2ª EDIÇÃO

ADRIANO **AFONSO**
ANDRÉ **MOREIRA**
FRANCISCO JOSÉ **SILVA**
JOÃO **COITO**
JORGE **RUÃO**
PAULO **GALVÃO**
PEDRO **JESUS**
TIAGO **CARRONDO**

MANUAL ABERTO DE REDES DE TELECOMUNICAÇÕES

Direitos de autor

Ficha Técnica

Título: Manual Aberto de Redes de Telecomunicações

Capa: BY-CC

Versão 2.1.1 | 06-09-2014 | 2ª Edição

Editor:

ISBN:

Autor(es)

Adriano Afonso André Moreira Pedro Jesus Tiago Carrondo

Comentários

Envie os seus comentários ou sugestões sobre este documento para:

www.libreoffice.pt | Adriano Afonso | *adrianoafonso@libreoffice.org*

Contribuidores

Francisco José Silva Jorge Ruão Paulo Galvão João Coito

Acordo Ortográfico

Escrito segundo o Acordo Ortográfico da Língua Portuguesa de 1945.

Índice

Índice de Ilustrações

Introdução

> O legado da distância como o preço fundamental das comunicações pode muito bem se comprovar como a influência mais significativa a delinear o próximo meio século. Seus efeitos serão tão penetrantes quanto os da descoberta da electricidade.
>
> *The Economist*, 30 de Setembro de 1995.

As redes locais, na evolução das tecnologias de comunicação, vieram dar resposta a vários tipos de operações, tais como as simples comunicações entre terminais e *mainframes*[1], comunicações entre computadores, a transmissão de dados, de voz e/ou vídeo, o controlo de processos e automatização dos procedimentos em escritórios, entre muitas outras.

As suas funções na actualidade são várias, mas focam-se sobretudo no intercâmbio de dados, mensagens e de informação, através de inúmeras de ferramentas de comunicação como é o exemplo do correio electrónico e dos mensageiros (*MSN Messenger*, *Google Talk*, *ICQ*, etc.). Outras funções podem ser atribuídas através de servidores dedicados para a partilha de diversos recursos, tais como a partilha de programas, de acesso a bases de dados, a partilha de documentos e a partilha de periféricos (impressoras, discos, drives, leitores suportes ópticos, etc.).

Uma rede local pode ser distinguida através da sua geografia, da sua função e respectivos serviços que oferece, da topologia da rede, do meio de transmissão, da sua arquitectura e dos protocolos[2] utilizados.

Qualquer que seja a sua aplicação, devem ser levados em consideração vários factores para a sua correcta identificação, dentro dos quais: dispersão geográfica, ambiente operativo, número máximo de nós, distância máxima e mínima entre os nós, tempo de resposta, tipo de informação transmitida, tipo de interacção entre dispositivos, taxa máxima de informação transmitida, fiabilidade exigida, tipo de tráfego, etc.

Conceito de Rede

Antes de mais, é necessário definir o conceito de rede que se entende por: dois ou mais nós (computadores) ligados entre si, através de meios de transmissão (cabo, linhas telefónicas, sem fios), e respectivos dispositivos de conectividade, controlados por *software* adequado, com o objectivo de trocarem informação de forma rápida e fácil, permitindo aos utilizadores a partilha de equipamentos e de recursos (aplicações, ferramentas de comunicação, bases de dados, etc.).

---

1 *Mainframes* são computadores capazes de realizar operações a grande velocidade sobre um grande volume de dados. Os mainframes provêem dos antigos computadores de grandes dimensões que necessitavam de ambientes especiais para o seu funcionamento (devido ao seu elevado aquecimento), actualmente possuem o mesmo tamanho dos demais servidores de grande porte mas com um menor consumo de energia eléctrica.

2 Na ciência da computação, um protocolo é uma convenção ou padrão que controla e possibilita uma conexão, comunicação, transferência de dados entre dois sistemas computacionais. De maneira simples, um protocolo pode ser definido como "as regras que governam" a sintaxe, semântica e sincronização da comunicação. Os protocolos podem ser implementados pelo hardware, software ou por uma combinação dos dois.

Para que uma comunicação possa acontecer são então necessários os seguintes componentes básicos:

- Emissor;
- Meio de transmissão;
- Dispositivos de conectividade;
- Mensagem;
- Receptor.

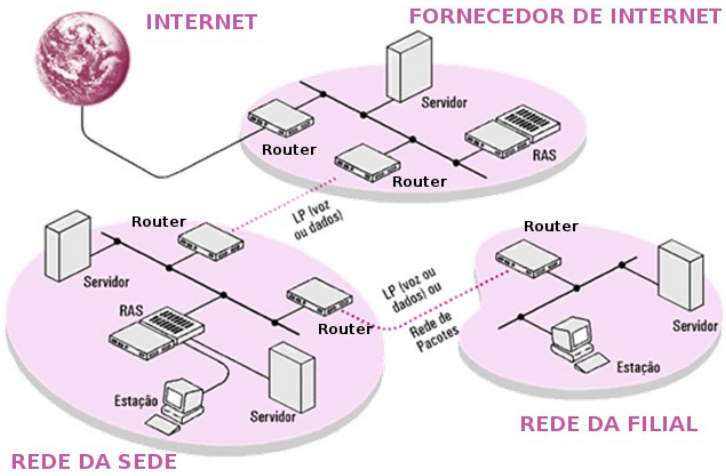

Ilustração 1: Esquema de uma rede empresarial

Vantagens de uma rede

A implementação de uma rede num ambiente empresarial pode trazer uma série de vantagens. De seguida identificam-se algumas das mais comuns.

- Centralizar/Descentralizar operações
  - Pode ser feita uma reorganização da arquitectura do processamento, como por exemplo: a especialização de computadores para cálculos específicos, a disponibilização de um centro controlo industrial e a partilha de uma aplicação com funções comerciais;
  - Pode-se coordenar (com dados actualizados) os vários ramos de uma organização a partir de uma aplicação, e até mesmo a evolução do seu desenvolvimento.
- Maior eficiência na distribuição e partilha de recursos;
  - O acesso a uma grande quantidade de informação está logo à partida assegurado, assim como a partilha dessa informação por vários utilizadores, tudo isto independente da distância a que se encontram os terminais.
  - Através de uma rede é possível vários utilizadores, cada qual no seu posto de trabalho, acederem a um mesmo programa localizado num dos computadores de rede, bem como terem acesso a dados (documentos, bases de dados, etc.) localizados noutros computadores através da partilha de recursos de Hardware, de periféricos e armazenamento, de recursos de Software e de software especifico.
  - A disponibilização e partilha de acessos a redes locais e à Internet.

- Melhoria dos processos organizacionais.
  - Gestão de diferentes níveis de acesso (consoante estatuto ou função do utilizador na rede);
  - Supervisão e controlo de trabalho, e de acessos à rede;
  - Constituição de Grupos de trabalho;
  - Calendarização de tarefas;
  - Troca de mensagens e de informação;
  - Facilitação da manutenção do parque informático através de administração remota;
  - Torna-se mais fácil a gestão de cópias de segurança.

Tipos de Redes

Considerações iniciais

A Tipologia de redes caracteriza-a quanto à sua dimensão e dispersão geográfica. Esta pode-se apenas confinar a uma sala onde por exemplo, são partilhados de dispositivos entre vários computadores. Pode também estar distribuída por dentro de um edifício onde por exemplo integra um serviço de escritório, ou uma área coberta por vários edifícios como é o caso dos *campus* universitários, áreas fabris, ou mesmo até uma pequena cidade.

Esta dispersão geográfica, como se irá verificar, é fundamental para a escolha da topologia e respectivos meios de transmissão, como também é um factor chave na escolha e/ou implementação de alguns tipos de protocolos.

O ambiente em que a rede irá operar influencia também a escolha dos seus meios de transmissão e respectiva topologia. Os ambientes propensos a ruídos (entenda-se interferências) e com problemas de gestão de espaço e segurança (i.e. húmidos, poeirentos, etc.) têm diferentes requisitos. A ocorrência de erros de transmissão resultantes do ruído envolvente exigirá, dos protocolos, mecanismos de detecção e recuperação desses mesmos erros.

O número máximo de nós, a distância de separação entre estes e a taxa máxima de dados transmitidos são requisitos que influenciam também estas escolhas. Em alguns tipos de topologia, a ligação ao meio de transmissão é um factor limitador do número de nós que uma rede pode suportar, assim como a distância máxima e mínima entre estes. Isto significa que em determinada topologia e determinado meio de transmissão poderemos ter uma distancia, mas noutra topologia com o mesmo meio de transmissão, a distancia entre nós pode ser muito superior. A escolha dos protocolos de transmissão também é directamente afectada por estes factores. O seu perfeito funcionamento, por vezes, depende igualmente da distância entre nós.

No à escolha dos protocolos diz respeito, normalmente existe uma exigência face ao tempo de resposta máximo bem como ao tipo ou quantidade de tráfego. Para programas que informam sobre o controlo de processos e aplicações que necessitem de comunicação em tempo real, a garantia de um tempo de resposta baixo é uma característica fundamental. Infelizmente, em qualquer transmissão, por qualquer meio, existe sempre uma possibilidade de um erro, o que causará uma limitação no tempo de resposta. Em muitas aplicações no entanto, é importante que este problema não seja causado pelo tipo de protocolo utilizado.

A quantidade de tráfego da rede relaciona-se directamente com a função da entidade que a detém. Pode variar simplesmente desde pequenas mensagens até quantidades volumosas de dados que precisam de ser transmitidos continuamente. É aqui que entra o conceito de fiabilidade. A fiabilidade de uma rede define-se pela sua capacidade de responder na totalidade a todos os requisitos. Também está relacionada tanto com a escolha do meio de transmissão, como com a topologia e o seu respectivo protocolo.

O tipo de informação transmitida através de uma rede pode ser desde simples dados, vídeo e/ou voz. Os diversos meios de transmissão vão diferir na capacidade de suportar: a natureza do sinal analógico ou digital; a frequência; a quantidade de informação transmitida; os requisitos de tempo real; de isenção de erros, etc.

Sempre que possível, a transmissão de dados entre os vários nós ou dispositivos deve ser isenta de erros. Aquando do erro, deve ser requerida uma retransmissão, a qual tem de ser suportada pelo protocolo utilizado. As transmissões de voz e de vídeo, em geral, devem ser efectivadas sem interrupção (tolerante a erros).

Desenhar uma rede que possa integrar e suportar muitos destes tráfegos heterogéneos é sempre desejável por razões económicas e operacionais. É importante que os equipamentos e os meios de transmissão sejam escaláveis, para assim poder dar resposta adequada a aplicações tais como a tele-conferência, que requer uma transmissão interrupta de dados (áudio e vídeo).

Regressando agora à tipologia das redes, esta caracteriza-se geralmente por cinco domínios respectivamente à cobertura geográfica.

PAN

Rede de área pessoal, traduzido de *Personal Area Network,* é uma rede local de acesso e transmissão de dados pessoais. É tipo de rede composta por poucos nós muito próximos uns dos outros, geralmente a uma distância não maior que uma dezena de metros.

Ilustração 2: Personal Área Network

Normalmente é associada às seguintes tecnologias de transmissão de dados:

- Irda (infravermelhos);
- Bluetooth;
- Wifi;

LAN

Rede de área local é o nome dado às redes cuja área de abrangência é limitada a uma área residencial, de um escritório ou a uma empresa (sala, piso ou prédio).

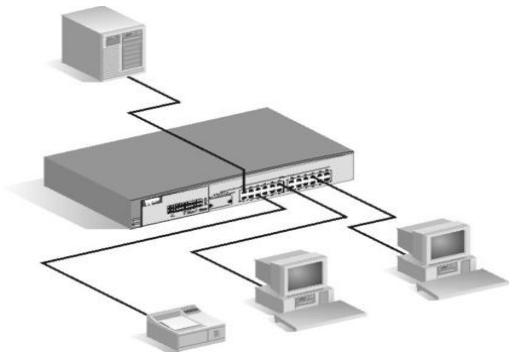

Ilustração 3: Local Area Network

Campus

As redes denominadas de Campus abrangem a extensão de vários prédios situados dentro de uma mesma região metropolitana (entre 10 a 100km). São associadas normalmente a redes que interligam diversos edifícios de uma mesma empresa, de uma universidade ou de uma organização.

MAN

Nome atribuído às redes que ocupam o perímetro de uma cidade. Permitem que empresas com filiais em locais diferentes da sede se interliguem entre si.

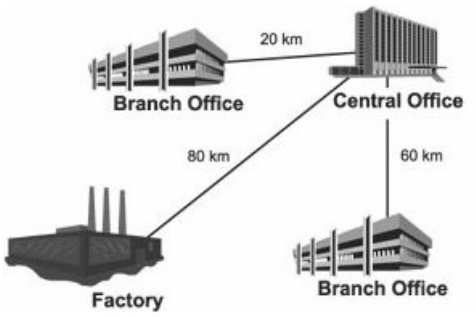

Ilustração 4: Metropolitan Area Network

WAN

As redes onde as estações de trabalho estão geograficamente distribuídas são denominadas por WAN. Estas redes permitem abranger largas distâncias, como um país ou continente. São normalmente formadas por várias LAN (aqui entenda-se como sub-redes). As WAN associam-se também ás infra-estruturas de satélites, fibra óptica, etc. que são geralmente de utilidade pública.

Ilustração 5: Wide Area Network

WLAN

As *Wireless* LAN (LAN sem fios) consolidaram-se como uma boa opção de rede local (LAN) onde exista necessidade de mobilidade de pontos de rede e/ou existam dificuldades de implementação de cablagem.

Uma ligação sem fios permite que aos computadores portáteis a mobilidade necessária sem sacrificar muitas das vantagens de estarem ligados a uma rede. Virtualmente, tais máquinas podem ser usadas em qualquer lugar dentro de um prédio que possua uma *Wireless* LAN implementada.

Estas redes podem combinadas com LAN cabladas, onde os pontos que necessitam de mobilidade são ligados à rede pelo meio sem fios e as estações fixas estão ligadas à rede física.

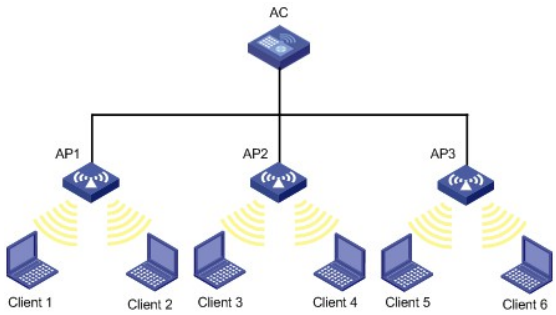

Ilustração 6: Wireless Local Area Network

Distância Entre Nós	Localização dos Nós	Nome das Redes
~1-10m	Desktop, ligação entre PC´s.	PAN - *Personal Area Network*
~ 10m	Sala, interligação no mesmo espaço.	LAN - *Local Area Network*
~ 100m	Prédio, interligação entre andares	LAN - *Local Area Network*
~ 2km	Campus, interligação entre edifícios.	*Campus*
~ 30-50km	Cidade, interligação entre espaços da mesma cidade.	MAN - *Metropolitan Area Network*
~ 100km	País, interligação entre cidades.	WAN - *Wide Area Network*
~ 1000km	Continente, interligação entre continentes.	WAN - *Wide Area Network*
~ 10.000km	Planeta, a Internet.	WAN - *Wide Area Network*
~ 100.000km	Sistema terra – espaço, terra e satélites artificiais.	WAN - *Wide Area Network*

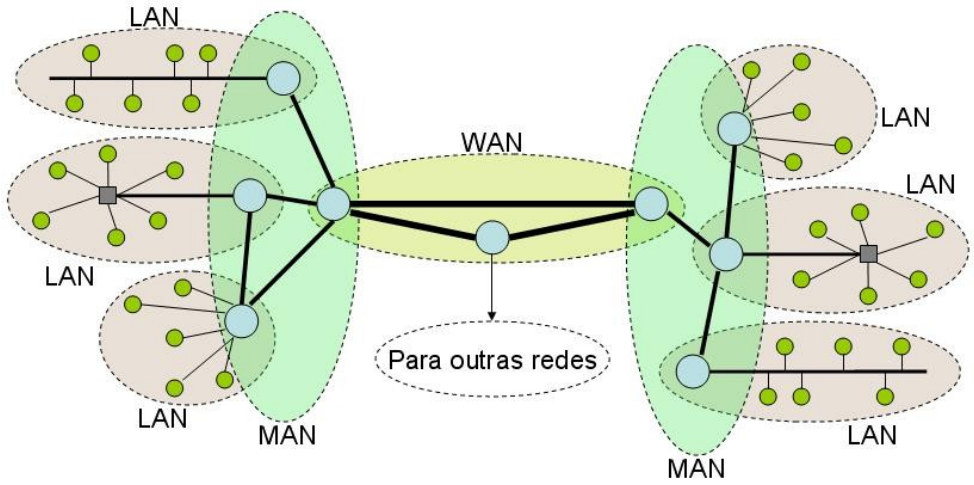

Ilustração 7: Interligação entre os vários tipos de rede

Topologias de Redes

Conforme anteriormente descrito, as redes locais constituem-se a partir de um conjunto de estações (nós) interligadas por um sistema de comunicação. Este sistema compõe-se num arranjo topológico que interliga os vários nós através de um conjunto de regras de forma a organizar a comunicação. Em suma, a topologia define a forma pela qual os vários componentes que compõem uma rede se interligam.

A topologia abrange dois principais campos: o físico e o lógico. O primeiro pode entender-se como a configuração da cablagem. O segundo, que diz respeito à configuração lógica dos equipamentos, descreve como a informação é tratada dentro da rede, como circula de um nó para o outro.

Bus/Barramento

Rede em que há exactamente dois nós terminais, um número qualquer de nós intermédios e um só caminho entre cada dois nós (todos os nós da rede se encontram ligados uns aos outros numa linha). O desenho desta rede é relativamente simples reduzindo-se a um único cabo que se estende de um nó até ao seguinte. Os extremos do cabo terminam com uma resistência chamada terminador que para além de indicar que não existem mais estações de trabalho nos extremos, permite encerrar o *Bus.*

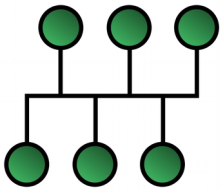

Ilustração 8: Topologia Bus

Esta rede utiliza uma transmissão em *broadcasting*, o que significa que quando um nó envia uma transmissão, a mesma é enviada para todos os nós da rede em simultâneo, tendo cada nó

que verificar se a informação lhe é destinada. Caso a informação tenha sido recebida sem anomalias é enviado um aviso de recepção ao nó emissor.

