Redes de Computadores

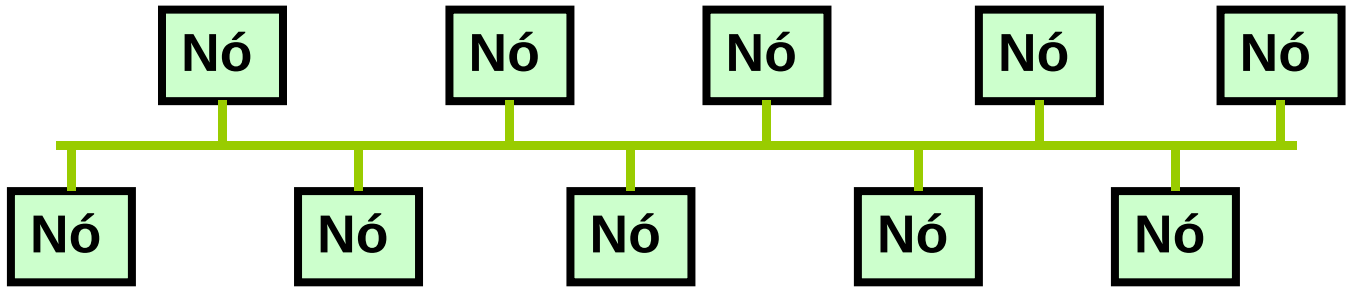
(RCOMP – 2015/2016)

Tecnologias de rede local ETHERNET
Redes locais virtuais (VLAN)
Redes locais sem fios

Redes ETHERNET – CSMA/CD

As redes ETHERNET (IEEE 802.3 / ISO 8802-3) foram originalmente desenvolvidas pela Xerox nos anos 70. Atualmente exercem um claro domínio nas redes locais cabladas.

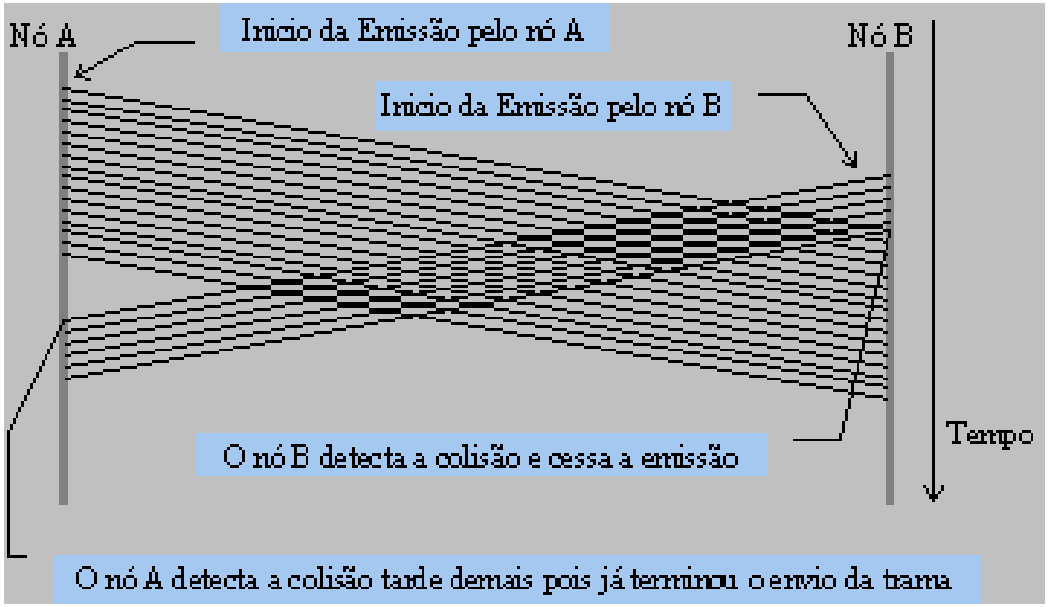
Originalmente o controlo de acesso ao meio (MAC – Media Access Control) era um aspeto fundamental, a técnica CSMA/CD usada neste tipo de rede não é propriamente ideal, trata-se de um mecanismo que não evita as colisões e como tal tem baixa eficiência sob tráfego elevado.
Nas primeiras versões a rede era constituída por um cabo coaxial ao qual todos os nós eram ligados (topologia BUS), as variantes mais importantes foram o 10base5 (10 Mbps/Digital/500m) e o 10base2 (10 Mbps/Digital/180m).



