle de fluxo - O TCP usa o campo janela ou *window* para controlar o fluxo. O receptor, à medida que recebe os dados, envia mensagens ACK (*Acknowledgement*), confirmando a recepção de um segmento; como funcionalidade extra, estas mensagens podem especificar o tamanho máximo do buffer no campo (janela) do segmento TCP, determinando a quantidade máxima de bytes aceite pelo receptor.
- O transmissor pode transmitir segmentos com um número de bytes que deverá estar confinado ao tamanho da janela permitido: o menor valor entre sua capacidade de envio e a capacidade informada pelo receptor.

PROTOCOLO UDP

- O User Datagram Protocol (UDP) é um protocolo simples da camada de transporte.
- Ele é descrito na RFC 768 e permite que a aplicação escreva um datagrama encapsulado num pacote IPv4 ou IPv6, e então enviado ao destino.
- Mas não há qualquer tipo de garantia que o pacote irá chegar ou não.
- O protocolo UDP não é confiável.
- Caso garantias sejam necessárias, é preciso implementar uma série de estruturas de controlo, tais como *timeouts*, retransmissões, *acknowlegments*, controle de fluxo, etc.

PROTOCOLO UDP

- Cada datagrama UDP tem um tamanho e pode ser considerado como um registo indivisível, diferentemente do TCP, que é um protocolo orientado a fluxos de bytes sem inicio e sem fim.



PROTOCOLO UDP

- Também dizemos que o protocolo UDP é um serviço sem conexão, pois não há necessidade de manter um relacionamento longo entre cliente e o servidor.
- Assim, um cliente UDP pode criar um socket, enviar um datagrama para um servidor e imediatamente enviar outro datagrama com o mesmo socket para um servidor diferente.
- Da mesma forma, um servidor poderia ler datagramas vindos de diversos clientes, usando um único socket.
- O UDP também fornece os serviços de broadcast e multicast, permitindo que um único cliente envie pacotes para vários outros na rede.

Noções sobre as camadas de Sessão e Apresentação do modelo OSI

A Camada Sessão

- A camada de sessão permite que dois utilizadores em máquinas diferentes estabeleçam uma sessão entre si.
- Uma sessão permite a troca comum de dados, como faz a camada de transporte, porém oferece outros serviços úteis em algumas aplicações.
- Um dos serviços da camada de sessão é gerir a troca de dados.
- Sessões podem permitir que o tráfego seja duplex ou half-duplex.
- Se o tráfego é half-duplex (só tem sentido por vez), então a camada de sessão controla de quem é a vez de transmitir.

A Camada Sessão

- Outro serviço dessa camada é a sincronização da comunicação.
- Para transacções de grande duração no tempo (transferência de grandes arquivos, por exemplo), pode-se optar por uma sincronização periódica associada com a transferência de dados entre as pontas comunicantes.
- Assim, em caso de ocorrência de falha durante a transacção, pode-se reiniciá-la a partir do último ponto de sincronização, não sendo necessário retornar ao início.

A Camada Apresentação

- A camada de apresentação é responsável pela sintaxe dos dados transferidos entre duas entidades de nível 7.
- Um exemplo típico de serviço é a conversão de códigos usados, que podem ser diferentes nas diferentes máquinas que se comunicam.
- É responsável também por outros aspectos de representação da informação.
- Por exemplo, pode-se usar compressão de dados para reduzir o número de bits a serem transmitidos e também criptografia para garantir segurança e privacidade da informação.