Ring/Anel

Numa rede em anel os nós estão ligados entre si através de um cabo que passa por todos, de forma sequencial, descrevendo uma circunferência (anel).

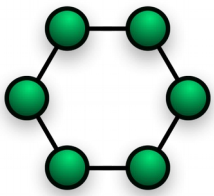

Ilustração 9:
Topologia Anel

A informação passa de nó em nó através da circunferência. O percurso é único e singular. Cada nó verifica se a informação em causa lhe é destinada e processa-a. Caso contrário remete-a para o nó seguinte que efectua o mesmo procedimento até que seja encontrado o nó destino da transmissão (tipo “passagem de testemunho”).

Star/Estrela

O desenho de rede em estrela é uma das primeiras configurações de rede. Todas as estações de trabalho estão conectadas a um nó central (concentrador/*hub*/*switch*) que funciona como distribuidor de todas as transmissões efectuadas pelos restantes nós, formando uma estrela física.

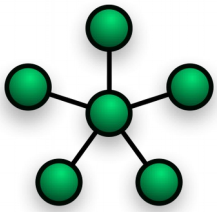

Ilustração 10:
Topologia Estrela

Cada vez que se pretende estabelecer comunicação entre dois computadores, toda a informação transferida de um para o outro nó, passa primeiro pelo nó central.

Tree/Árvore

Topologia com base numa estrutura da rede em que são utilizados diversos dispositivos de centralização (da topologia *Star*/Estrela), permitindo assim uma estruturação hierárquica de redes e sub-redes.

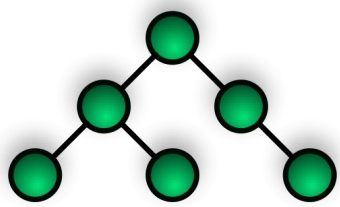

Ilustração 11: Topologia Árvore

Backbone

Caracteriza-se pela existência de uma ligação que desempenha o papel de *Backbone*. Esta ligação pode conter um ou mais cabos, normalmente de elevado desempenho que cobre determinada área, mais ou menos, extensa, ao qual se ligam diversas redes ou sub-redes, através de dispositivos de interligação.

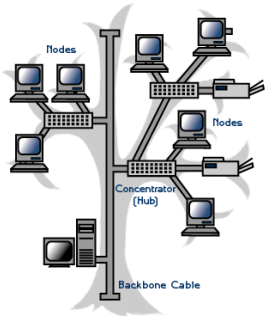

Ilustração 12:
Topologia Backbone

As redes Backbone podem assumir uma topologia *Bus* ou *Ring,* bastante adequada a redes de dimensão intermédia, (Campus, MAN), que normalmente, são constituídas por diversas sub-redes e indicada para redes que necessitam de estar em comunicação umas com as outras numa base regular ou permanente.

Na tabela seguinte apontam-se, de modo muito genérico, algumas vantagens e desvantagens das diferentes topologias de rede.

Topologia	Pontos Positivos	Pontos Negativos
Bus/Barrramento	- Simples e fácil de instalar. - Requer normalmente pouca cablagem. - Fácil de ampliar.	- A rede fica mais lenta em períodos de uso intenso. - Os problemas são difíceis de isolar.
Ring/Anel	- Razoavelmente fácil de instalar. - Requer normalmente pouca cablagem. - Desempenho uniforme. - Se um nó falha, a rede pode compensar no sentido inverso.	- Os problemas são difíceis de isolar. - Em topologias mais antigas, se um nó falhava, todos os restantes paravam.
Star/Estrela	- É mais tolerante a falhas, a falha de um nó “filho” não afecta os restantes. - Fácil de acrescentar novos nós. - Gestão centralizada.	- Custos acrescidos dos passivos (cabos) pela necessidade de interligação de todos os nós ao ponto central. - Se o ponto de centralização falha, a rede falha.

No caso de redes mais complexas, é frequente observar-se a utilização de redes em Árvore, Anel e Estrela em conjunto. Apesar da desvantagem do aumento de complexidade (e custo) da rede e da sua configuração, é possível atingir elevados níveis de robustez e fiabilidade, para além da escalabilidade.

Meios de Transmissão

A generalidade das redes locais utiliza meios de transmissão que mantêm os dados no formato digital. Porém em alguns casos, como é o exemplo da rede telefónica tradicional, os sinais são transmitidos em formato analógico. Decorrente deste facto, existe a necessidade da utilização de um modem[3].

Um meio físico de transmissão numa rede de computadores é o canal de comunicação pelo qual os nós enviam e recebem os sinais que transportam a informação. É comum numa instalação de rede a utilização de vários tipos de cabos ou mesmo de meios de transmissão.

Porém também existem redes e sistemas de comunicação entre nós que funcionam sem fios, através da propagação de ondas no espaço. É chamada de comunicação *wireless* ou sem fio.

Na altura de escolher um cabo para uma rede deve ter-se em atenção o seguinte:

- Velocidade de transmissão pretendida;
- Distância máxima entre as máquinas a conectar;
- Nível de ruído e interferências na zona de instalação da rede.

Interferências nas transmissões

Nenhum meio de transmissão é capaz de transmitir sinais sem que haja perdas de energia durante o processo.

Assim sendo, as transmissões podem sofrer interferências de diferentes proveniências. As mais significativas são:

- Interferência eletromagnética (EMI): campos magnéticos;
- Interferência radiofrequência (RFI): transmissores de rádio, relés e comutadores, termostatos e lâmpadas fluorescentes.

A tabela abaixo apresenta algumas das fontes de interferência mais comuns:

Tipo	Faixa	Fonte
Baixa frequência	10 KHz a 150 KHz	Lâmpadas fluorescentes Aquecedores
Média frequência	150 KHz a 100 MHz	Rádio Dispositivos eletrónicos Esterilizadores de ar
Alta frequência	160 MHz a 1 GHz	Rádio e TV Computadores Dispositivos eletrónicos Sensores de movimento Radares

3 Este equipamento será caracterizado posteriormente.

Tipo	Faixa	Fonte
Impulso	10 KHz a 100 MHz	Motores Comutadores Máquinas de solda Ignição eletrónica

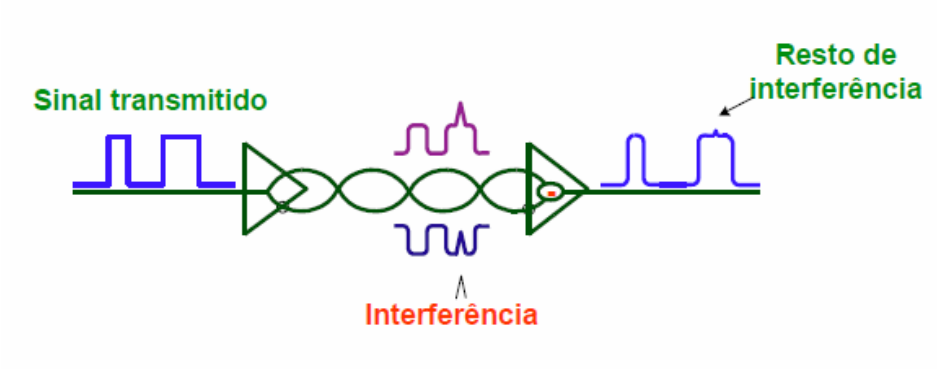

Ilustração 13: Interferência

Atenuação

A atenuação ocorre com qualquer sinal, tanto digital como analógico, transmitido através de cabos. Quanto maior for o comprimento do cabo, maior é a atenuação, até ao ponto do sinal se tornar cada vez mais fraco e deixar de ser entendido pelo destinatário. Utilizam-se repetidores ou outros equipamentos similares para aumentar a força do sinal.

Diafonia ou crosstalk

Ocorre quando o receptor num canal de comunicações recebe inadvertidamente informação enviada pelo canal de comunicação adjacente. O *crosstalk* é o ruído ou interferência causada por acoplamento magnético entre dois caminhos de sinal. Nas frequências de áudio, o *crosstalk* é conhecido como diafonia ou popularmente como “linha cruzada”.

Tipos de Cablagem

Cabo Coaxial

Este tipo de cabo foi durante muitos anos o meio por excelência utilizado na troca de dados entre dois ou mais nós. Hoje existem vários tipos de cabos coaxiais, cada um com as suas características específicas, mas deixaram de ser utilizados como meio de transmissão nas redes locais. Hoje em dia são usados nas infraestruturas domésticas para transmissão de sinal TV, Internet e/ou telefone.

Utilizado nas redes locais é bastante durável mas não muito flexível, podendo transmitir até 10Mb/s. Consiste num núcleo de cobre envolvido por um material isolante, por sua vez envolvido num revestimento de plástico. O núcleo é usado para transportar dados enquanto que o condutor externo serve como escudo e protege o primeiro de interferências externas.

Uma das características é a sua grande capacidade de imunidade a ruídos electromagnéticos (de baixa frequência) e por isso foram largamente utilizados nos meios transmissão em redes locais.

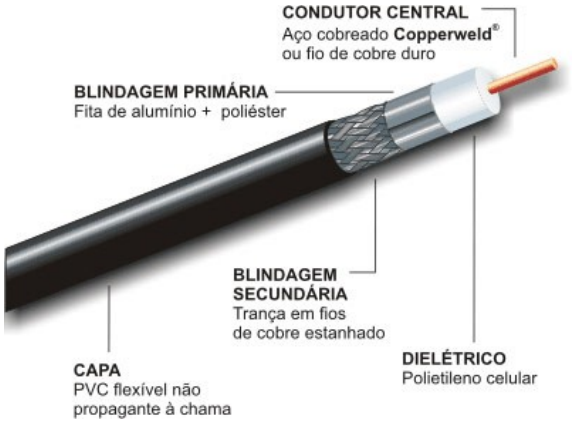

Ilustração 14: Cabo Coaxial

Ao contrário do cabo UTP[4] que será analisado de seguida, este mantém uma capacidade de tráfego constante, independente do seu comprimento. Por esta razão oferece apenas velocidades da ordem dos megabits/seg (Mb/s), não sendo necessária a regeneração do sinal, não tendo distorção ou eco.

As ligações dos cabos coaxiais causam uma reflexão do sinal, por isso, a colocação destes nas ligações multi-ponto deve ser controlada de forma a garantir um baixo índice de reflexões.

A maioria dos sistemas de transmissão em Baseband (banda base) utiliza cabos de impedância com características de 50 Ω[5] (geralmente utilizados nos sistemas de TV por cabo e em redes de banda larga) porque este tipo de transmissão sofre menos reflexões.

UTP/STP/FTP (Par Trançado)

É um cabo com boas características de transmissão (de 10Mb/seg a 10Gb/seg), de baixo custo nas categorias mais baixas, utilizado em redes locais e alargadas. Os cabos de par trançado possuem dois ou mais fios entrelaçados em espiral com o objectivo de criar à sua volta um campo electromagnético que reduz a possibilidade de interferências de sinais externos. Um dos condutores transmite o sinal e o outro recebe e podem suportar transmissões tanto analógicas como digitais.

A massificação da utilização deste tipo de meio de transmissão deve-se à falta de flexibilidade de outros cabos e à urgência e necessidade de um meio físico que pudesse debitar uma taxa de transmissão mais alta e mais rápida.

Embora o conceito do par traçado seja diminuir o ruído externo, a desvantagem deste tipo de cabo é e continua a ser a sua susceptibilidade às interferências a ruídos (electromagnéticos e de radio frequência). Porem, estes efeitos podem ser minimizados com a escolha de uma versão com blindagem e de uma categoria mais alta.

4 *Unshielded Twisted Pair* ou cabo par trançado como é conhecido em Português.
5 Lê-se “Óhm”, unidade de medida da resistência eléctrica, padronizada pelo SI (Sistema Internacional de Unidades).

Ilustração 15: Cabo UTP e S/FTP

Existem ainda versões com diferentes blindagens por camadas, consoante a categoria. No caso da imagem, o cabo da direita é na realidade um S/FTP porque é blindado com malha exterior, e depois cada par traçado blindado individualmente com folha de alumínio.

Letra	Designação
U	De *unshielded*, sem blindagem
F	De *foiled shielding*, blindagem com folha de alumínio
S	De *braided shielding*, blindagem em malha

Os cabos com as diferentes blindagens são normalmente utilizados em ambientes industriais onde existem grandes quantidades de fontes de interferências. Esta interferência é reduzida através da blindagem. Por sua vez, os cabos sem blindagem são utilizados em ambientes onde as fontes de interferência não são tão comuns, ou não é necessária a devida protecção.

A tabela seguinte apresenta as actuais nomenclaturas para os diferentes tipos de cabos e respectivas blindagens. È normal encontrar diferentes nomenclaturas e diferentes descrições em diferentes autores, e por isso é apresentada na primeira coluna o ISO, e na segunda os acrónimos industriais mais utilizados. A terceira e quarta coluna descrevem o tipo de blindagem.

ISO/IEC 11801	Acro. Industriais	Blindagem Cabo	Blindagem Par
UTP	UTP	Sem	Sem
F/UTP	FTP, STP, ScTP	Folha	Sem
S/UTP	STP, ScTP	Malha	Sem
SF/UTP	S-FTP, SFTP, STP	Malha+Folha	Sem
U/FTP	STP, ScTP, PiMF	Sem	Folha
F/FTP	FFTP	Folha	Folha
S/FTP	SSTP, SFTP, STP PiMF	Malha	Folha

Nesta tabela e ilustração seguintes são apresentadas as normas mais comummente utilizadas nas instalações de rede. Embora o EIA/TIA 568A seja um standard de âmbito fora da união europeia, a configuração dentro do conector é o mais utilizado para as ligações em par-traçado.

Normas	Âmbito	Revestimento	Blindagem
ANSI EIA/ TIA 568A	América do Norte, Ásia	Material termoplástico	Cabo de 100 Ω sem qualquer tipo de blindagem (UTP)
ISO/IEC 11801	Internacional	Material termoplástico, opcionalmente com características LSZH	Cabo de 100 Ω com blindagens exteriores e individuais (em cada par) opcionais (UTP, S/UTP, STP)
EN 50173	União europeia	Material termoplástico, obrigatoriamente com características LSZH	Cabo de 100 Ω com blindagem exterior obrigatória e blindagens individuais (em cada par) opcionais (S/UTP ou STP)

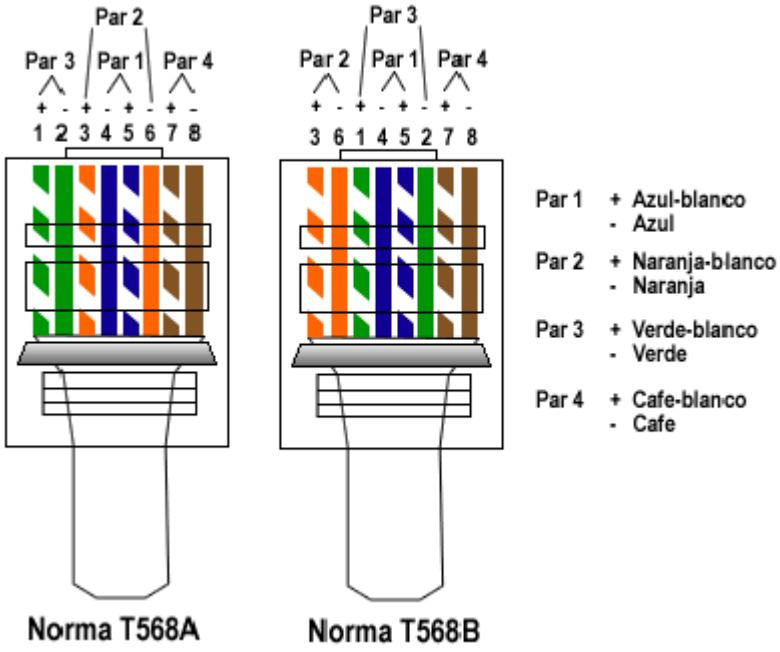

Ilustração 16: EIA/ TIA 568A/B

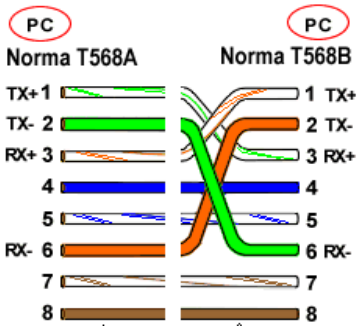

Ilustração 17: Visualização do par cruzado T568A-T568B

Fibra Óptica

Este tipo de cabo é composto por um ou vários filamentos, muito finos, de sílica e de plástico onde é feita a transmissão da luz, rodeado por materiais isolantes e amortecedores de choque, com capacidade de transmissão a grande distância e a grande velocidade. As fontes de transmissão de luz podem ser Díodos Emissores de Luz (LED) ou lasers.

A transmissão de dados por fibra óptica é realizada pelo envio de um sinal de luz codificado, dentro do domínio de frequência do infravermelho a uma velocidade de 10 a 15 MHz.

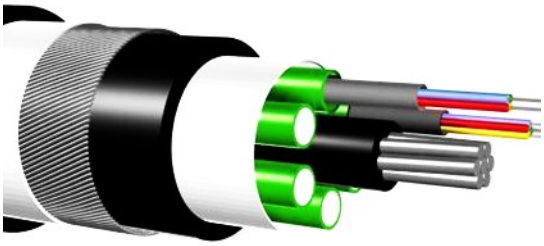

Ilustração 18: Fibra Óptica

O cabo óptico com transmissão a partir de raios laser é o mais eficiente, devido à sua potência e à sua espessura reduzida. Os cabos em que a transmissão é feita com díodos emissores de luz são mais baratos, mais adaptáveis à temperatura ambiente e têm um ciclo de vida maior.

A cablagem de fibra óptica não é passível a interferências por ruídos electromagnéticos e radio-frequências. Permitem um total isolamento entre transmissor e receptor, o que torna a transmissão segura e rápida.

Ondas no espaço/Sistemas Wireless (sem fios)

As ligações sem fios integram e possibilitam a transmissão de dados, utilizando tecnologias como radio frequência (RF), infravermelho, microondas, laser, etc…

Ondas de Infravermelhos e Laser

As redes baseadas em infravermelhos ou lasers utilizam a mesma tecnologia usada em produtos como o controlo remoto dos aparelhos de TV. Assim, estes raios infravermelhos podem ser usados para transmitir sinais digitais entre computadores exigindo que os mesmos se encontrem relativamente próximos uns dos outros, bem como a inexistência de obstruções físicas no espaço onde os sinais circulam.

Os sistemas a laser são utilizados para interligar redes em prédios separados. A distância entre os pontos de ligação é um dos principais pontos que diferenciam a utilização de sistemas wireless laser e sistemas wireless infravermelho. O primeiro é utilizado em ambientes internos (escritórios, oficinas), enquanto o segundo é adequado a longas distâncias.