Redes ETHERNET – Domínio de Colisão

A técnica CSMA/CD obriga a que as colisões de dados sejam detetadas por todos os nós antes da transmissão do pacote cessar. Isto introduz limites na relação entre o tempo de transmissão do pacote e o atraso de propagação.

Para garantir a deteção de colisões por todos os nós fixa-se um tamanho mínimo para os pacotes (tempo de transmissão) de 64 octetos, e um tamanho máximo para a rede (atraso de propagação). Esta limitação relativa ao tamanho da rede deriva da necessidade de detetar as colisões e designa-se domínio de colisão.



- O domínio de colisão pode não coincidir com a extensão da rede ETHERNET, os dispositivos *store & forward* isolam os domínios de colisão.
- Maiores taxas de transmissão resultam em domínios de colisão cada vez mais pequenos.

Redes ETHERNET – pacotes e endereços

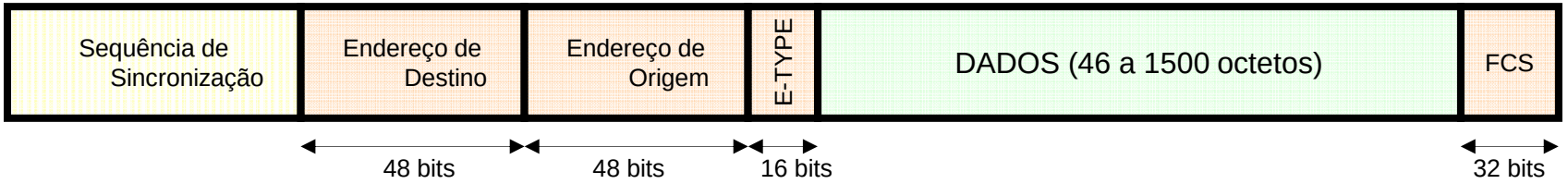
As redes ETHERNET evoluíram muito ao longo do tempo, mas mantiveram desde a origem o mesmo formato de pacote e endereçamento. Isto permite compatibilizar totalmente as várias evoluções técnicas ocorridas, de tal forma mesmo as últimas versões surgidas a 10 Gbps sobre fibra ótica podem ser ligadas a segmentos de rede 10base5 e 10base2.

Cada nó é identificado por um número de 48 bits, designado de endereço de nó, endereço físico ou endereço MAC.

- Normalmente estes endereço são representados sob a forma de 6 octetos em notação hexadecimal, separados por dois pontos, por exemplo: **00:60:B0:3C:93:DB**.
- Para garantir que os endereços são únicos, a cada fabricante de hardware é atribuída uma sequência fixa para os primeiros 24 bits.
- O endereço **FF:FF:FF:FF:FF:FF** é o endereço de *broadcast*, um pacote com este endereço de destino chega a todos os nós da rede.

Redes ETHERNET – formato de pacote

A manutenção de um formatos de pacote fixos ao longo da sua evolução foi um fator importante para o sucesso das redes ETHERNET. Os pacotes na camada de ligação lógica são habitualmente designados de tramas, *frames* ou quadros. Podem coexistir sem grandes problemas vários formatos de trama numa mesma rede ETHERNET, mas o mais divulgado é o *Ethernet II*, também conhecido por DIX (Digital, Intel, Xerox):



De entre os vários formatos existentes, este é o mais simples, mas implementa tudo o que é necessário. Endereços de nó de origem e destino, identificador para multiplexagem (E-TYPE) e código para deteção de erros (FCS – Frame Check Sequence). O formato de pacote ETHERNET é tão divulgado que as novas tecnologias como o 802.11 suportam este formato para permitir a interligação direta.

