

Administração de Redes

Equipamento de rede

Este documento é uma introdução muito básica aos equipamentos de rede mais comuns, a maior parte dos quais iremos utilizar nas aulas de Laboratório de Redes.

Transceiver

Um *Transceiver* (de *Transmitter* + *Receiver*), também designado *Media Attachment Unit* (MAU), é um dispositivo que funciona como receptor e emissor de um dado sinal eléctrico. Existem *transceivers* para amplificar sinais ou para adaptar duas interfaces eléctricas diferentes. Sendo dispositivos que trabalham a nível eléctrico e/ou mecânico, os *transceivers* trabalham na camada física (camada 1) do modelo OSI.



Figura 1: Interface AUI



Figura 2: Transceiver

Nas aulas de Lab. Redes vamos utilizar *transceivers* como os ilustrados na fig. 2 para adaptar a interface AUI (*Attachment Unit Interface* — fig. 1) à interface RJ-45 usada pela norma 10BaseT (Ethernet a 10Mbps).

Hub (concentrador)

Por vezes também designado repetidor, o concentrador (*hub*, em Inglês) é um dispositivo que permite interligar uma série de dispositivos Ethernet para que funcionem como um único segmento de rede (domínio de colisão). Uma rede constituída por uma série de dispositivos Ethernet interligados através de um *hub* tem uma topologia em estrela a nível físico, mas a nível lógico tem uma topologia em barramento (segmento partilhado).

Tal como os *transceivers*, os *hubs* funcionam na camada de ligação física (camada 1) do modelo OSI. Embora na versão mais pura um *hub* apenas seja capaz de interligar interfaces a funcionar à mesma velocidade, existem *dual-speed hubs* capazes de interligar segmentos a 10Mbps com segmentos a 100Mbps. No entanto, se quisermos ser preciosistas, estes dispositivos são híbridos entre *hubs* e *bridges* ou comutadores (discutidos mais adiante), pois não existe um único segmento de rede, mas dois — um a 10Mbps e outro a 100Mbps. O conjunto destes dois segmentos funciona como um único domínio de difusão, mas cada um dos segmentos é um domínio de colisão separado.

Existem duas classes de *hubs* Fast-Ethernet: classe I e classe II. A diferença reside no facto de os primeiros recuperarem o sinal para uma forma digital para o retransmitir, enquanto os segundos apenas amplificam e reenviam o sinal recebido de forma analógica. Uma vez que os *hubs* classe I introduzem um atraso superior (máx. 140 bits) aos classe II (máx. 92 bits), pode existir um único *hub* classe I entre qualquer par de máquinas numa rede, mas podem existir dois *hubs* classe II.



Figura 3: Fast-ethernet hub



Figura 4: SOHO fast-ethernet mini-hubs

Bridge

A *bridge* é um dispositivo que permite interligar dois segmentos de rede, unindo dois domínios de colisão num único domínio de difusão. Uma *bridge* “aprende” que endereços MAC se encontram de um lado e do outro; uma trama recebida de um segmento é retransmitida no outro se (1) se destinar a um endereço MAC que a *bridge* sabe estar do outro lado, (2) se destinar a um endereço MAC de difusão (*broadcast* ou *multicast*) ou (3) se destinar a um endereço MAC ainda desconhecido. Para evitar ciclos de retransmissão em redes com várias *bridges*, estas correm um algoritmo para gerar uma *spanning tree*, utilizada para o reenvio de tramas incluídas nos casos (2) e (3).

As tramas são recuperadas para uma memória antes de (eventualmente) serem retransmitidas pela *bridge*, o que possibilita a interligação de segmentos que operem a velocidades diferentes. Uma vez que trabalha ao nível da trama e faz filtragem através de endereços MAC, a *bridge* opera na camada de ligação lógica (camada 2) do modelo OSI.



Figura 5: Bridge ethernet 10base2 (coaxial)



Figura 6: Bridge ethernet 10base2/10baseT

Switch (comutador)

Embora o termo *switch* possa referir-se a diferentes tipos de dispositivos que trabalham em diferentes camadas do modelo OSI — um comutador ATM (*Asynchronous Transfer Mode*) trabalha na camada de rede (camada 3), e historicamente utilizou-se o termo *packet switch* para designar *routers* — no uso mais frequente, hoje em dia, refere-se a dispositivos que comutam tramas, efectuando auto-aprendizagem e filtragem com base nos endereços MAC. No fundo, um comutador Ethernet é uma *bridge* com múltiplas portas. É, portanto, um dispositivo que opera na camada de ligação lógica (camada 2) do modelo OSI.



Figura 7: Computador fast-ethernet

Em termos de aspecto, um computador Ethernet é muito semelhante a um *hub*, como pode ver-se na fig. 7; por vezes, a única maneira de os distinguir visualmente é pelo fato de ter escrito *hub* ou *switch*...