Ondas de Rádio e MicroOndas

Trata-se do mesmo tipo de ondas utilizadas nas transmissões de rádio. A constituição de redes baseadas em ondas de rádio ou micro-ondas implica a instalação de antenas ou dispositivos de emissão e recepção, que devem estar em linha de vista para transmitir e receber os sinais. O seu principal uso é interligar redes locais em diferentes prédios (conseguem ultrapassar pequenos obstáculos como por exemplo paredes finas), mas a partir de certa distância torna-se necessária a instalação de retransmissores.

Ilustração 19: Logótipo indicador de acesso a redes Wi-Fi (Wireless)

Ondas de Satélite

Os satélites utilizados para transmissão de dados sob a forma digital encontram-se situados em órbitas geostacionárias, em torno do equador, a cerca de 30-40Km da superfícies terrestre. A comunicação com esses satélites implica antenas parabólicas, ou seja, dispositivos de transmissão capazes de efectuar *uplinks* (emissões da terra para o satélite) e *downlinks* (recepções do satélite para a terra).

Relação entre a Topologia e meio de Transmissão

Certas topologias estão directamente relacionadas à unidirecionalidade ou bidirecionalidade do meio de transmissão. Fora esse factor, teoricamente, qualquer meio de transmissão pode ser usado em qualquer topologia. Mas o estado actual do desenvolvimento tecnológico só permite que algumas combinações sejam usadas nas redes locais comercializadas hoje, pois o custo de outras combinações é proibitivo.

A tabela seguinte mostra as combinações que hoje são economicamente viáveis. Nela também foi levada em conta a uni ou bidirecionalidade do meio de transmissão, quando requerida.

Meio de Transmissão	Barramento	Estrela	Anel	Árvore
UTP/Par Trançado	X	X	X	X
Coaxial 50 Ω	X		X	
Coaxial 75 Ω	X			X
Fibra Óptica		X(ª)	X	X

A topologia em *Bus* pode utilizar como meio de transmissão o par trançado e os cabos coaxiais de 50 Ω ou 75 Ω. Ainda não é economicamente vantajoso usar fibra óptica em ligações multiponto, se bem que o crescimento da sua utilização tenha aumentado.

A topologia em anel pode ser construída com par trançado, cabos de 50 Ω ou fibra óptica. O uso do cabo de 75 Ω exigiria um número elevado de repetidores para múltiplos canais, o que o tornaria a instalação economicamente inviável.

A topologia em estrela, hoje, é viável economicamente para taxas de transmissão até 10Gb/s, o que leva a escolher o par trançado como o meio de transmissão mais adequado. No entanto, para ligações superiores (ª) a 100m torna-se mais viável e fiável utilizar fibra óptica.

Tipos de Transmissão de dados

As transmissões de dados podem-se agrupar pela sua tipologia. Quanto ao sentido podem ser:

- *Simplex* – As transmissões apenas podem ser feitas num só sentido, de um dispositivo emissor para um dispositivo receptor.
- *Half-duplex* - As transmissões podem ser feitas nos dois sentidos, mas alternadamente.
- *Full-Duplex* - As transmissões podem ser feitas nos dois sentidos em simultâneo, ou seja, um dispositivo pode transmitir informação ao mesmo tempo que recebe.

Quanto à largura de banda, podem ser:

- *Baseband* / Banda base - É uma transmissão em que se utiliza toda a largura de banda do canal para uma única transmissão;
- *Broadband* ou Banda larga – É uma transmissão em que a largura de banda pode ser utilizada por várias transmissões em simultâneo (Multiplexação).

E quanto ao sincronismo, podem ser:

- Síncrona - Ocorre quando no dispositivo receptor é activado um mecanismo de sincronização relativamente ao fluxo de dados proveniente do emissor;
- Assíncrona - Ocorre quando é não estabelecido, no receptor, nenhum mecanismo de sincronização relativamente ao emissor e, portanto, as sequências de bits emitidos tem de conter em si uma indicação do início e do fim.

Quanto ao tipo de transmissão ainda podem ser:

- *Unicast* – A emissão do sinal é feita com apenas um destinatário. Nas redes de computadores, o pacote de informação é endereçado a um único nó.
- *Broadcast* - Quando um único dispositivo transmite uma mensagem para todos os outros dispositivos dentro de um intervalo de endereços. Esta transmissão pode chegar a todos os *hosts* da sub-rede, todas as sub-redes, ou todos os *hosts* em todas as sub-redes.

  Um exemplo de *broadcast* são as emissões das estações de rádio. Aplicado ás redes de computadores, por norma, os *Routers* mais modernos bloqueiam o tráfego de *broadcast* e restringem-no à sub-rede local. Um exemplo são os pacotes de informação enviados dos ISP's para os clientes.
- *Multicast* – Este modo define a entrega de informação para múltiplos destinatários simultaneamente, no entanto estes pacotes de informação contêm os dados do destinatário, e só são entregues a quem tiver autorização. Um exemplo disso são as transmissões de televisão por cabo onde o cliente apenas vê os canais que subscreveu.

Ilustração 20: Unicast

Ilustração 21: Multicast

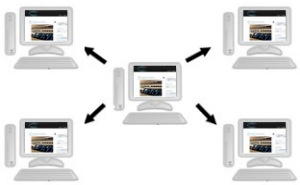

Ilustração 22: Broadcast

Tecnologias e Protocolos de Comunicação

Introdução

De acordo com comités estabelecidos por organizações como o IEEE (*Institute of Electrical and Electronics Engineers*), a EIA (*Eletronic Industries Association*) e o CCITT (C*omité Consultatif Internationale de Télegraphic Téléphonic*), foram designados protocolos como padrão para a cablagem de rede e controlo de acessos, utilizando os meios físicos de uma rede.

Dos protocolos estabelecidos por estes comités destacam-se o Ethernet, o Token Ring e o Arcnet. A seguir serão descritas algumas das principais características técnicas desses protocolos e de outros protocolos mais utilizados.

Ethernet

A Ethernet IEEE 802.3 é uma das tecnologias standard de rede mais popularmente conhecida que foi desenvolvida pela Xerox, INTEL (*International Technology Corporation*) e a DEC (*Digital Equipament Corporation*). Esta pode ser utilizada com diferentes topologias, como por exemplo: Barramento com cabo coaxial ou estrela com o cabo de par trançado.

Neste tipo de rede, cada nó perscruta o tráfego na rede e, quando nada está a ser transmitido, é iniciada uma comunicação. Em comunicações half-duplex, se dois nós transmitirem informações ao mesmo tempo, são automaticamente alertados para a colisão. De seguida, param a transmissão e aguardam por um período aleatório de tempo (na ordem dos milisegundos) antes de tentar novamente. Este método é conhecido como CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*).

Padrão	Tipo Cabo	Transmissão	Topologia	Núm.Nós	Dist.Mín	Máx.Segmt	Dist.Máx
1BaseT	UTP/2P/4F	1Mbits	Estrela	-	1,0m.	250m.	500m.
10Base2	Coaxial	10Mb	Barra	100	0,5m	185m.	185m.
10Base5	Coaxial	10Mb	Barra	30	2,5m.	500m.	500m.
10BaseFP	Fibra óptica	10Mb	Estrela	33	-	500m.	1000m.
10Broad36	Coaxial75	10Mb	Barra	-	N/D	1800m.	1800m.
10BaseT	UTP/Cat3	10Mb	Estrela	-	1,0m.	100m.	200m.
100BaseT	UTP/Cat4	100Mb	Estrela	-	1,0m.	100m.	200m.
100BaseTX	UTP/Cat5	100Mb	Estrela	-	0,5m.	100m.	200m.
100BaseT4	UTP/Cat5	100Mb	Estrela	-	1,0m.	100m.	200m.
100BaseFX	Fibra óptica	100Mb	Estrela	-	-	1Km.	2Km.
1000BaseX	Fibra óptica	1/2Gb	Estrela	-	-	1Km.	0Km.
1000BaseT	Fibra óptica	1/2Gb	Estrela	-	-	1Km	10Km.
1000BaseT	UTP/Cat5e	1Gb	Estrela	-	-	100m.	200m.
10GBase-T	S/FTP/Cat6	10Gb	Estrela	-	-	100m.	200m.
1000BaseTX	S/FTP/Cat7	1Gb/10Gb	Estrela	-	-	100m.	200m.
40GBase-T	UTP/Cat8	40Gb	Estrela	-	-	100m.	>=30m.

Gestão de Colisões de dados

É um método de gestão de rede para evitar que dois ou mais computadores enviem pacotes de dados ao mesmo tempo. O problema relacionado com as colisões de dados, é que baixam significativamente a desempenho e, durante curtos espaços de tempo, podem mesmo parar a rede.

A topologia utilizada neste protocolo é a de Barramento, ou seja, todas as máquinas fazem ao mesmo tempo a gestão do modo de transmissão na rede.

Actualmente, a menor taxa que uma rede Ethernet transfere é de 10 Mb/s (10.485.760 bits por segundo), ou ainda, 1,25 MB/s. A distância máxima recomendável entre uma estação e outra, é de 2,5 quilómetros (2.500 metros).

O sistema Ethernet opera com pacotes pequenos, sendo que o maior é de 1514 e 1526 Bytes (12.112 e 12.208 bits, respectivamente, de comprimento). E desses 1514 Bytes, 14 Bytes (112 bits no mínimo), são destinados para reconhecer e assegurar a integridade desses pacotes de dados que navegam pela rede.

CS (Carrier Sense)

Este protocolo funciona de modo muito simples. Primeiro verifica se existem pacotes de informação na rede com destino à sua placa de rede e, caso não exista, liberta o pacote de dados a ser enviado.

MA (Multiple Access)

Esta técnica refere-se ao duplo (ou mais) envio de pacotes na rede, e ao mesmo tempo.

O protocolo *CS* da placa de rede da estação A, por exemplo, não detectou mensagens na rede e, em seguida, libertou o seu pacote de dados. Acontece que no mesmo instante, o protocolo *CS* da placa de rede da estação C, por exemplo, também não detectou mensagens pela rede e envia o seu pacote de dados. Como a estação A, e também a estação C, enviaram pacotes de dados ao mesmo tempo, ocorre uma colisão de dados.

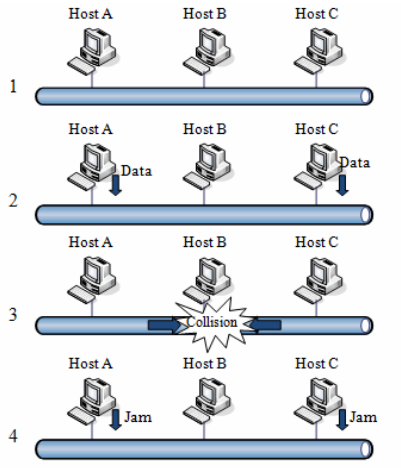

Ilustração 23: Descrição do protocolo CSMA/CD

Neste caso, a função primordial do protocolo *MA*, é evitar que duas ou mais estações enviem pacotes de dados ao mesmo tempo.

CD (Collision Detection)

O protocolo *CD* tem funções similares às de um polícia sinaleiro. Quando ocorre uma colisão entre dois pacotes de dados na rede, o sinal emitido pela colisão torna-se mais intenso e constante, chegando até aos *CD*'s de todas as placas envolvidas na rede. Quando isto acontece, as placas de rede envolvidas, param de enviar os seus pacotes de dados até que se desfaça a colisão, e aguardam um tempo aleatório limitado para voltarem a transmitir novamente.

Token Ring

A tecnologia de acesso Token Ring IEEE 802.5 faz uso da topologia em anel. O controlo do acesso à rede é feito através do protocolo *Token Passing*. Para o nó poder transmitir dados, este terá de primeiro receber o sinal *Token* que lhe dará o direito de transmitir. Este sinal especial viaja de nó em nó através da rede.

Apenas um destes sinais está disponível na rede, o que faz com que um único dispositivo possa transmitir, evitando conflitos na transmissão. O exemplo que se segue explica de forma resumida o processo de trespasse do *Token*:

1. O *Token* circula no anel;
2. O emissor espera que o *Token* chegue até ele;
3. Captura o *Token* e transmite os dados;
4. O receptor recebe o *Token*, verifica se os dados lhe são remetidos, se sim, liberta o *Token*, se não, reencaminha o pacote junto com o *Token* para o próximo nó.

Wireless

São várias as tecnologias e protocolos em que se utilizam as redes wireless, mas aqui apenas se vão focar as mais comuns na transmissão de dados. O formato mais generalizado para as redes WLAN (*Wireless Local Area Network*) actuais é o IEEE 802.11 e as suas variantes. Estas tecnologias especificam uma interface de comunicação sem fios entre um nó e uma estação base/concentrador ou entre dois nós.

A classe IEEE 802.11 neste momento divide-se nos principais protocolos:

Protocolo	Data	Freq. (GHz)	Velocidade (Mbit/s)
IEEE 802.11a	1999	5 GHz	54 Mbps
IEEE 802.11b	1999	2,4 GHz	11Mbps
IEEE 802.11g	2003	2,4 GHz	54 Mbps
IEEE 802.11n	2009	2.4 / 5 GHz	150 Mbps - 1 Gbps
IEEE 802.11ac	2013	5GHz	600 Mbps - 1 Gbps

Para além destes protocolos, existem outras tecnologias que, associadas a estes, aumentam consideravelmente o desempenho, e por sua vez a velocidade da rede *wireless*. O MIMO é uma tecnologia que permite a utilização de várias antenas enviem o sinal (e várias antenas o recebam), permitindo uma maior propagação do sinal pelo espaço. Permite também que sejam enviadas/recebidas várias *streams* em simultâneo (da mesma forma que uma auto-estrada com várias faixas). Esta tecnologia permite ainda o *beamforming*, que direcciona a emissão do sinal wireless para cada cliente, optimizando ainda mais a conexão.

As WLAN podem ser usadas em combinação com LAN cabladas, onde pontos que necessitam de mobilidade são ligados à rede via wireless e as estações fixas são ligadas à rede via cabo.

Este tipo de rede assume dois tipos de configuração:

- ***Ad-hoc*** - É composta por estações dentro de um mesmo espaço que se comunicam entre si sem a ajuda de uma infra-estrutura. Qualquer estação pode estabelecer uma comunicação directa com outra estação.
- ***Infrastructure*** - É utilizado um ponto de acesso (AP) que é responsável por quase toda a funcionalidade da rede. De modo a aumentar a cobertura, vários pontos de acesso podem ser interligados através de um *backbone*.

Bluetooh

Bluetooth é um padrão de tecnologia proprietária para a troca de dados a curtas distâncias através de redes sem fio (usando transmissões de ondas de rádio de curto comprimento na banda 2400-2480 MHz) em dispositivos fixos e móveis, permitindo criar redes de área pessoal (PAN) com altos níveis de segurança. Criado pela *Ericsson* em 1994, foi originalmente concebido como uma alternativa sem fio para as conexões em modo série.

Arquitectura GSM

O interface de transmissão entre o subscritor e a rede GSM (*Global System For Mobile Communication*) é feito através do terminal GSM. Este terminal é conhecido como um telefone móvel, que só funciona quando o cartão SIM de acesso à rede nele for introduzido.

À área de cobertura de cada estação base dá-se o nome de célula e é por esta razão que a rede se designa celular. As células estão todas interligadas pelo que é possível mudar de uma célula para outra, sem perder a ligação (processo de *Handover*).

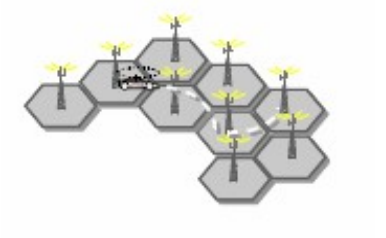

Ilustração 24: Representação da rede celular móvel

O GSM é um standard internacional de funcionamento de telefones móveis que pode funcionar em várias frequências: 850MHz, 900MHz, 1800MHz e 1900MHz. Estas frequências variam consoante o país e podem não ser suportadas por todos os equipamentos móveis. Alguns equipamentos móveis publicitam que a sua capacidade de recepção de sinal é dual-band (GSM-900/1800 ou GSM-850/1900), tri-band (GSM-850/900/1900, GSM-850/1800/1900, GSM-900/1800/1900 ou GSM-850/900/1800) ou quand-band (GSM-850/900/1800/1900). Devido ás diferentes frequências adoptadas pelos diferentes países (mesmo dentro da união europeia) antes de viajar é conveniente verificar se o equipamento é compatível com o tipo de frequência usada no país de destino.

O interface de transmissão entre o subscritor e a Internet pode ser feito através de um terminal GSM com uma destas categorias de transmissões de dados, que variam na velocidade de acesso:

- GPRS (*General Packet Radio Service*) ou 2G;
- EDGE/EGPRS (Enhanced Data rates for Global Evolution / Enhanced GPRS) ou 2,5G;
- UMTS (*Universal Mobile Telecommunications System*) ou 3G;
- HSPA/HSPA+ (*High-Speed* Packet Access / *Evolved HSPA*) ou 3,5G;
- LTE (*Long Term Evolution*) ou 4G estará disponível em Portugal em 2012.

A tabela seguinte distingue as velocidades de acesso dos vários tipos de protocolo para as comunicações feitas através de GSM.

Geração GSM	Uplink Máximo*	Downlink Máximo*	Tipo
1G	Usado apenas em comunicação de voz e ainda em uso nos EUA. Sem segurança.		Analógico / DECT
2G	Desenvolvido para dar prioridade ás comunicações de voz seguras, mas muito lento para transferências de dados.		Digital
2,5G	56kb/s ~ 236.8 kb/s	56kb/s ~ 236.8 kb/s	Digital
3G	>200kb/s	>200kb/s	Digital
3,5G	>22Mb/s	>56 Mb/s	Digital
4G	100Mb/s ~ 500mb/s	100Mb/s ~ 1Gb/s	Digital

*****Valores máximos teóricos que podem variar consoante vários factores (interferências, distância da antena, capacidade do equipamento, etc.)*

Resumindo, todos os telemóveis, *smartphones, pads* e as comuns *pens* de acesso à banda larga, são equipamentos GSM, que podem suportar várias frequências (dual-band, tri-band, etc.) e dentro dessas frequências pode suportar 2G, 2.5G, 3G, etc. Tudo depende do equipamento que se está a utilizar, o país onde se encontra e o plano de dados que está subscrito.

Componentes de Rede

NIC/Placa de Rede

A placa de Rede ou NIC (*Network Interface Card*) permite a ligação de equipamentos à rede e trata de enviar e receber mensagens, aceitar ou rejeitar, conforme o seu endereço físico ou do destinatário (*MAC*[6] *address*).