Redes ETHERNET – do barramento à estrela

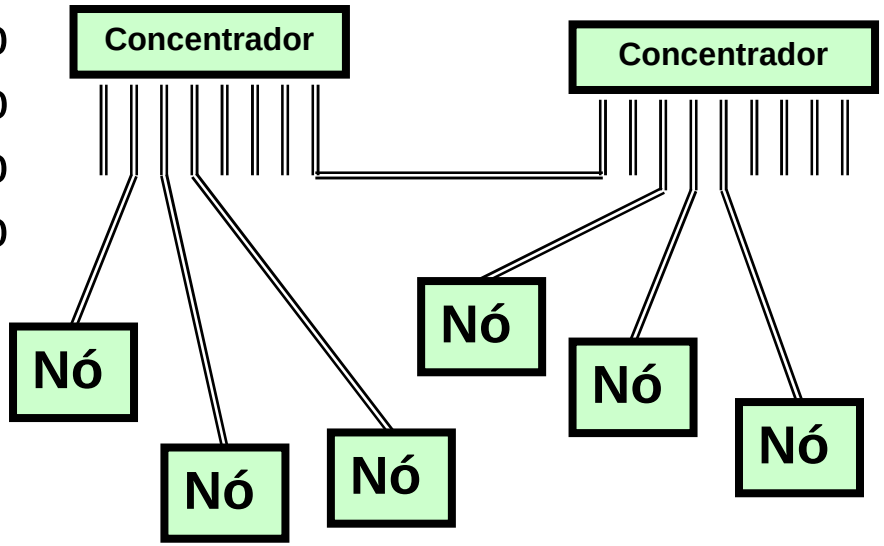
A topologia em barramento de cabo coaxial das variante 10base5 e 10base2 proporcionaram redes de custo extremamente reduzido, é a este fator que a redes ETHERNET devem a sua expansão inicial.

No início dos anos 90 começaram a surgir outras implementação baseadas em dois pares de cobre entrançados (10baseT) ou duas fibras óticas (10baseFL e 10baseFB). Nestas variantes cada nó possui duas ligações separadas (TX e RX) a um dispositivo concentrador, a topologia foi então modificada para estrela.

Apesar da nova topologia, o modo de funcionamento mantém-se e o CSMA/CD impõe restrições quanto ao domínio de colisão, por exemplo para o 10baseT é de 500 metros.

Mas há novas possibilidades:

- Comutação.
- *Full-duplex*.



Redes ETHERNET – comutação de tramas

A topologia em estrela veio abrir novas possibilidades, ao existirem ligações separadas TX e RX para cada nó da rede torna-se possível modificar radicalmente o modo de funcionamento destas redes. Se o dispositivo concentrador/repetidor for modificado por forma a poder:

- Receber várias tramas simultaneamente em quaisquer portas.
- Emitir várias tramas simultaneamente em quaisquer portas.
- Armazenar temporariamente tramas quando necessário.
- Fixar os endereços de origem das tramas que vão chegando a cada porta (tabela MAC).
- Analisar os endereços de destino e retransmitir as tramas apenas nas portas correspondentes (tabela MAC).

Este concentrador é rebatizado de comutador (*switch*) e introduz melhorias enormes no funcionamento da rede.
Existindo ligações duplas dedicadas torna-se impossível a ocorrência de colisões, usando um comutador o CSMA/CD é desativado.

Redes ETHERNET comutadas

Muito mais do que qualquer aumento de taxa de transmissão, a comutação foi um progresso enorme pois eliminou os maiores problemas originais das redes ETHERNET.

>> Funcionamento em *full-duplex*, sem colisões e sem controlo de acesso ao meio.
>> Encaminhamento com base no endereço de nó para que as tramas cheguem apenas ao nó de destino (gestão da tabela MAC).
>> Eliminação dos domínios de colisão, eliminando as restrições nas dimensões máximas da rede.
>> Redução ao máximo de congestionamentos por ação dos comutadores.

Estes fatores aumentaram de forma drástica a eficiência geral da rede, traduzindo-se num aumento de velocidade aparente muito mais importante do que qualquer aumento de taxa de transmissão.