Uma funcionalidade disponibilizada pela maioria dos computadores (excepto os de pequena dimensão destinados a uso em *SOHO*) é a divisão da rede em diferentes domínios de difusão, designados VLAN (LAN virtuais). Do ponto de vista lógico, diferentes VLAN funcionam como se fossem redes independentes com cablagem e equipamentos separados; como não há ligação directa entre máquinas pertencentes a diferentes VLAN, a comunicação entre elas tem que ser feita através de um *router*¹ (ver abaixo). A atribuição de uma porta (física) do computador a uma dada VLAN pode ser feita através de configuração (VLAN estáticas), ou então de forma automática (VLAN dinâmicas) com base em critérios como o endereço MAC da máquina ligada na porta (critério de camada 2) ou do seu endereço IP (critério de camada 3), ou ainda através do protocolo 802.1x. É ainda possível que numa porta circulem tramas de diferentes VLAN; esta funcionalidade designa-se *VLAN Trunking*, e é frequentemente usada em portas que interligam dois computadores, obrigando a adicionar a cada trama uma etiqueta (*VLAN tag*) indicando a VLAN a que pertence (processo especificado na norma 802.1Q).

Ponto de acesso

Os pontos de acesso usam-se para interligar segmentos de rede sem fios (*wireless*) entre si ou a segmentos de rede cablada. Um ponto de acesso é, portanto, uma *bridge* em que pelo menos um dos segmentos é sem fios. Os pontos de acesso funcionam na camada de ligação lógica (camada 2) do modelo OSI.



Figura 8: Ponto de acesso 802.11

Router

O *router* é um dispositivo que permite interligar redes diferentes. A função primordial de um router é o reenvio (*forwarding*) de pacotes entre as suas diferentes interfaces. No entanto, para desempenhar esta função, os *routers* necessitam de manter tabelas de encaminhamento. Para o

¹ Alguns computadores são capazes de detectar os endereços IP em uso nas suas VLAN e encaminhar pacotes entre elas, prescindindo assim de um *router* (salvo para comunicação com o exterior).

fazerem de forma autónoma e distribuída, os *routers* correm um ou mais protocolos de encaminhamento (*routing*) que lhe permitem preencher e actualizar as suas tabela de encaminhamento. Enquanto o reenvio de pacotes é uma função do plano de dados, o encaminhamento é uma função do plano de controlo. Além destas duas funções, a esmagadora maioria dos *routers* suporta muitas outras (NAT, DHCP, etc.); contudo, são estas as fundamentais e as que lhe dão o nome.

Os *routers* transportam os pacotes (datagramas) desde o terminal de origem até ao terminal de destino. Trabalham, portanto, na camada de rede (camada 3) do modelo OSI.



Figura 9: Mini-router com 1 porta WAN, 1 LAN e 1 wireless



Figura 10: Routers de acesso (Cisco 2500)



Figura 11: Router de core (Cisco CRS-1)

NAT Box

Embora possa existir num equipamento independente (NAT box), a função NAT está quase sempre integrada num *router* ou numa *firewall*. A versão mais simples do NAT (tradução apenas de endereços IP) funciona na camada de rede (camada 3) do modelo OSI; versões mais elaboradas (NAPT, *masquerading*) funcionam nas camadas de rede e de transporte (camadas 3 e 4).

Firewall

Uma *firewall* é um dispositivo que inspecciona o tráfego que a atravessa e, mediante um conjunto de regras, permite ou nega a passagem a determinados pacotes. A *firewall* intercala-se entre a rede interna e a rede externa, isolando a primeira da segunda por motivos de segurança — pode permitir-se o acesso à rede externa por parte de máquinas da rede interna, mas normalmente nega-se o acesso de máquinas da rede externa à rede interna. Além destas duas zonas, normalmente as *firewalls* suportam uma terceira, designada zona desmilitarizada (DMZ), na qual se colocam máquinas às quais se permite o acesso (embora restrito) a partir do exterior.

As *firewalls* de primeira geração efectuavam apenas uma filtragem *stateless*; as de segunda geração podem manter informação de estado para as conexões que as atravessam e efectuar a filtragem com base não apenas em pacotes individuais, mas também na relação de cada pacote com os anteriores da mesma conexão (*stateful*); as de terceira geração podem, adicionalmente, entender (pelo menos parcialmente) alguns protocolos de aplicação (http, ftp, DNS, protocolos P2P) e, assim, detectar se pacotes de algum protocolo indesejado estão a circular numa porta não-standard ou se algum serviço está a ser atacado usando o protocolo de uma forma que se sabe ser nociva.

As *firewalls* trabalham pelo menos nas camadas de rede e de transporte (camadas 3 e 4) do modelo OSI, embora algumas possam usar também critérios de camadas superiores.



Figura 12: Firewall Cisco PIX



Figura 13: Firewall Nokia para montagem em rack

Servidor

Um servidor é um dispositivo que disponibiliza um ou mais serviços de rede a clientes, segundo o modelo cliente/servidor. Muito embora o termo servidor se associe, normalmente, a máquinas de grande capacidade e fiabilidade, nem todos os servidores encaixam neste estereótipo (sobretudo a nível de capacidade) — é possível construir servidores com base em *hardware* comum. De facto, uma vez que não necessitam de uma interface gráfica, os servidores dispensam aquele que, hoje em dia, é o subsistema mais complexo e consumidor de recursos num computador pessoal ou *workstation* — o subsistema gráfico.

Os servidores trabalham nas camadas superiores (5 a 7) do modelo OSI (camada 5, ou de aplicação, no modelo TCP/IP).



Figura 14: Servidor modular da Sun



Figura 15: Servidor HP ProLiant



Figura 16: Servidor PicoLinux

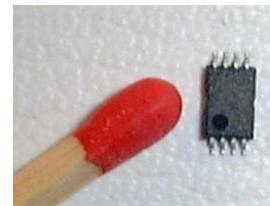


Figura 17: Servidor *web* num único chip — o mais pequeno do mundo?