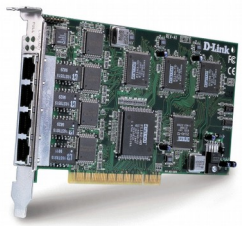

Ilustração 25: Placa de Rede com 4 portas Rj45

6 Do inglês *Media Access Control*.

Cada placa de rede ou interface de rede contém um endereço *MAC* que representa um endereço físico de 48 bits. Este representa-se por 12 dígitos hexadecimais agrupados dois a dois, separados por dois pontos. Exemplo: 00:00:5E:00:01:03.

Modem

O termo significa MOdulator/DEModulator e a sua função consiste em converter sinais digitais em sinais capazes de serem transmitidos por outros meios de transmissão.

Recorrendo ao exemplo da linha telefónica analógica convencional, o MODEM converte os impulsos digitais que provêm de um computador para sinais analógicos próprios para linhas telefónicas e vice-versa.

Ilustração 26: Conversão do sinal analógico para digital por um Modem

A velocidade de transmissão de um Modem é medida em *bps* (bits por segundo), mas as velocidades indicadas são apenas velocidades máximas que o dispositivo suporta (que nem sempre depois são atingidas). Estas velocidades dependem de vários factores, nomeadamente das infra-estruturas de telecomunicações disponíveis a partir do ponto de ligação e também das infra-estruturas do ISP[7] através do qual é feita a ligação.

Ilustração 27: Representação das ligações à Internet via linha telefónica.

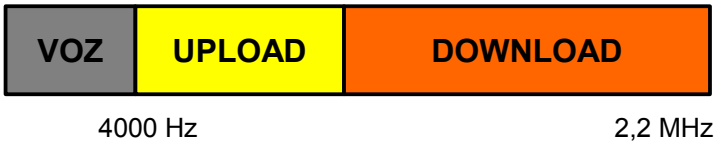

Ilustração 28: Distribuição das frequências nas ligações à Internet via linha telefónica.

Repetidor

A propagação de sinais transportados por cabos tem distâncias limitadas. De um modo geral, numa rede *Ethernet* com cabo UTP, um sinal pode ser transportado em intervalos de 100 metros até uma distância de 300 metros e num sistema *Token Ring*, até 180 metros. Para solucionar este

7 ISP (acrónimo para *Internet Service Provider*) ou fornecedor de serviços de Internet.

problema, são usados repetidores. A limitação do número de repetidores é obtida de acordo com o protocolo utilizado (por exemplo, no protocolo *Ethernet* o número máximo é de quatro).

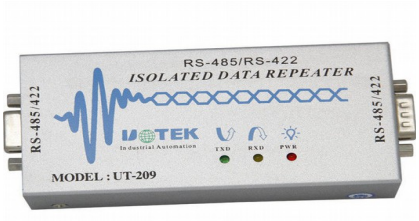

Ilustração 29: Repetidor de dados série

O repetidor apenas regenera e/ou amplifica o sinal, não desempenha qualquer função no controlo do fluxo de dados. Todos os pacotes presentes no primeiro segmento da rede ou de cabo serão replicados para os demais segmentos de rede ou restante cabo.

Hub

Quando é utilizado um Hub como concentrador numa rede, embora esta fisicamente esteja conectada como estrela, logicamente é uma rede de topologia *Bus*, pois este dispositivo distribui todos os pacotes para todas as portas simultaneamente (o que por vezes faz com que ocorra colisões). Por esta razão somente uma transmissão pode ser efectuada de cada vez.

O Hub apresenta diversas vantagens sobre a topologia *Bus* tradicional. Entre elas, permite a remoção e inserção de novos nós com a rede ligada e, quando há problemas com algum cabo, somente o nó correspondente é afectado.

Ilustração 30: HUB com a primeira porta de uplink

Um Hub pode ser distinguido pelo seu número de portas: 4, 8, 16, 24 ou 32. A maior parte dos Hubs possui uma porta chamada *uplink* com a função de *stack*, isto é, permite que outros *Hubs* possam ser empilhados numa topologia *Tree,* aumentando desta forma a quantidade de pontos de ligação e por conseguinte o aumento da rede.

Na actualidade, este tipo de equipamentos está a ficar obsoleto devido a todos os problemas já enumerados (colisões, falta de fiabilidade, etc) e estão a dar lugar ao *Switch*.

Switch

Pode-se considerar o *Switch* como um *Hub* inteligente. Fisicamente é similar a um *Hub*, porém logicamente opera num sistema comutador de portas. Desta forma, permite a troca de mensagens entre várias estações ao mesmo tempo pois os pacotes são enviados directamente para o destino, sem serem replicados (desnecessariamente) para todas as máquinas.

Se dois computadores estiverem a comunicar, as duas portas utilizadas comutam e interligam-se de modo que os restantes computadores possam também comunicar em simultâneo, desde

que a origem e o destino dos pacotes sejam diferentes. Para além de aumentar o desempenho, aumenta a segurança dentro da rede.

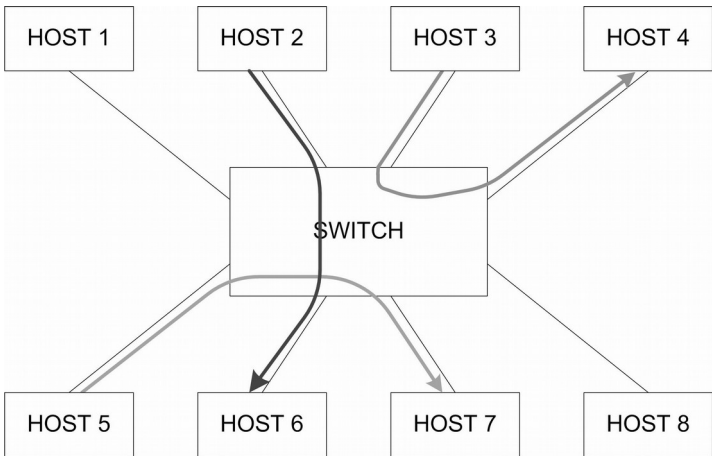

Ilustração 31: Descrição de funcionamento de um Switch

Bridge/Ponte

Este dispositivo interliga ou segmenta duas redes locais que usam a mesma tecnologia de rede. Conecta por exemplo uma rede cablada a uma rede *Wireless.* Permitem combinar duas redes locais, além de admitir que estações de uma rede local acedam a recursos de outra rede local.

Na segmentação permite a criação de sub-redes (ou segmentos), isolando e permitindo a passagem de pacotes de uma sub-rede para outra, apenas quando o emissor e o receptor estão em sub-redes (ou segmentos) diferentes. Na interligação, assumem a função de *transciever*, permitindo a comunicação de duas redes diferentes (Wireless - Fibra Óptica).

Ilustração 32: Bridge de Fibra - UTP

A Bridge pode actuar também como um filtro, permitindo a separação do tráfego entre dois segmentos, evitando a propagação da informação sem interesse para restantes segmentos.

As pontes utilizam protocolos de controlo de acesso ao meio físico (via endereço MAC). Através desse recurso, é possível ligar meios físicos diferentes entre si, como os cabos de fibra óptica e os cabos coaxiais, desde que as duas partes utilizem o mesmo protocolo (p.e. Ethernet).

Router

Dispositivo de (re)encaminhamento de mensagens entre redes diferentes e, eventualmente, quando entre emissor e receptor existem vários caminhos (rotas) possíveis. Especificamente a

função de um r*outer* é examinar o endereço de origem e de destino de cada mensagem ou pacote e decidir qual o melhor caminho (rota) para o destinatário.

Este dispositivo pode traduzir sinais enviados por diferentes meios de comunicação. Por exemplo, um *Router* pode receber mensagens através de uma linha ADSL e colocá-las numa rede privada Ethernet.

Ilustração 33: Router ADSL

Existem basicamente dois tipos de *Routers*: estáticos e os dinâmicos. O *Router* estático é mais barato e escolhe o menor caminho para o pacote de dados. Acontece que este não leva em consideração o congestionamento da rede, onde o melhor caminho pode estar sobre-lotado, existindo caminhos alternativos que podem estar com um fluxo menor de dados. Portanto, o menor caminho não é necessariamente o melhor caminho.

No caso do *Router* dinâmico, escolhe o melhor caminho com base nos melhores tempos de resposta dos intervenientes (*hops*). É provável que o pacote possa seguir por um caminho mais longo, porém menos congestionado, resultando numa entrega mais rápida.

Gateway

O *Gateway* permite a comunicação entre redes com protocolos de comunicação completamente distintos. No sentido lato, o *Gateway* é todo o dispositivo que permite o acesso de uma rede a outra rede exterior (o que pode englobar *Bridges* e *Routers*). Normalmente interliga redes internas a externas (WAN – LAN e vice versa).

Modelo OSI

Visão Geral do Modelo OSI

A gestão de uma rede de comunicação de dados é uma questão relativamente complexa e requer, em particular, a realização de um grande número de funções muito diferenciadas e com diversos graus de dificuldade. Acresce a isso o facto de estas funções terem de se realizar num ambiente distribuído (distribuição física de recursos) e potencialmente adverso (erros, falhas), envolvendo sistemas heterogéneos.

Para além do transporte de dados através da rede, essencial para assegurar a comunicação entre sistemas utentes da rede, coloca-se também o problema da troca de informação de controlo entre os referidos sistemas, entre estes e a rede e no interior da própria rede, de forma a permitir uma eficiente gestão de recursos e uma boa coordenação das respectivas actividades. A interacção entre os sistemas constituintes da rede requer, deste modo, mecanismos de comunicação, controlo e sincronização.

Isto coloca novos problemas pois os mecanismos de controlo são em geral distribuídos, a geração e transmissão de informação tem carácter essencialmente assíncrono e a comunicação está sujeita a erros. Interessa assim que estes mecanismos sejam coerentes e robustos e tanto quanto possível independentes das aplicações.

O propósito deste modelo de referência, que é uma norma internacional, é proporcionar uma base comum à coordenação do desenvolvimento de normas para a interligação de sistemas, enquanto assegura igualmente a continuidade através da consideração dos sistemas actuais, enquadrando-os no modelo de referência.

O modelo OSI (*Open System Interconnection*) permite então uma descrição de como o *hardware* e o software de rede trabalham em conjunto numa disposição por camadas para possibilitar a comunicação. Cada camada refere-se a diferentes actividades, equipamentos e protocolos de rede e prepara os dados para a camada superior ou inferior.

Este modelo tem como objectivos:

- Ser um modelo de referência de sistemas abertos (à cooperação com outros sistemas);
- Independência relativamente a fabricantes;
- Universalidade.

O objectivo do desenho de uma estrutura em camadas para um protocolo de comunicação surge com a necessidade de delimitar e isolar funções dos vários tipos de comunicações a cada uma das respectivas camadas.

Neste tipo de estrutura, os dados não são transferidos directamente ao outro nó, mas sim "descem" verticalmente através de cada camada até ao nível físico (onde na realidade há a única comunicação entre máquinas), para depois "subir" novamente através de cada camada do nó receptor.

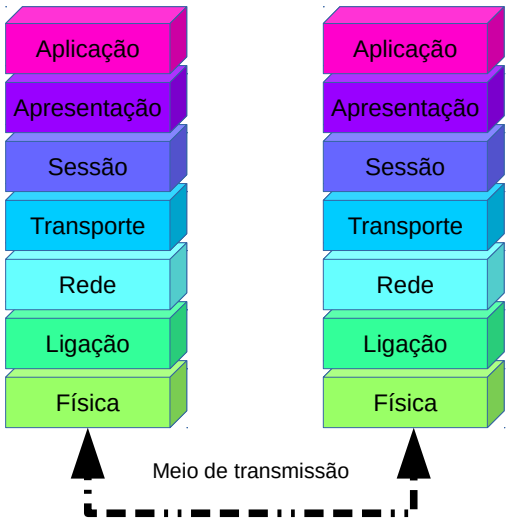

Ilustração 34: Modelo OSI

Nível 1 – Camada Física

A camada física define as características mecânicas, eléctricas e funcionais para activar, manter e desactivar as conexões físicas para a transmissão de dados entre nós. É neste domínio que é decidida a duração das transmissões (em microsegundos (µs)), se esta é *simplex*, *half-duplex* ou f*ull-duplex*, como será iniciada e finalizada e mesmo até quantos pinos terá o conector da rede.

A função eléctrica deste nível é de apenas permitir o envio de cadeias de pacotes para rede, sem a preocupação com o significado destes ou do seu agrupamento.

Nível 2 – Camada de Ligação

Esta camada tem como função detectar e opcionalmente corrigir erros que possam ocorrer na camada física. Vai assim converter todos os pacotes provenientes do canal de transmissão que possam não estar confiáveis ou em boas condições num resultado fiável para o uso posterior da camada de rede.

Para a verificação dos pacotes são utilizadas quatro metodologias:

- Contagem dos pacotes;
- Integridade do pacote,
- Contagem de bits e detecção de pacotes pela presença ou ausência de sinal no meio físico.

Em geral todos os protocolos da camada de ligação incluem bits de controlo nos pacotes para e detecção de erros, mas não servem para a sua correcção. Adicionam também informação sobre a identificação física da placa de rede (MAC) de origem e de destino.

Nível 3 – Camada de Rede

Esta camada é a responsável por endereçar as mensagens e traduzir endereços lógicos (IP) em físicos (MAC) e vice-versa. É também a responsável por gerir o tráfego na rede (roteamento, controlo de congestionamento) e onde se define a sua topologia.

Nível 4 – Camada de Transporte

Esta camada essencialmente garante as transmissões e a sua qualidade. É da sua responsabilidade assegurar que os pacotes são entregues “livres” de erros, na correcta sequência, sem perdas, ou duplicações, mantendo assim a integridade de dados. É também da responsabilidade desta camada gerir o início e o fim das transmissões, controlar, dividir e agrupar o fluxo de mensagens garantindo a eficiência da transmissão.

Nível 5 – Camada de Sessão

A camada de sessão é a responsável por estabelecer as conexões (sessões) entre dois computadores. É da sua competência realizar a sincronização (controlo de fluxo de dados) e estabelecer o tipo de comunicação (o que é que transmite, quando e por quanto tempo, etc.). É também responsável pela marcação dos dados de forma a que caso haja uma quebra no envio/recepção dos dados, estes continuarão a ser enviados a partir do momento da quebra logo que a conexão esteja reposta.

Nível 6 – Camada de Apresentação

A camada de apresentação determina o formato para transmissão de dados (actuando como tradutora da rede). É nesta camada que se processa a criptografia, compressão e descompressão de dados, e as conversões de caracteres. Ou seja, “traduz” a informação recebida pela Camada de Aplicação para a Camada de Sessão e vice-versa.

Nível 7 – Camada de Aplicação

Esta camada interage directamente com o software respondendo directamente aos protocolos que solicitam dados, quer sejam de transferências de ficheiros (FTP), de navegação na Internet

(HTTP/S), de correio electrónico (POP e SMTP), etc.. Esta camada controla também o fluxo dos pacotes de informação e a recuperação de erros.

Arquitectura de Redes TCP/IP

Introdução

O TCP/IP não é um protocolo, mas sim, um conjunto de protocolos originalmente desenvolvido pela Universidade da Califórnia em Berkeley, a pedido do Departamento de Defesa dos EUA.

Veio a tornar-se o padrão das redes locais e alargadas, sobrepondo-se a conjuntos de protocolos desenvolvidos por grandes marcas como a IBM (SNA), Microsoft (NetBIOS/NetBEUI) e a Novell (IPX/SPX).

A razão do seu grande sucesso deve-se justamente ao facto do TCP/IP não ter nenhuma grande empresa associada ao seu desenvolvimento. Isto possibilitou a sua implementação e utilização em diversas aplicações por praticamente todos os tipos de hardware e sistemas operativos existentes. A adopção por parte da Microsoft como o protocolo preferencial para a geração dos sistemas operativos Windows NT, devido às limitações técnicas do seu próprio conjunto de protocolos NetBIOS/NetBEUI, foi um grande contributo para o crescimento da sua utilização.

Mesmo antes do crescimento exponencial da Internet, o TCP/IP já se tinha afirmado como o protocolo para grandes redes, formadas por produtos de vários fornecedores distintos.

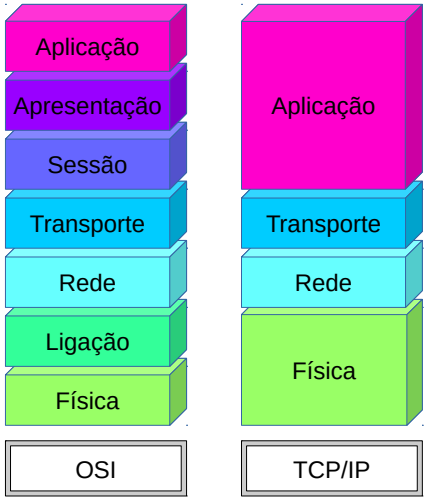

Ilustração 35: Modelo OSI vs TCP/IP

Protocolos em Camada

Todos os protocolos de redes são construídos com base numa arquitectura de camadas, por essa razão é feita a referência a estes normalmente como “protocolos em pilha” ou “protocolos em camada”, que provêem do inglês, *protocol stack*, ou por exemplo *the TCP/IP stack*. O termo "pilha" ou “camada” é utilizado porque os protocolos de uma dada camada normalmente interagem apenas com os protocolos das camadas imediatamente superior e inferior.

As arquitecturas em pilha trazem a vantagem de a evolução do protocolo poder ser modular (isto é, por camada), permitindo a expansão com novos recursos, novas tecnologias ou aperfeiçoamentos sobre a estrutura existente, de forma gradual.

O nome TCP/IP tem origem nos nomes dos protocolos mais utilizados desta pilha, o *Internet Protocol* e o *Transmission Control Protocol*. Dentro do TCP/IP encontram-se ainda muitos outros protocolos, vários deles necessários para que o TCP e o IP desempenhem correctamente cada uma das suas funções.

Ao contrário do modelo OSI, o TCP/IP possui apenas quatro camadas:

4. Aplicação (FTP, TELNET, HTTP);
3. Transporte (TCP, UDP);
2. Rede (IP);
1. Ligação (Ethernet);

Funções de cada camada do TCP/IP

A função de cada camada dentro do TCP/IP são em tudo similares ás das funções do Modelo OSI. A comparação entre as camadas é feita na ilustração anterior onde é possível verificar que camadas ficam “agregadas”.

Nível 1 – Camada de Ligação

Através dos diversos protocolos da camada de Ligação, os pacotes são transmitidos de um nó para outro pelo meio de transmissão (Ethernet, Wireless, etc). A função destes é permitir o estabelecimento das conexões para que os nós da rede possam enviar e receber dados.

O protocolo ARP constrói uma tabela de correspondência entre os endereços TCP/IP e os endereços Ethernet (MAC), de modo a que os pacotes possam atingir o seu destino numa rede. Convém recordar que a responsabilidade da entrega do pacote na rede é do protocolo Ethernet, e não do TCP/IP.

Nível 2 – Camada de Rede

Na camada de rede, o Internet Protocol (IP), é responsável por fazer com que as informações enviadas por um nó cheguem aos restantes nós, mesmo que estes estejam em redes fisicamente distintas. Como o próprio nome “Inter-net” diz, o IP realiza a interconexão entre redes, permitindo reconfigurar caminhos (rotas) quando uma parte da rede está indisponível, procurando uma rota alternativa.

Nível 3 – Camada de Transporte

O melhor exemplo para expressar o funcionamento da camada de transporte consiste na utilização de vários programas num computador, trabalhando simultaneamente na rede com um *browser* e um leitor de correio electrónico. Aqui, os protocolos de transporte UDP e TCP atribuem a cada programa um número de porta, que é anexado a cada pacote de modo que o TCP/IP saiba a qual programa entregar cada mensagem recebida pela rede.

Pela ilustração 26 pode-se observar que existem dois protocolos de transporte no TCP/IP. O UDP é um protocolo que trabalha com datagramas, que são mensagens com um comprimento máximo pré-estabelecido e cuja entrega destes não é garantida. Caso a rede esteja congestionada, um datagrama pode ser *dropped* (deitado fora) sem que a aplicação seja

informada da ocorrência. Pode acontecer também que o congestionamento numa rota da rede possa fazer com que os pacotes cheguem ao seu destino numa ordem diferente daquela que foram enviados. Isto acontece porque o UDP é um protocolo de comunicação simples que transmite sem estabelecer conexões entre os softwares e/ou os nós que estão a comunicar.

Ao contrário do UDP, o TCP é um protocolo que transmite com base no estabelecimento de uma conexão. Permite então que sejam enviadas mensagens de qualquer tamanho e trata de as segmentar em pacotes que possam ser enviados pela rede. Têm também a capacidade de reorganizar os pacotes no destino e de retransmitir qualquer pacote que tenha sido perdido na rede, de modo que o destino receba a mensagem integralmente e igual à original.

Nível 4 – Camada de Aplicação

Finalmente, no nível quatro, retomando as aplicações no computador, os protocolos tornam-se específicos para cada programa que faz uso da rede. Desta forma existe um protocolo para a comunicação entre um servidor web e um browser (HTTP), um protocolo para a comunicação entre um cliente Telnet e um servidor Telnet, etc. Cada aplicação de rede tem o seu próprio protocolo de comunicação, que utiliza os protocolos das camadas mais baixas para poder atingir o seu destino.

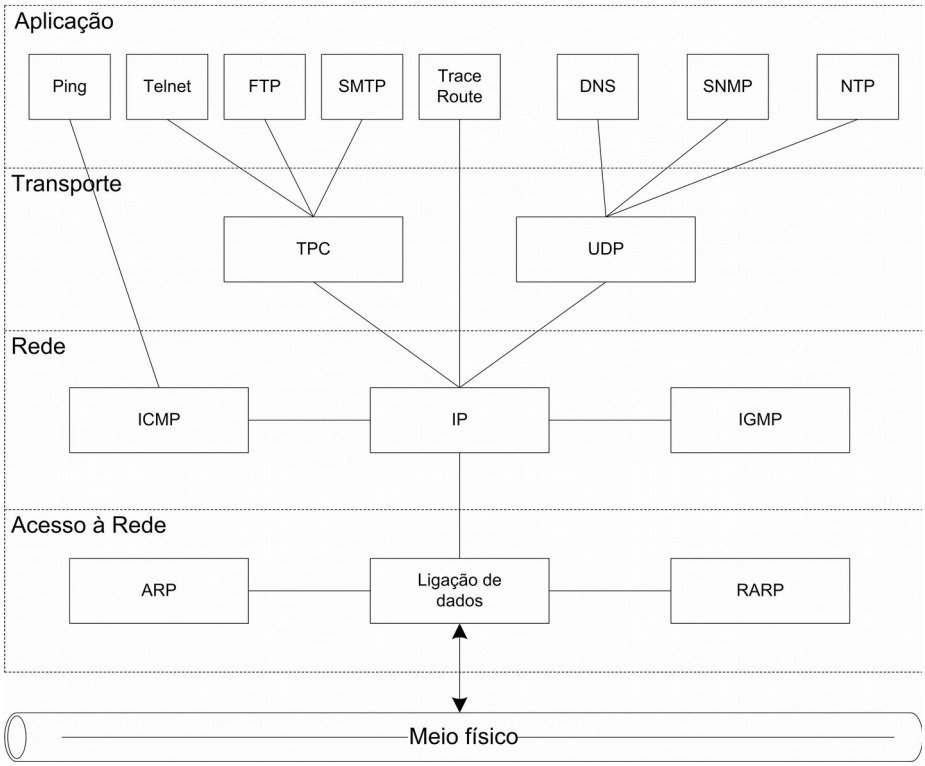

Ilustração 36: Esquema de camadas do TCP/IP

Endereçamento e roteamento

Numa rede TCP/IP v4, a cada *host* é atribuído um endereço numérico formado por 4 octetos (4 bytes), geralmente escritos na forma w.x.y.z. Além deste endereço IP, cada computador possui uma máscara de sub-rede (*network mask* ou *subnet mask*), que é um endereço com a mesma estrutura mas que deve começar sempre por uma sequência contínua de bits a 1, seguida por uma sequência contínua de bits a zero. Isto é, por exemplo, a máscara de rede pode ser 255.255.0.0, mas nunca 255.255.7.0.

11111111.11111111.00000000.00000000 (255.255.0.0)

~~11111111.11111111.00000111.00000000 (255.255.7.0)~~

A máscara de sub-rede serve para identificar no endereço IP que parte pertence ao endereço de rede e que parte pertence ao endereço de *host.* Todos os *hosts* de uma rede local devem ter o mesmo endereço de rede, e cada um deve ter um endereço de *host* diferente.

Máscara de sub-rede	255.255.255.0
Endereço IP - Rede	**192.168.2**.0
Endereço IP - Host	0.0.0.**1**
Endereço IP - Geral	192.168.2.1

Então, numa rede TCP/IP (incluindo também toda a Internet) cada *host* possui um endereço IP único e exclusivo.

Quando um *host* pretende estabelecer uma comunicação, o endereço IP é decomposto pelo protocolo IP, assim como também o endereço IP de destino. Fazendo uso da máscara de sub-rede, ambos os endereços IP são comparados. Se os endereços de rede forem iguais, significa que a mensagem será enviada para um *host* na mesma rede local. Este é então encaminhado para o seu destino através da rede local e dos respectivos meios de transmissão. Se os endereços forem diferentes, o protocolo IP envia directamente o pacote para o *default gateway*, o equipamento que interliga a rede local com a rede exterior e que se encarrega de o encaminhar para a rede externa onde está o endereço IP do destino.

É importante que o *default gateway* tenha o seu endereço IP na mesma rede que todos os restantes *hosts*, caso contrário a rede não lhe poderá endereçar pacotes, podendo esta apenas comunicar-se com os restantes *hosts* da rede.

Finalizando, para a correcta configuração de um *host* numa rede TCP/IP, este deve ser configurado com pelo menos três parâmetros:

- o endereço IP (exclusivo);
- a máscara de rede (que deve ser a mesma utilizada pelos demais *hosts* na mesma rede);
- o endereço IP do *default gateway*.

Classes de Redes

Como já foi dito, a máscara de sub-rede serve para determinar qual a parte do endereço IP corresponde à rede e qual parte que corresponde à identificação do *host*, ao mesmo tempo identificado se este se encontra dentro da (sub-)rede local, se localizado numa rede remota (exterior).

Para uma correcta divisão das redes a comunidade Internet definiu originalmente 5 classes de endereços para acomodar as redes de tamanhos variados. A classe de uma máscara de sub-rede define quantos bits estão a ser usados para identificação de rede e quantos para identificação do *host*.

Classe	Máscara	n.º redes	n.º hosts
Classe A (/8)	255.0.0.0	126	16.777.214
Classe B (/16)	255.255.0.0	16.384	65.534
Classe C (/24)	255.255.255.0	2.097.152	254

A Classe D é uma classe reservada para endereçamento IP de Multicast, e a Classe E é reservada ao endereçamento experimental, para uso futuro.

Endereços Reservados

Existem alguns endereços IP que são reservados para funções específicas e que não podem ser utilizados como endereços para *hosts*.

- 127.0.0.0 – Os endereços da gama 127.0.0.0 são utilizados como um *alias* para uma máquina local, isto é, um endereço interno. Normalmente é utilizado o endereço 127.0.0.1, o qual é normalmente associado ao nome *localhost* (máquina local).
- 0.0.0.0 – Os endereços com zeros num dos seus constituintes representam sempre endereços de rede. Numa rede da gama 200.220.150.[1-254], o endereço 200.220.150.0 representa o seu endereço de rede com a respectiva máscara de sub-rede 255.255.255.0.
- 255.255.255.255 – Os endereços com os bits a 1 nos seus octetos representam endereços de *broadcast,* e consequentemente associados às máscaras de sub-rede. Uma mensagem enviada para o endereço do *broadcast* é endereçada para todos as máquinas da rede.

Sub-/sobre-endereçamento

Antes da década de 90, o espaço de endereçamento era largamente superior a qualquer tipo de necessidade em qualquer instituição. Porém, com a consequente interligação de várias redes IPv4 e o crescimento exponencial da Internet começou a avolumar-se um grave problema. Todos os endereços tinham de ser únicos e o espaço de endereçamento começou a não ser suficiente para as crescentes necessidades. Concretamente enfrentava-se os seguintes problemas:

- O esgotamento a curto prazo dos endereços de rede de classe B;
- O crescimento excessivo das tabelas roteamento globais da Internet;
- O esgotamento dos endereços de 32 bits IPv4.

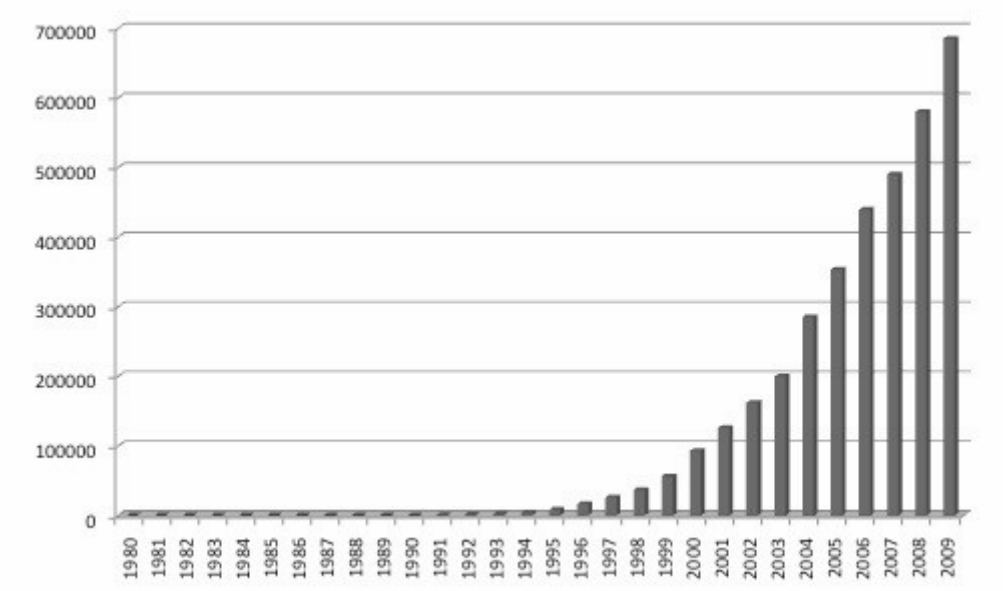

Ilustração 37: Evolução dos hosts na Internet até 2009

Para além dos espaços de endereçamento limitado (32 bits), as regras de endereçamento que dividem as redes em classes revelaram-se também muito restritivas, levando ao "desperdício" de muitos endereços, pois o aproveitamento de cada rede apenas se verifica para um número exacto de nós, que raramente corresponde às situações concretas.

Para resolver este problema foi iniciado o desenvolvimento do IPv6, já com um endereçamento de 128 bits. O arrancar do projecto foi algo demorado e tiveram de ser encontradas alternativas mais expeditas para manter o IPv4 no activo, das quais:

- **CIDR** – de *Classless Inter-Domain Routing*, também conhecido por Sub-redes e Super-redes, trata-se de reduzir ou eliminar o desperdício de endereços devido à divisão em classes.
- **NAT** – ou tradução de endereços, esta técnica permite ligar uma rede IP à "internet" usando um único endereço oficial, em lugar de um endereço para cada nó no interior dessa rede.

Sub-Redes e Super-Redes

O CIDR foi oficialmente documentado a setembro de 1993 no RFC1517, 1518, 1519 e 1520. A sua implementação entre 1994 e 1995 impediu que as tabelas de roteamento da Internet excedessem as 70.000 rotas, ficando apenas com pouco mais de 30.000.

Possui duas características importantes que beneficiam o sistema de roteamento:

- Elimina os conceitos tradicionais de redes de Classe A, B e C. Isto possibilita a alocação eficiente dos endereços IPv4, o que lhe permitirá crescer até que seja implementado o IPv6.
- Suporta o agrupamento de rotas. Uma única entrada na tabela pode representar o espaço de endereços de talvez milhares de rotas das classes tradicionais.

Na prática o CIDR é uma técnica que consiste na manipulação da máscara de rede. Inicialmente as máscaras de rede possuíam apenas três valores possíveis correspondentes às três classe de rede. Os routers utilizam o prefixo de rede, ao invés dos 3 primeiros bits do endereço IP, para determinar a divisão entre o número de rede e o número de *host*. Desta forma,

o CIDR permite suportar qualquer tipo de tamanho de número de rede, não sendo obrigatória a utilização dos tamanhos padrão anteriormente descritos, de 8 bits (/8), 16 bits (/16) e 24 bits (/24) dos modelos de classes.

Classe	Máscara Decimal	Máscara Binário
Classe A (/8)	255.0.0.0	11111111.00000000.00000000.00000000
Classe B (/16)	255.255.0.0	11111111.11111111.00000000.00000000
Classe C (/24)	255.255.255.0	11111111.11111111.11111111.00000000

A manipulação da máscara de rede consiste no avanço ou recuo da máscara, no primeiro caso criam-se sub-redes, no segundo caso criam-se super-redes.

O avanço da máscara consiste em activar bits (passar ao valor 1) imediatamente à direita dos bits que estão activos na máscara "normal". Isso significa que o número de bits usados para identificar os nós em cada rede diminui, teremos então redes mais pequenas, mas por outro lado teremos mais bits para identificar a rede, o que significa que teremos mais redes (sub-redes).

O recuo da máscara consiste em desactivar bits (passar ao valor 0) imediatamente à esquerda dos bits que estão inactivos na máscara "normal". Isso significa que o número de bits usados para identificar os nós em cada rede aumenta, teremos então uma rede de maior dimensão (super-rede), mas por outro lado teremos menos bits para identificar a rede, o que significa que teremos menos redes.

Para melhor compreender as sub-redes, tome-se o exemplo de um ISP ao qual foi atribuído o bloco de endereços 206.0.64.0/18. Num ambiente de classes, só poderiam ser atribuídos endereços /8, /16 ou /24. Mas com CIDR, o ISP já poderá disponibilizar blocos de endereços, indo de encontro às necessidades de cada cliente, criando um espaço para futuro crescimento.

Considerando o bloco anteriormente referido, este representa 16.384 (2^{14}) endereços IP que podem ser interpretados como 64 sub-nets /24. Se um cliente solicitar 800 endereços (*hosts*), o ISP, em vez de atribuir uma classe B (65534 *hosts* disponíveis para apenas 800 *hosts* necessários) ou quatro classes C individuais (254x4=1016 *hosts* disponíveis esgotando o ISP, e o que ainda iria introduzir 4 novas rotas nas tabelas de roteamento globais), poderá atribuir o bloco de endereço 206.0.68.0/22 (sendo necessária apenas uma sub-rede com 1022 *hosts* disponíveis).

Bloco	Máscara Decimal	Máscara Binário	n.º hosts	Subnets
ISP	206.0.64.0/18	**11001110.00000000.01**000000.00000000	16382	4

Bloco	Máscara Decimal	Máscara Binário	n.º hosts	Subnets
Cliente	206.0.68.0/22	**11001110.00000000.010001**00.00000000	1022	64

Bloco	Máscara Decimal	Máscara Binário	n.º hosts	Subnets
Classe C (1)	206.0.68.0/24	11001110.00000000.010001**00**.00000000	254	256
Classe C (2)	206.0.69.0/24	11001110.00000000.010001**01**.00000000	254	256
Classe C (3)	206.0.70.0/24	11001110.00000000.010001**10**.00000000	254	256
Classe C (4)	206.0.71.0/24	11001110.00000000.010001**11**.00000000	254	256

Outro exemplo seria definir uma rede IP sobre a ligação dedicada, sem criar sub-redes. A única solução era atribuir a essa ligação uma rede de classe C. Isto constituía um desperdício enorme de endereços, já que dos 254 endereços de nó de uma rede de classe C, apenas eram usados 2.

Bloco	Máscara Decimal	Máscara Binário	n.º hosts	Subnets
Dedicada	10.0.0.0/24	11111111.11111111.11111111.00000000	254	-

Usando sub-redes, pode-se definir a máscara até que apenas fique 2 bits com o valor 0. Nestas condições, uma única rede de classe C permite criar 64 sub-redes com capacidade para dois nós cada.

Bloco	Máscara Decimal	Máscara Binário	n.º hosts	Subnets
Dedicada	10.0.0.0/30	11111111.11111111.11111111.11111100	2	64

O exemplo apresentado ilustra também outro facto. Em termos teóricos a divisão em sub-redes conduz a um desperdício de endereços. Dos 254 nós de uma rede de classe C passamos a ter 64 redes com dois nós cada, ou seja 128 nós no total (64 subnets x 2 *hosts*). Isto deve-se ao facto de em cada rede estarem reservados o endereço do nó 0 (endereço da rede) e o endereço de nó com os bits todos 1 (endereço de *broadcast*). Para além destes dois endereços, a definição de uma rede implica também a ligação a um encaminhador (*router*) o que ocupa ainda mais um endereço. Mas obviamente este desperdício é meramente teórico pois é largamente compensado pela melhor adaptação do tamanho das redes às realidades existentes.

A manipulação das máscaras de rede deve ser realizada de uma forma consciente:

- O primeiro cuidado fundamental é garantir que nunca existe sobreposição das redes (endereços comuns).
- Ao definir uma super-rede ocupa-se o espaço de endereçamento de várias redes. Por exemplo, em redes de classe C, para criar uma super-rede por recuo de um bit na máscara de rede será necessário usar as duas redes de classe C correspondentes aos dois valores possíveis para esse bit, para recuar 2 bits serão necessárias as 4 redes de classe C correspondentes aos valores possíveis desses bits.
- Na divisão em sub-redes colocam-se os mesmos problemas, embora a separação das várias sub-redes seja normalmente clara, se forem aplicadas simultaneamente várias máscaras a uma mesma rede é necessário ter cuidado para evitar qualquer tipo de sobreposição.

Tradução de endereços (NAT)

O manuseamento das máscaras de rede (divisão em sub-redes e agrupamento em super-redes), permite eliminar os grandes desperdícios de endereços que de outra forma seriam inevitáveis. Mesmo assim, o número de endereços disponibilizado acabou por se revelar insuficiente para a grande expansão da Internet. O que verdadeiramente "salvou" o IPv4 de uma substituição rápida pelo IPv6 foi a tradução de endereços.

Ao observar o tipo de nós finais ligados à Internet (normalmente um computador pessoal), facilmente se constata que a grande maioria assume unicamente o papel de cliente, ou seja apenas recebem respostas aos pedidos por eles formulados, raramente recebendo pedidos provenientes da "internet".

Desta forma, os nós finais, atrás desta ligação, não necessitam de estar directamente ligados à Internet. Para isto ser possível o *router* que assegura a ligação pode ser substituído por servidores *proxy* de aplicações.

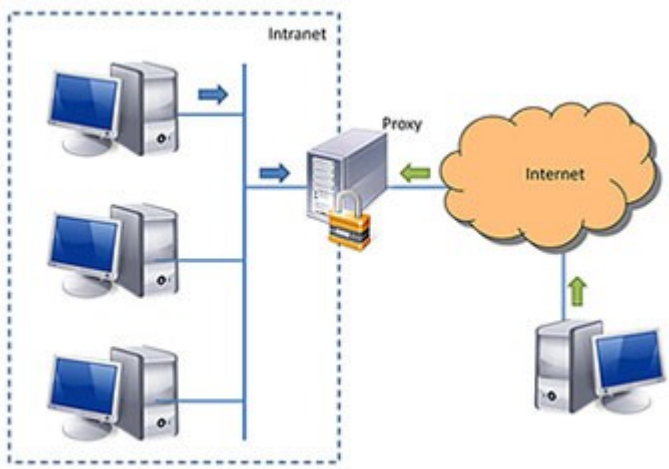

Ilustração 38: Proxy Server

Os servidores *proxy* têm como finalidade optimizar o acesso aos servidores na Internet. Para executarem essa operação, são colocados numa posição de intermédia entre os cliente e servidor (ISP). Por exemplo, quando um cliente na rede local (configurado para usar o servidor *proxy*), usa um navegador para abrir uma página WEB:

- O cliente, em vez de contactar o servidor onde a página reside, contacta o servidor *proxy* (1) e fornece-lhe o endereço da página.
- O servidor *proxy* verifica se possui uma cópia da página e se a cópia está actualizada, se tal não acontecer contacta o servidor (2) e copia a página para a sua *cache* (3).
- O servidor *proxy* responde ao cliente, enviando-lhe a página pedida (4).

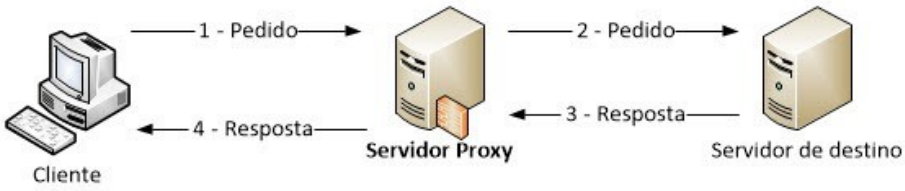

Ilustração 39: Funcionamento de um servidor Proxy

Neste contexto os endereços dos clientes mantêm-se privados porque acabam por nunca comunicar directamente com a Internet, ou seja, os pedidos circulam na Internet tendo como endereço de origem o endereço do servidor *proxy*. mesmo modo as respectivas respostas têm como destino o endereço do servidor *proxy*, acabando por nunca os endereços dos clientes transparecerem para a Internet. Sob o ponto de vista exterior, estes clientes são completamente desconhecidos.

Para que uma rede privada baseada em *proxies* de aplicação funcione é necessário um servidor *proxy* (processo/aplicação) para cada protocolo de aplicação usado. Para além disso a utilização deste tipo de *proxy* não é directa, isto é, cada protocolo de aplicação usado e respectivo software cliente de rede tem de suportar a utilização de *proxy*.

NAT - Proxy Transparente

Para solucionar este problema, os *proxy* transparentes funcionam a um nível muito inferior nas camadas ISO/TCP/IP. Em vez de trabalharem no nível de aplicação, trabalham no nível de rede ou transporte e ao contrário dos anteriores, assemelham-se mais a um *router*.

Os *proxies* transparentes encaminham pacotes (ex.: os datagramas UDP) de forma absolutamente idêntica à de um vulgar *router.* Contudo manipulam os endereços de origem e destino, algo que um *router* por si só não faz. Deste facto provém a designação de *Network Address Translation*. Assim o *proxy* evita que os endereços privados cheguem à Internet, substituindo os endereços de origem de todos os pacotes que são enviados para fora pelo seu próprio endereço.

Com este modo de funcionamento, nem o cliente, nem o servidor se apercebem do que se está a passar, esta técnica é portanto independente dos protocolos de aplicação, destas características provém a designação *transparente*. É igualmente importante notar que são processadas duas traduções de endereços:

- Na saída do pedido o endereço de origem é alterado - SNAT (*Source NAT*).
- Na entrada da resposta o endereço de destino é alterado - DNAT (*Destination NAT*).

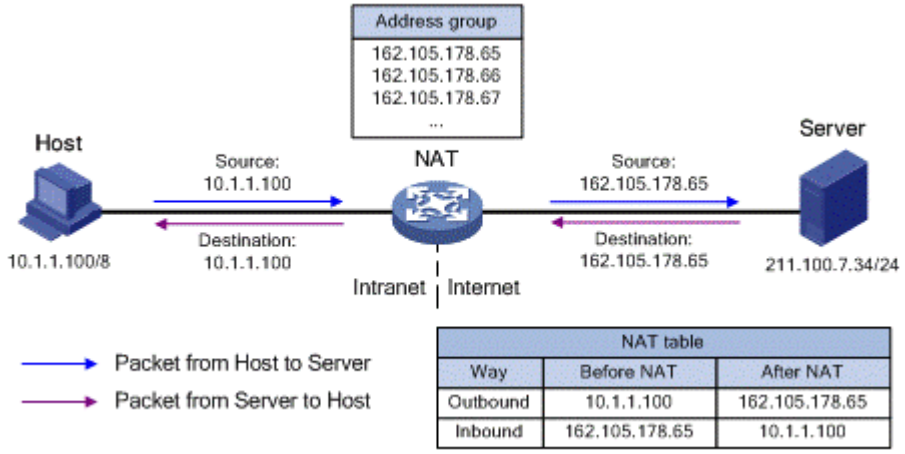

Ilustração 40: NAT Transparente

NAT estático

Quando os pedidos são originários dos clientes que se encontram na rede privada, a tabela NAT é criada automaticamente. Estas entradas na tabela NAT servem para indicar que a chegada de dados a uma dada porta da interface externa deve ser redireccionada (DNAT) para um dado número de porta e endereço IP na rede privada.

Sendo isto verdade, então também será possível definir estaticamente entradas DNAT nessa mesma tabela e com isso facultar o acesso externo a servidores na rede privada. Cada uma destas entradas estáticas deverá conter:

- Número de porta a escutar na interface da "internet".
- Endereço IP de destino (na rede privada).
- Número de porta de destino.

Os clientes residentes na Internet apenas podem contactar estes servidores usando o endereço IP oficial que assegura a ligação externa do *router*. Sob o ponto de vista do cliente, localizado na Internet, aparentemente está a comunicar com um servidor que se encontra localizado na interface externa do *router*.

A definição de entradas estáticas DNAT permite facultar o acesso a vários servidores no interior da rede privada, contudo estes servidores terão de ser de tipos diferentes para que usem diferentes números de porta e assim possam ser distinguidos na interface externa. Se for necessário facultar acesso a vários servidores do mesmo tipo na rede privada, existe um problema de encaminhamento.

Para facultar acesso a vários servidores do mesmo tipo terá de ser usado outro factor além do número de porta, pois esta é igual para todos os respectivos servidores. A técnica mais simples consiste em atribuir mais do que um endereço oficial à interface externa do *router*, e depois, deste modo torna-se simples distinguir os vários servidores no interior da rede privada, cada endereço oficial corresponde a um servidor distinto. As entradas estáticas DNAT passam então a conter:

- Número de porta a escutar na interface da Internet (externa).
- Endereço IP a escutar na interface da Internet (externa).
- Endereço IP de destino (na rede privada).
- Número de porta de destino.

No entanto este procedimento nem sempre é possível, pois o custo da aquisição de mais um IP ao ISP poderá ser proibitivo. A outra solução reside na mudança de porta de acesso ao nível do exterior.

Por exemplo, quando é necessário consultar dois servidores diferentes mas que utilizam a mesma porta, e ambos partilham o mesmo IP externo, é necessário fazer um mapeamento especifico das portas externas para as portas internas necessárias

Num exemplo prático, muitas vezes é necessário aceder à intranet da empresa, que normalmente está acessível através da porta 80. Imaginando que seria necessário aceder a outro servidor web interno, igualmente disponível na porta 80, existe um conflito de portas.

Para solucionar este problema normalmente atribui-se o acesso por portas diferentes no exterior, mas igual, no interior (rede privada). A entrada DNAT ficaria então assim:

- Número de porta a escutar na interface da Internet (externa), por exemplo:
  - 207.168.30.45:8080.
- Endereço IP de destino+porta (na rede privada).
  - 192.168.1.30:80

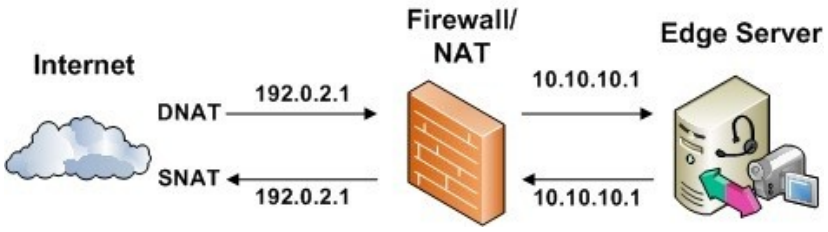

Ilustração 41: NAT Estático

Processo de comunicação numa rede TCP/IP

Pressupondo que o *host* com o endereço IP 172.16.1.101 deseja enviar um pacote para o endereço 172.16.2.102. Caso a máscara de rede seja 255.255.0.0, o AND[8] binário do endereço fonte será 172.16.0.0, e o AND do endereço destino será 172.16.0.0, indicando que ambos possuem o mesmo endereço de rede e portanto estão ambas no nível 1 - da camada de ligação de dados.

Neste caso, o protocolo IP envia um pacote ARP pela rede Ethernet para identificar qual o endereço *MAC* do *host* cujo IP é 172.16.2.2. Este pacote é enviado em *broadcast*, de modo que todos os *hosts* conectados ao mesmo segmento Ethernet recebam o pacote. O *host* configurado com o endereço desejado responde ao pacote ARP indicando qual o seu endereço *MAC*, e assim o IP pode montar o pacote Ethernet correctamente endereçado e enviar o pacote para o seu destino.

Se a máscara de rede não fosse 255.255.0.0, mas sim 255.255.255.0, os endereços de rede da origem e destino seriam diferentes, respectivamente 172.16.1.0 e 172.16.2.0. Significa então que não existe conectividade directa ao nível da camada de ligação de dados entre os dois *hosts.* Por esta razão o pacote deverá ser entregue por intermédio de um *Router*, representado pelo *default gateway*.

Se ao *default gateway* corresponder o IP 172.16.1.1 (o endereço de rede do *default gateway* é 172.16.1.0, o mesmo do *host* de origem), então o *host* poderá irá enviar um pacote ARP à rede para descobrir o endereço *MAC* do *default gateway.* Após a resposta, poderá agora enviar-lhe o pacote com o dado e com o destino 172.16.2.102.

Ao receber o pacote, o *default gateway* irá verificar o endereço IP do remetente e do destinatário. Se o pacote estiver endereçado para a mesma rede local na qual o *default gateway* estiver configurado, o pacote é entregue ao destinatário. Caso contrário, o pacote é direccionado para o *router* mais próximo. O processo de reencaminhamento do pacote pelo *default gateway* segue o mesmo processo de verificar o endereço IP utilizando a máscara de rede, e de, em seguida, enviar um pacote ARP pedindo o endereço *MAC* do próximo *host* a receber o pacote (que aqui será o *Router*). A diferença só se encontra no final do processo, em que o *Router* não tem um *default gateway*, mas sim uma tabela de roteamento, que informa quais endereços de rede que podem ser alcançados, e quais os respectivos *Routers*.

Note-se que este exemplo considera apenas a comunicação entre dois equipamentos, não entre duas peças de software. Este apenas focou a camada de rede da pilha TCP/IP. Acima dela o processo torna-se simples: o IP verifica que tipo de pacote foi recebido (TCP, UDP ou outro) e reencaminha o pacote para o protocolo respectivo.

TCP

Até aqui tem sido maioritariamente descrita a função do protocolo IP, mas como foi visto, este é um protocolo composto por dois principais protocolos, o *Internet Protocol* e o *Transmission Control Protocol*.

O papel do protocolo IP resume-se então a fornecer uma forma de identificar de forma única cada *host* numa rede (endereço IP) e uma forma de encontrar uma rota, ou rotas, entre a origem e o destino de uma comunicação (Roteamento).

Já o papel do protocolo TCP é garantir que os dados, depois de transformados em pacotes, sejam entregues de forma organizada e fiável. Numa comunicação pode acontecer, ou que os

8 Conjunção ou operador "e" (também chamado pela denominação latina "et" ou pela denominação inglesa "and") é um operador lógico utilizado em lógica matemática. É intimamente relacionado à operação de intersecção de conjuntos numéricos.

pacotes não cheguem na ordem que foram anteriormente enviados, ou serem perdidos pacotes durante a transmissão. Em último caso, o TCP tem que informar a origem de que determinado pacote não foi recebido no tempo esperado e solicitar que este seja retransmitido.

Mais aprofundadamente, são então as principais funções deste protocolo:

- **Garantir a entrega dos pacotes** – através de vários mecanismos consegue garantir que os pacotes sejam entregues sem alterações, sem terem sido corrompidos e na ordem correta.
- **Garantir a correta sequência dos pacotes** – é da competência do TCP dividir ficheiros em pacotes e transmitir cada pacote separadamente. Estes podem ser enviados por caminhos diferentes pela rede (roteamento) e não chegar na ordem em que foram transmitidos. No destino os pacotes são ordenados correctamente, antes de serem entregues ao destino, e solicitar a retransmissão quando necessário.
- **Garantir a integridade dos pacotes** – através de cálculos matemáticos o TCP procede a uma verificação de cada pacote para garantir que os dados não foram alterados ou corrompidos durante a transmissão entre a origem e o destino.
- **Garantir a transmissão completa da mensagem** – no destino, os pacotes recebidos são verificados, e, em caso afirmativo, é enviada uma mensagem para a origem, confirmando que cada pacote foi recebido correctamente. Caso um pacote não tenha sido recebido ou tenha sido recebido com falhas, é enviado um pedido de retransmissão do pacote. Este processo apenas se limita aos pacotes danificados, o que contribui para a redução do tráfego na rede, agilizando o envio dos pacotes.
- **Garantir uma transmissão confiável** – porque a transmissão é efectuada através de sessões criadas entre o emissor e o receptor, este é o protocolo por excelência utilizado para funcionalidades como *logins* em servidores, acesso a bases de dados, transporte de correio electrónico, etc.

Portas TCP

Hoje em dia é normal em qualquer computador o utilizador estar a trabalhar em diversas aplicações ao mesmo tempo, como estar a aceder a um ou mais sítios da Internet, usar o programa de recepção de correio electrónico, estar a transferir ficheiros a parir de um servidor de FTP, etc.

A questão que se coloca agora é, depois de os pacotes chegarem à placa de rede, ao chegarem à camada aplicação, como o sistema operativo sabe para qual dos programas se destina cada um dos pacotes recebidos? A resposta para esta questão está na divisão por portas realizada pelo TCP/IP na camada de transporte. Cada programa trabalha com um protocolo/serviço específico, ao qual está associado a um número de porta.

Por exemplo, o serviço de FTP normalmente opera na porta 21 (na verdade opera em duas portas, uma para controlo e outra para o envio de dados). Todo o pacote que for enviado do servidor FTP para o *host*, terá, além dos dados que estão a ser transmitidos, uma série de dados de controlo (ex. número do pacote, código de validação dos dados) e o número da porta associado ao programa. Quando o pacote chega à camada de transporte, é consultado o número da porta do pacote e este é encaminhado para a respectiva aplicação.

Outro exemplo aplicável é o conhecido protocolo HTTP, utilizado para o transporte de informações de um servidor Web até ao navegador do cliente, o qual opera por norma na porta 80. Os pacotes que chegam destinados à respectiva porta são directamente encaminhados para o navegador. Quando existe mais do que um acesso diferente a partir de várias janelas ou

separadores, o protocolo pode incluir informações para além da porta que identificam cada janela ou separador individualmente.

Porta	Protocolo	Descrição
20	FTP (*File Transfer Protocol*) (dados)	Transferência de ficheiros
21	FTP (controlo)	Transferência de ficheiros
23	Telnet	Acesso remoto
25	SMTP (*Simple Mail Transfer Protocol*)	Envio de correio electrónico
80	HTTP (*Hypertext Transfer Protocol*)	Páginas de Internet
110	POP3 (*Post Office Protocol* v3)	Recepção de correio electrónico
139	NetBIOS	Serviço de nomes

UDP

O UDP (*User Datagram Protocol*) é um protocolo que está embutido no protocolo composto TCP/IP. Ao contrário do TCP, este é apenas utilizado para algumas tarefas devido ás suas características. Este permite uma transmissão de dados mais rápida entre *hosts*, porém não dá qualquer garantia na entrega e na verificação de dados. Resumindo, de uma maneira simples, os dados são enviados para o destino mas não existe qualquer controlo se a mensagem vai chegar correctamente, sem erros, e completa.

Esta propriedade deve-se ao facto de o UDP ser desenhado especialmente para transmissões em *Multicast* e *Broadcast* áudio e vídeo, onde não é tão necessária a integridade da mensagem. Para isto o protocolo não utiliza pacotes mas sim datagramas, uma versão mais simples dos primeiros, sendo mais pequenos, porque contêm apenas um cabeçalho e a mensagem.

A seguir apresenta-se uma descrição dos protocolos TCP e UDP e um estudo comparativo.

Serviços e protocolos do TCP/IP

DHCP

O DHCP, abreviatura de *Dynamic Host Configuration Protocol* é um serviço que automatiza as configurações do protocolo TCP/IP nos dispositivos de rede (computadores, impressoras, *hubs*, *switchs,* ou qualquer dispositivo ligado à rede e que utilize como protocolo de comunicação o TCP/IP).

Sem o serviço de DHCP, as configurações TCP/IP de cada *host* terão de ser configurados manualmente. Num cenário possível sem DHCP, sempre que seja necessário efectuar uma alteração nos parâmetros de configuração, como por exemplo uma mudança no número IP do servidor DNS, a reconfiguração teria de ser realizada manualmente em todas as estações de trabalho.

Com um servidor ou um equipamento que disponibilize este serviço, esta tarefa pode ser completamente automatizada, trazendo também consigo diversos benefícios, dentro dos quais se podem destacar os seguintes:

- Automatização e delegação a um equipamento de toda a responsabilidade do processo de configuração do protocolo TCP/IP nos dispositivos da rede.

- Facilidade de alteração de parâmetros tais como *Default Gateway*, Servidor DNS, etc., em todos os dispositivos da rede, apenas através da alteração no servidor DHCP.
- Eliminação de erros de configuração, tais como digitação incorrecta de uma máscara de sub-rede ou utilização do mesmo número IP em dois dispositivos diferentes (o que gera um conflito de endereços IP).

Numa rede com este tipo de serviço, basta que um qualquer equipamento seja ligado à rede (cablada ou wireless), que passado alguns segundos, é configurado automaticamente.

No ponto **Endereçamento e roteamento** foi visto que são necessários pelo menos três parâmetros para que uma rede funcione. Mas num contexto empresarial, que normalmente inclui também um acesso à Internet, bem como muitos outros serviços, são necessários os seguintes elementos para a configuração do TCP/IP de cada *host*:

- Endereço IP
- Máscara de sub-rede
- *Default Gateway*
- Endereço IP de um ou mais servidores DNS
- Endereço IP de um ou mais servidores WINS
- Sufixos de pesquisa do DNS

Este serviço é composto por diversos elementos para a correcta configuração. No servidor DHCP irão ser definidas as configurações que os clientes DHCP irão receber. A seguir são apresentados e identificados os principais termos relacionados com a correcta configuração de um servidor DHCP.

- **Servidor DHCP** – O Servidor DHCP pode assumir diversas formas, desde um Servidor propriamente dito, um computador com um sistema operativo de rede, a um pequeno *router* ou mesmo um s*witch.* Sistemas operativos de rede como qualquer distribuição GNU/Linux ou Microsoft Windows Server podem ser configurados como servidores DHCP.
  - ***Scope*** – A escopo é o intervalo consecutivo de endereços IP possíveis de atribuir para uma rede, por exemplo, o intervalo de [100-150] (10.10.10.100 a 10.10.10.150), na rede 10.10.10.0/255.255.255.0. Em geral, o escopo define uma sub-rede física na rede na qual é disponibilizada o serviço DHCP. O escopo também permite ao servidor gerir a distribuição e atribuição dos endereços IP e restantes parâmetros de configuração (tais como o *Default Gateway*, o Servidor DNS etc.).
  - **Intervalo de exclusão** – Um intervalo de exclusão é uma sequência limitada de endereços IP dentro do escopo que não podem ser atribuídos. Os intervalos de exclusão asseguram que qualquer dos endereços que se encontre neste intervalo não serão atribuídos pelo servidor. Por exemplo, dentro da faixa [100-150], na rede 10.10.10.0/255.255.255.0, pode ser criado um intervalo de exclusão do [120-130].
  - ***Pool*** – Após ter sido definido o escopo e ter sido definido o, ou os intervalos de exclusão, os endereços remanescentes formam uma *pool* de endereços disponíveis dentro do escopo. São estes os endereços que estão seleccionados para serem atribuídos dinamicamente. No exemplo, o escopo [100-150] com a faixa de exclusão de [120-130], a *pool* de endereços é formada pelos intervalo de [100-119] em conjunto com o intervalo de [131-150].

- ***Lease time*** – O *lease time* é um período de tempo durante o qual o IP é atribuído ao *host.* A concessão do IP apenas está activa enquanto estiver a ser utilizada pelo cliente. Desta forma, se o *host* for desligado ou desconectado, quando for reactivado, se o endereço IP atribuído já tiver expirado, pode-lhe ser atribuído um novo IP.
- **Reserva** – A reserva destina-se à atribuição de endereços IP's de forma permanente pelo servidor DHCP. As reservas asseguram que um dispositivo de hardware identificado possa usar sempre o mesmo endereço IP. Esta atribuição consiste numa associação do endereço IP ao endereço *MAC* (endereço de hardware) da placa de rede.

- **Cliente DHCP** – O cliente é um qualquer dispositivo de rede capaz de obter as configurações de TCP/IP a partir de um servidor DHCP. Pode ser um computador, um *switch*, uma impressora, uma câmara de vigilância, entre muitos outros.

DNS

Toda a comunicação entre *hosts* e demais equipamentos de uma rede é feita através do número IP, entre o *host* de origem e o *host* de destino. Porém, para um utilizador, não seria nada produtivo se tivesse de decorar, ou mais realisticamente, consultar uma tabela de números IP toda a vez que tivesse que aceder um recurso na rede.

Quanto a escala de rede é reduzida, entre uma e dez máquinas, utilizar apenas os endereços IP para identificar cada *host* acaba por ser viável, agora em redes de larga escala, como a Internet, identificar cada máquina através do seu endereço IP, torna-se impraticável.

No início do desenvolvimento do TCP/IP, cada *host* continha um ficheiro que listava os nomes de todos os restantes equipamentos e respectivos endereços IP[9]. Na Internet, esta prática seria inviável, porque seria uma tarefa hercúlea manter actualizados todos os milhões ficheiros distribuídos em todas as máquinas, não só pelo seu tamanho mas também pela dificuldade de se manter milhões de cópias sincronizadas. Para resolver este problema foi desenvolvido o DNS, abreviatura de *Domain Name System/Server* que é um serviço de resolução de nomes, pelo qual diversos servidores mantém uma base de dados distribuída com os nomes lógicos e os respectivos endereços IP.

O papel do DNS é então resolver endereços IP em nomes de domínios e vice-versa. Quando é introduzido o URL *www.empresa.tld*, o papel do DNS é traduzir o URL em endereço IP e informar o *Router* do caminho a tomar.

Para uma fácil gestão do DNS, este funciona de forma hierárquica. Um URL típico é composto no mínimo por três partes, o "www" que apenas significa *World Wide Web*, o *alias* ou nome do domínio “empresa” e por fim o .tld (*Top Level Domain*) que representa o tipo ou a localização do domínio (ex.: .pt, .es, .com, .edu). Cada entidade pode ter o seu respectivo servidor de DNS, que contém os nomes dos *hosts* (e respectivos endereços IP correspondentes) sob a sua autoridade. Desta forma é possível criar sub-domínios dentro de um domínio, como por exemplo, departamento.empresa.tld ou país.empresa.tld.

Quando os *hosts* da empresa fazem pedidos por URL's ao servidor do seu domínio, mas que não pertencem ao seu TLD, por exemplo *www.companhia.com*, o DNS transmite esses pedidos a outros servidores DNS quando necessário.

9 Este ficheiro ainda hoje existe, mas existem outros protocolos que obedecem a rotinas automatizada e produzem o mesmo efeito, facilitando a descoberta de *hosts* na rede.

Neste exemplo o pedido seria reencaminhado ao servidor DNS dos TLD comerciais “.com”. Se o pedido fosse feito através do URL *www.escola.edu*, a resolução seria pedida ao DNS dos TLD de “.edu”.

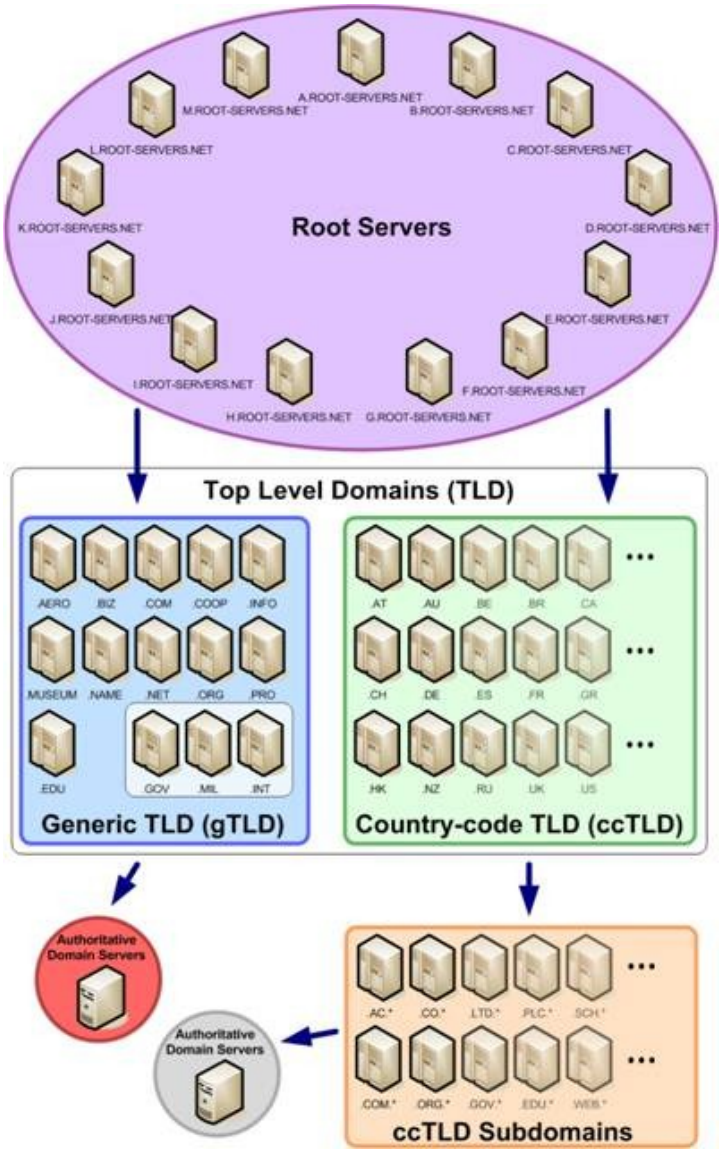

Ilustração 42: Estrutura do DNS

WINS

O WINS (Windows Internet Name Service) é também um serviço de resolução de nomes mas que ainda é mantido por questões de compatibilidade com versões anteriores do Microsoft Windows (95, 98, Me, 3.11) e de compatibilidade com aplicações mais antigas, que ainda dependam da resolução de nomes NetBios, a qual é feita pelo WINS.

Na maior parte dos sistemas operativos da Microsoft os *hosts* podem tem dois nomes, o nome do *host* e o nome NetBios. Nas versões mais actuais estes nomes estão sincronizados, mas nas versões mais antigas, estes podiam ser distintos e ser motivo de incoerências.

O serviço WINS permite que os *hosts* façam o registo do nome NetBios dinamicamente durante o arranque. Desta forma o SO cliente regista o nome NetBios e o respectivo endereço IP na sua

base de dados, podendo desta forma fornecer o serviço de resolução de nomes NetBios para a toda a rede.

Outras Arquitecturas

NetBIOS/NetBEUI

Inicialmente desenvolvido em 1983 pela Sytek Inc. para as redes IBM PC-Network, o NetBIOS (*Network Basic Input/Output System*) é um dos primeiros protocolos com base em datagramas[10] para a transmissão de dados que inclui um serviço de nomes que identifica *hosts* na rede.

Na prática não é um protocolo de comunicação de redes de computadores, mas sim uma API que fornece diversos serviços para camada de sessão do modelo OSI, permitindo que qualquer aplicação comunique com outra aplicação, entre computadores com sistemas operativos distintos, numa rede local. Disponibiliza essencialmente os seguintes três serviços:

- Estabelece nomes lógicos na rede (nomes de *hosts*);
- Estabelece conexões entre *hosts* (chamadas sessões) através dos nomes lógicos;
- Transmite dados entre *hosts* na rede através das sessões;

Nos sistemas operativos mais antigos este protocolo corria sobre o IEEE 802.2 e o IPX/SPX (arquitectura abordada a seguir) e actualmente ainda é executado sobre redes TCP/IP através do protocolo *NetBIOS over TCP/IP* (NetBIOS sobre IPX/SPX).

Esta arquitectura foi desenhada para ser dinâmica e auto-configurável para redes não superiores a 200 nós, e onde a instalação de um novo nó da rede deveria ser tão simples quanto possível. A configuração de uma máquina foi reduzida apenas (ou quase) à definição de seu nome na rede.

Foi nesta estrutura que foi implementado o conceito de nome de serviço ou nó, permitindo que uma máquina se conecte à rede reservando um nome para si. Não existe um servidor central para gerir os nomes, portanto cada máquina é livre de utilizar um nome, desde que este não esteja já em uso. Por ser de tão simples configuração, foi desenhado para pequenas redes e como tal não permite o roteamento de pacotes.

O NetBEUI (*NetBIOS Extended User Interface*) é uma versão actualizada do protocolo NetBIOS originalmente concebida com o propósito, entre outras coisas, de suportar o maior número de nós em *Token Ring* e aumentar a sua velocidade. O nome supostamente deveria representar essa implementação, mas em 1985 a Microsoft elegeu este nome para a implementação do protocolo NBF (*NetBIOS Frames protocol*) literalmente renomeando a implementação do protocolo de transporte nos seus sistemas operativos após a segunda versão da API NetBIOS da IBM.

IPX/SPX e NetWareLink

O IPX/SPX é um protocolo de comunicação de redes sobre Ethernet desenvolvido pela Novell com base no protocolo XNS da Xerox. Construído para ser o padrão no sistema operativo

10 Um datagrama é uma unidade de transferência básica associada a uma rede comutada de pacotes em que a entrega, hora de chegada e a ordem não são garantidas.

NetWare, também da Novell, o IPX/SPX é, à semelhança do TCP/IP, um protocolo dividido por camadas.

À similitude do NetBIOS, este foi desenvolvido para ser um protocolo pequeno e rápido, mas com a diferença que permite o roteamento. Suporta mais do que um tipo de standards, tais como o Ethernet II, IEEE 802.2 e IEEE 802.3.

O IPX/SPX também implementa e suporta a API NetBIOS, permitindo a comunicação com outros *hosts* e/ou sistemas operativos que tenham instalado este protocolo. Tanto a Novell como a Microsoft (NWLink ou *NetWareLink*) implementaram o protocolo *NetBIOS over IPX/SPX* nos respectivos sistemas operativos, permitindo que ambos os SO comuniquem entre si a partir deste protocolo de forma transparente.

Tipos de Rede

Peer-to-Peer/Ponto-a-Ponto

Este tipo de rede define-se por um sistema distribuído de organização horizontal caracterizado pela descentralização das funções na rede, onde cada nó pode realizar tanto a função de servidor como a de cliente. Aqui, cada nó está ligado entre si e têm o mesmo estatuto (*peer*) na rede.

Nesse tipo de rede, pastas, ficheiros, dados podem ser partilhados por qualquer nó e cada um deles pode (dependendo das permissões atribuídas) facilmente aceder, ler, alterar e editar os conteúdos armazenados nos restantes nós. Podem também ser partilhados periféricos e utilizados pelos restantes nós, como é normalmente o caso de drives ópticas, impressoras, etc.

Características de uma rede Ponto-a-Ponto:

- Utilizada em redes de pequena dimensão (normalmente até 10 *hosts*);
- Implementação fácil e de baixo custo;
- Baixos níveis de segurança;
- Sistemas simples de cablagem;
- Os *hosts* podem funcionar sem estar conectados à rede;
- Normalmente não existe um administrador de rede;
- Normalmente não existem máquinas servidoras, cada *host* pode ser um tipo de servidor;

Client-Server/Cliente-Servidor

Aqui todo o sistema deixa de ser distribuído e horizontal e passa para uma estrutura centralizada e vertical (hierárquico) num novo elemento denominado servidor.

O servidor é um computador que disponibiliza um ou mais recursos para os demais clientes (deixa-se aqui a denominação de *host*) na rede, ao contrário do que acontece com a rede ponto-a-ponto. Esta estrutura permite gerir, administrar e configurar a rede de forma centralizada, convergindo todas as acções e funcionalidades apenas neste equipamento, melhorando a segurança e organização da rede.

Concentrar determinadas funcionalidades num servidor dedicado permite o aumento da velocidade de resposta às solicitações dos vários clientes (estações de trabalho), pois este é normalmente desenhado para tarefas específicas. Nas redes onde o desempenho pode ser um

factor crítico, algumas tarefas podem ser distribuídas por vários servidores não dedicados, melhorando a capacidade de resposta, mas de forma transparente para as estações de trabalho.

Características de uma rede Cliente-Servidor:

- Desenhada para redes de larga escala (superior a 10 clientes);
- Necessidade de desenho e estruturação, com maior custo de implementação;
- Maior nível de segurança;
- Desenhada para o desempenho comparada com uma rede ponto-a-ponto;
- Configuração e manutenção da rede centralizada;
- Requer mão-de-obra especializada;

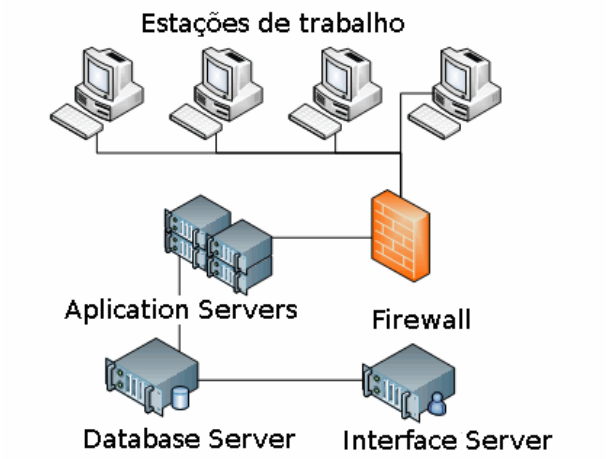

Ilustração 43: Exemplo de arquitectura cliente-servidor

Actualmente uma configuração de uma rede local típica, na perspectiva de hardware, assenta essencialmente num servidor que deve disponibilizar serviços de forma ininterrupta e deve ser suficientemente flexível para suportar grandes aumentos de carga, numa interface de rede, nos meios de transmissão, nos postos de trabalho e nos dispositivos para realização de cópias de segurança.

Tipos de Servidores

Como foi abordado no início do capítulo, algumas das vantagens das redes locais focam a centralização e a partilha de recursos, quer eles sejam equipamentos, programas, bases de dados, ou meios de comunicação.

Entre os diversos serviços, destacam-se os seguintes: o armazenamento e a partilha de ficheiros, a disponibilização e gestão de base de dados, o suporte de impressão, a resolução de nomes (DNS), acesso remoto a servidores e terminais, a gestão e monitorização de redes, a criptografia, o correio electrónico, *gateways* para outras redes e outras funções de partilha de hardware e software.

A um nível mais abstracto, os servidores podem ser também clientes de serviços de outros servidores. Por exemplo, um servidor de impressão pode ser cliente de um servidor de ficheiros ao fornecer serviços de impressão através dos restantes clientes. O serviço comum de correio electrónico é um outro exemplo de servidor que muitas vezes depende de um servidor de correio

externo, o qual armazena e reencaminha as comunicações para os outros servidores das outras empresas.

Dependente da estrutura necessária para cada caso específico de cada empresa, podem existir vários servidores, cada um disponibilizando determinado(s) serviço(s). Se dependentes de um servidor central denominado de Servidor Primário, estes passarão a denominar-se Servidores Secundários.

Também poderão existir um ou mais servidores que estão sincronizados com o Servidor Primário e estão prontos a entrar em funcionamento sempre que existir um problema, ou simplesmente o Primário falhar, denominados de Servidores de *Backup*.

Servidor de Rede

Este servidor tem como função a gestão e a monitorização da rede ao nível do tráfego, do estado, do desempenho e da presença dos clientes (*hosts*) na rede, assim como a monitorização dos meios de transmissão. Desta forma é possível a um administrador de rede detectar erros e efectuar diagnósticos com o fim de resolver eventuais problemas da rede, tais como falhas de comunicação, quebras de desempenho, etc.

Servidores de Ficheiros

O Servidor de ficheiros tem a função de disponibilizar a toda a rede, independente do sistema operativo, um serviço de armazenamento, partilha e acesso a ficheiros, através da partilha de uma parte ou da totalidade de uma ou mais unidades de armazenamento. O seu papel é também controlar essas mesmas unidades bem como o acesso ao seu conteúdo. Através de sistemas operativos de rede, pode também controlar os tipos de acesso (ler, alterar, apagar, etc.) e também que tipo de acesso terá cada utilizador ou grupos de utilizadores.

Para que o acesso e a partilha de ficheiros funcione para diferentes sistemas operativos de rede, é necessário que esteja a ser utilizado um standard para o sistema de ficheiros (NFS[11] por exemplo). Os vários ficheiros das demais estações de trabalho devem ser então convertidos (pelos protocolos da camada apresentação) para o correcto armazenamento no servidor.

Servidor de Aplicações/Serviços

Este tipo de servidor permite disponibilizar à rede determinados serviços e aplicações inseridas no contexto da estrutura cliente/servidor, como, por exemplo, uma base de dados, um servidor Web, servidor de calendários, acesso remoto a determinado software, entre outros.

Servidor de Impressão

O Servidor de Impressão tem como finalidade facultar serviços de impressão aos restantes clientes da rede. Este servidor é passível de ter várias configurações, entre ser um equipamento ou um computador com vários tipos de impressoras acopladas, cada uma adequada à qualidade ou rapidez de uma necessidade particular, ou simplesmente uma impressora que contem uma placa de rede e que permite a impressão através desse meio. O servidor de impressão pode ainda ser parte constituinte de um servidor de aplicações ou serviços.

O modo de funcionamento é relativamente simples e onde normalmente é utilizada a técnica de *spooling*. Esta palavra deriva do termo s*pool* (*Simultaneous Peripheral Operation Online*) e refere-se a um processo de transferência de dados e colocação destes num espaço de memória temporária enquanto um determinado equipamento não os processa. A técnica de s*pooling*

11 NFS (acrónimo para *Network File System*) é um sistema de ficheiros desenvolvido pela *Sun Microsystems, Inc*., a fim de permitir a partilha de ficheiros e pastas entre computadores com sistemas operativos distintos numa rede local.

aplicada à impressora consiste em colocar os trabalhos de impressão num *buffer*[12] a que normalmente se dá o nome de fila de espera enquanto não é iniciado o processo de impressão. São também colocados em fila de espera todos os trabalhos enviados por outros clientes e que tem de esperar que o documento anterior seja impresso.

Servidor de Correio Electrónico

O servidor de correio electrónico é o responsável pelo envio, processamento e entrega de mensagens de correio electrónico.

O funcionamento de um servidor de correio electrónico é baseado na utilização de uma caixa de correio. Aquando do envio de uma mensagem, esta é encaminhada de servidor em servidor até ao servidor de serviço de mensagens do destinatário. Mais exactamente, a mensagem é enviada ao servidor de correio electrónico encarregado do transporte nomeado *Mail Transport Agent* (MTA), até ao MTA do destinatário. Na Internet, os MTA comunicam entre eles graças ao protocolo SMTP.

O servidor MTA do destinatário entrega então o correio ao servidor de correio electrónico que entra, nomeado de *Mail Delivery Agent* (MDA), que armazena a mensagem esperando que o utilizador a descarregue. Existem dois protocolos principais que permitem levantar o correio de um MDA:

- o protocolo POP3 (*Post Office Protocol*), mais antigo, permite descarregar o correio e eventualmente deixar uma cópia no servidor.
- o protocolo IMAP (*Internet Message Access Protocol*), permitindo uma sincronização do estado dos correios (lido, suprimido/apagado, deslocado) entre vários clientes de serviço de mensagens. Com o protocolo IMAP uma cópia de todas as mensagens é conservada no servidor para poder assegurar a sincronização.

Por analogia com o mundo real, o MTA funciona como um posto dos correios (centro de triagem e carteiro que assegura o transporte), enquanto os MDA funcionam como caixa de correio, para armazenar as mensagens (no limite da sua capacidade em volume), até os destinatários abrirem a sua caixa. Isto significa nomeadamente que não é necessário que o destinatário esteja conectado para poder receber correio.

Servidor de Comunicações

O servidor de comunicações realiza tarefas relacionadas com as várias possibilidades de comunicação quer da rede interna, quer com redes externas. O seu principal papel normalmente é de *Gateway/Router* entre a rede interna e a externa, disponibilizando o acesso à Internet.

Em conjunto com a sua principal função de rotear todo tráfego interno para outra rede ou a Internet, este servidor pode correr vários serviços de comunicação, tais como um servidor de correio electrónico, um servidor de mensageiro (*XMPP/Jabber*)[13], um servidor de Intranet[14], bem como outros serviços que permitam a comunicação interna e/ou externa.

12 Região ou espaço de memória temporário utilizado para escrita e leitura de dados quando existe uma diferença entre a velocidade em que os dados são recebidos e a velocidade a que estes podem ser processados.

13 *Extensible Messaging and Presence Protocol* (XMPP) (conhecido anteriormente como *Jabber*) é um protocolo aberto, extensível, baseado em XML, para sistemas de mensagens instantâneas.

14 O conceito de Intranet pode ser interpretado como "uma versão privada da Internet", ou uma mini-Internet confinada a uma organização.

Servidor de Directório

Um serviço de directorias normalmente disponibilizado por um servidor de Directório permite armazenar informação de forma extensível e que pode ser acedida através de rápidas pesquisas. Embora sejam muitas vezes confundidos com bases de dados, os serviços de directorias distinguem-se em vários aspectos:

- São geralmente organizadas de forma hierárquica e orientada a objectos. A organização das entradas em árvore espelha as relações existentes entre os objectos.
- Nos serviços de directorias, é usado um *schema* (esquema) que define o que pode e o que deve ser guardado, para uma certa classe de objectos, o que facilita a interoperabilidade.
- Oferecem um modelo de segurança que permite a herança de permissão de acesso às entradas.
- As directorias são feitas para serem submetidas a mais operações de leitura do que de escrita, enquanto que nas bases de dados se assume que estas operações ocorrem em número semelhante.

O LDAP (*Lightweight Directory Access Protocol*) é um protocolo que define um pequeno conjunto de operações de acesso a directorias. É baseado no modelo TCP/IP, e, em comparação com os protocolos antes existentes, pode ser considerado *lightweight*, isto é, leve para sistema operativo. Na última versão do LDAP, o LDAPv3, definem-se várias mecanismos para autenticação de clientes, desde a autenticação anónima até outras mais seguras e robustas, como SSL[15]/TLS[16] ou SASL[17].

Sistemas Operativos de Rede

A evolução das formas de trabalho com base em plataformas tecnológicas obrigou a diversas modificações ao nível do *hardware* para que as diversas máquinas pudessem comunicar entre si e em rede. Foram feitos diversos ajustes aos Sistemas Operativos, adaptando-os para este novo ambiente.

Os computadores pessoais, que antes apenas funcionavam isoladamente, sempre funcionaram os seus respectivos Sistemas Operativos Locais (SO). Com o advento e a evolução das redes de comunicação surgiram os Sistemas Operativos de Rede (SOR), estendendo as funcionalidades permitidas pelos SO, complementando-os com o conjunto de funcionalidades necessárias à operação das estações de trabalho (clientes), de forma a tornar o mais transparente possível o uso dos recursos partilhados em todo sistema computacional e na restante rede.

Um Sistema Operativo de Rede (SOR) é um SO que foi desenhado para servir de suporte à conexão de redes locais por parte de *Workstations*, computadores pessoais, e, em algumas instâncias, antigos terminais que necessitavam de ligações a *Mainframes*. São exemplos dos primeiros SOR o *Artisoft LANtastic, Banyan VINES, Novell's NetWare* e *Microsoft's LAN Manager*.

Por norma um SOR disponibiliza diversos serviços, tais como: a partilha de impressoras, a partilha de espaço de armazenamento, o acesso a base de dados, a partilha de aplicações, para

15 SSL (acrónimo para *Secure Sockets Layer*) é a tecnologia padrão de segurança para estabelecer uma conexão criptografada entre um servidor web e um navegador. Esta ligação assegura que todos os dados transferidos entre o servidor web e os navegadores (*browsers*) permanecem privados e integrais.

16 TLS (acrónimo para *Transport Layer Security*) é o método de encriptação de dados mais utilizado na comunicação entre os servidores Web e os browsers, mas também pode-se utilizar para os servidores de email e os seus clientes.

17 SASL (acrónimo para *Simple Authentication and Security Layer*) é um protocolo que tem como objectivo fornecer um mecanismo de autenticação dos clientes perante o servidor.

além da capacidade de gerir vários aspectos importantes de uma rede, como o domínio, a segurança e o controlo de acessos. Nos sistemas mais actuais, é papel do SOR ajudar a gerir os fluxo de dados entre o(s) servidor(es) e os restantes clientes da rede.

O conceito de transparência anteriormente referido é um dos requisitos fundamentais dos SOR. Nesse sentido, estes devem actuar de forma que os utilizadores possam fazer uso dos diversos recursos da rede ou do servidor como se a operação estivesse a ser realizada localmente. Esta funcionalidade é disponibilizada através de um módulo de reencaminhamento de pedidos que foi desenvolvido durante a evolução dos SOR para permitir o acesso aos diversos recursos que a rede ou o servidor disponibilizam.

No caso de uma máquina local, a interface entre o software e o SO funciona com base numa interacção de solicitação/resposta, onde a aplicação solicita um serviço (abertura de um ficheiro, impressão, reserva de uma área de memória etc.) através de um pedido ao SO. Este, em resposta, executa o serviço solicitado e responde, informando o estado da operação (se foi executado com sucesso ou não) e transfere os dados resultantes da execução para a aplicação, se assim for o caso.

No modo de Cliente-Servidor, o processo é em tudo similar, mas a entidade que solicita um serviço é chamada de cliente e a que presta o serviço é chamado de servidor. As estações de trabalho que disponibilizam o acesso aos seus recursos através da rede a outras estações devem ter instalado de alguma forma um módulo servidor.

O SOR, para além das funções de comunicação inerentes a todo o processo aqui já enumeradas, poderá correr vários outros serviços de elevada importância na actualidade. Um dos mais importantes é o serviço de controlo de acessos aos recursos partilhados aos vários utilizadores/clientes. Este tem como função evitar, por exemplo, que um utilizador não autorizado tenha acesso ou apague ficheiros que não lhe pertencem.

Administração

O Administrador de Rede é a entidade que instala, opera e gere a rede, bem como o SOR. É da sua competência configurar os equipamentos e o software para que ambos trabalhem em conjunto.

A instalação e manutenção de um SOR são normalmente efectuadas através de uma interface composta por opções que podem ser seleccionadas por teclado, ou nos mais recentes, também com o rato. Através desta interface o administrador pode efectuar uma série de operações, como formatar unidades de armazenamento e configurá-las para acesso partilhado, configurar um servidor DHCP e respectivo *lease* e *scope,* configurar um domínio de uma rede, configurar o acesso à Internet, proceder à criação de utilizadores e respectivas credenciais, definir restrições de segurança (com base nos utilizadores ou grupos de utilizadores). A partir desta interface também podem ser instalados, configurados e partilhados diversos dispositivos como impressoras e/ou scanners, ou configurar procedimentos automáticos de cópias de segurança.

Na actualidade, reconhecem-se mais comummente os SOR *UNIX*®, *GNU/Linux*, *Windows Server*®, e *Netware*®. Cada um destes é distinto entre si, embora com funções similares, mas podem servir diferentes necessidades. Para a sua conveniente administração é necessário um conhecimento aprofundado, quer das suas características, quer das suas metodologias. Num ambiente empresarial é conveniente que os administradores de rede sejam de alguma forma certificados a fim de gerirem convenientemente as redes locais sob a sua alçada.

Estrutura

A estrutura de um SOR está dividida nas seguintes entidades:

- Servidor
- Serviços
- Cliente
- Grupo de Utilizadores
- Utilizador

Cada uma destas entidades distingue e define as diferentes formas de como o sistema operativo de rede interage com a restante rede. A forma como são organizados e configurados normalmente também reflectem a estrutura da organização ou empresa onde estão inseridos. Cada uma delas tem as suas propriedades, as quais podem ser configuradas diferentemente, consoante:

- Servidor – a entidade Servidor já foi abordado anteriormente, onde foram apresentados os vários tipos de servidores disponíveis. Na prática esta entidade é a conjunção do sistema operativo, dos vários serviços que disponibiliza em conjunto com os serviços de gestão de (máquinas) clientes, grupos e utilizadores.
- **Serviços** – correspondem aos diversos serviços disponibilizados pelo servidor que também já foram abordados anteriormente. Destes destacam-se os serviços de DNS, de DHCP, de Directório, de partilha de recursos, etc.
- **Cliente** – equipamento ou máquina que está dependente do servidor e importa definições e serviços deste.
- **Grupo de Utilizadores** – é um conjunto de contas de utilizador a que são atribuídas as mesmas configurações e os mesmos direitos de segurança através de Políticas de grupo. Na prática tem a função de agregar os utilizadores em conjuntos, da mesma forma que são organizados nas empresas e definir o que pode ou não fazer. Ainda assim, o sistema prevê que uma conta de utilizador possa ser membro de mais do que um grupo. Em *Microsoft Windows Server*, os grupos de utilizadores são denominados por grupos de segurança. Os SOR já trazem alguns grupos predefinidos:
  - Grupo de Utilizadores padrão – ao utilizador que esteja inserido neste grupo é normalmente atribuído a denominação de conta padrão. Este é normalmente um grupo restrito que implementa algumas restrições de segurança que impedem, por exemplo, de efectuar configurações ou alterações profundas no sistema operativo cliente (instalar e remover hardware/drivers), instalar e remover programas e aceder a documentos de outros utilizadores.
  - Grupo de Administradores – uma conta de administrador permite não só gerir todo o SOR, como os utilizadores, os seus grupos, bem como todos os seus privilégios ou restrições de segurança.
- **Utilizador** – são as contas de utilizador inseridas dentro dos grupos de utilizador, dependentes das suas restrições e configurações, que permitem a cada pessoa, através das suas credenciais (nome de utilizador e palavra-passe) aceder ao sistema, normalmente de uma máquina cliente e proceder ao seu trabalho.

Bibliografia

Sousa.Sérgio (1997). “Tecnologias de Informação. O que são? Para que servem?”. FCA.

Exame Informática (Março de 2004, n.º 105, Ano 8).

Connect (Dezembro de 2003, n.º 59)

BIT (Março de 2004, n.º 66, Ano 6)

MARITNS.Eulália (1998). “Redes Locais – Perspectiva de Hardware”. Instituto de Informática.

BOAVIDA, F., BERNARDES, M., VAPI, P., *Administração de Redes Informáticas*, FCA, Março de 2009

Edmundo Monteiro, Fernando Boavida, *Engenharia de Redes Informáticas*, FCA – Editora de Informática, 2000.

ANSI (Ed.), *TIA/EIA-T568-A – Commercial Building Telecommunications Cabling Standard*, ANSI, 1991.

CENELEC (Ed.), *EN 50173 – Information Technology – Generic Cabling Systems*, CENELEC, 1995.

HALSALL, Fred, Data Communications Computer Networks and Open Systems (4 Ed), Addison Wesley, Reading, MA, 1995.

ISO/IEC (Ed.), *International Standard ISO/IEC 11801 – Information technology – Generic cabling for customer premises cabling*, ISO/IEC, 1996.

Cibergrafia

http://wireless.com.pt

http://hotspotportugal.com

http://www.ptwireless.pt

http://netcabo.sapo.pt/wireless

http://www.telepac.pt/suporte/wifi

http://www.vodafone.pt/main/Servicos+Roaming/Servicos/WapDados/WirelessLan.htm

http://www2.ufp.pt/~lmbg/textos/norma_osi.html

http://www.wisegeek.com/what-is-a-network-operating-system.htm

http://pt.kioskea.net/contents/courrier-electronique/fonctionnement-mta-mua.php3

http://www.dei.isep.ipp.pt/~andre/documentos/index.html

http://www.subnet-calculator.com/subnet.php