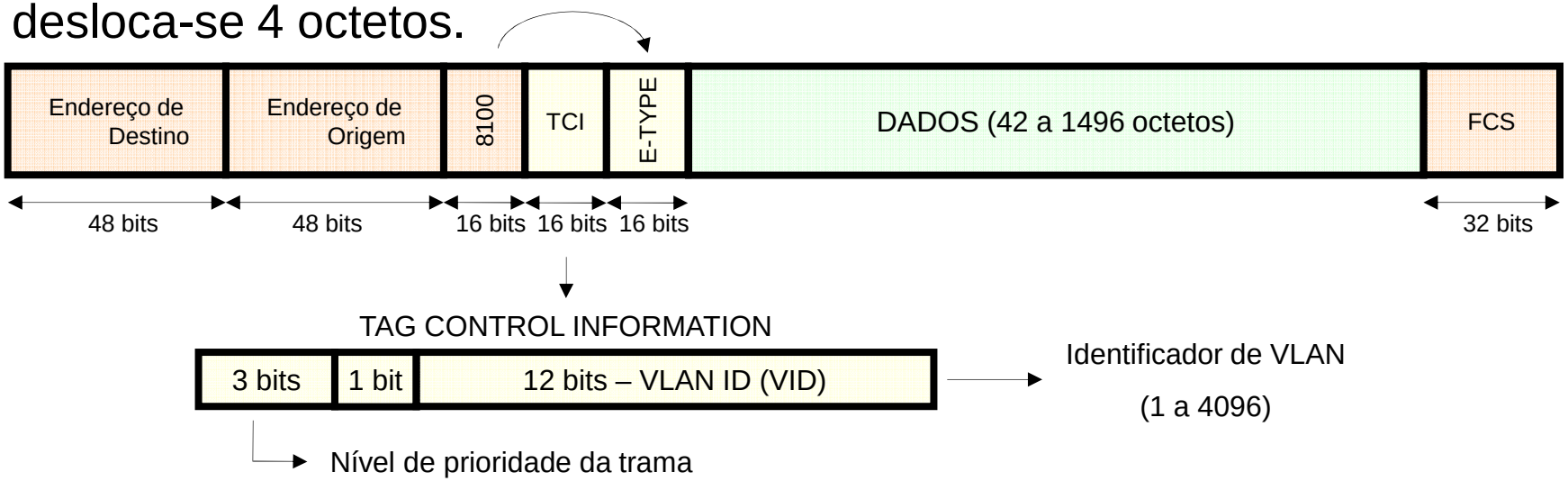
Redes Ethernet – resumo de tecnologias atuais

100base…	**TX**: Usa dois pares de cobre de um sistema de cablagem tipo 5 ou superior, o comprimento máximo de um segmento é 100 metros. **FX**: Usa duas fibras multimodo, o comprimento máximo de um segmento é 2 Km.
1000base…	**T**: Usa quatro pares de cobre de um sistema de cablagem tipo 5E ou superior, o comprimento máximo de um segmento é 100 metros. Não suporta *full-duplex*. **SX**: Usa duas fibras multimodo, o comprimento máximo de um segmento é 220 metros ou 550 metros, respetivamente para fibras de 62,5 ou 50 micons. **LX**: Usa duas fibras monomodo, o comprimento máximo de um segmento é de 5 Km, mas pode ser superior, de acordo com as especificações do fabricante.
10Gbase…	**SR/LRM/LR/ER/LX4**: são várias normas correspondentes a diversos tipos de fibra ótica que resultam em vários distâncias máximas suportadas que podem ir desde as dezenas de metros até à centena de Km. **CX4/Kx/T**: utilizam vários tipos de cablagem de cobre especial, com características elétricas especiais, o 10GbaseT usa 4 pares CAT6A.
40Gbase…	**CR4/SR4/LR4**: a primeira usa 4 cabos de cobre coaxiais de características especiais, a segunda utiliza quatro fibras multimodo e a terceira utiliza quatro fibras monomodo.
100Gbase…	**CR10/SR10/LR4/ER4**: As primeiras duas utilizam, respetivamente, 10 cabos de cobre coaxial especial e 10 fibras multimodo. As duas últimas utilizam quatro fibras monomodo e diferem no comprimento máximo que podem atingir.

Próximas evoluções previstas: 400 Gbps e 1 Tbps

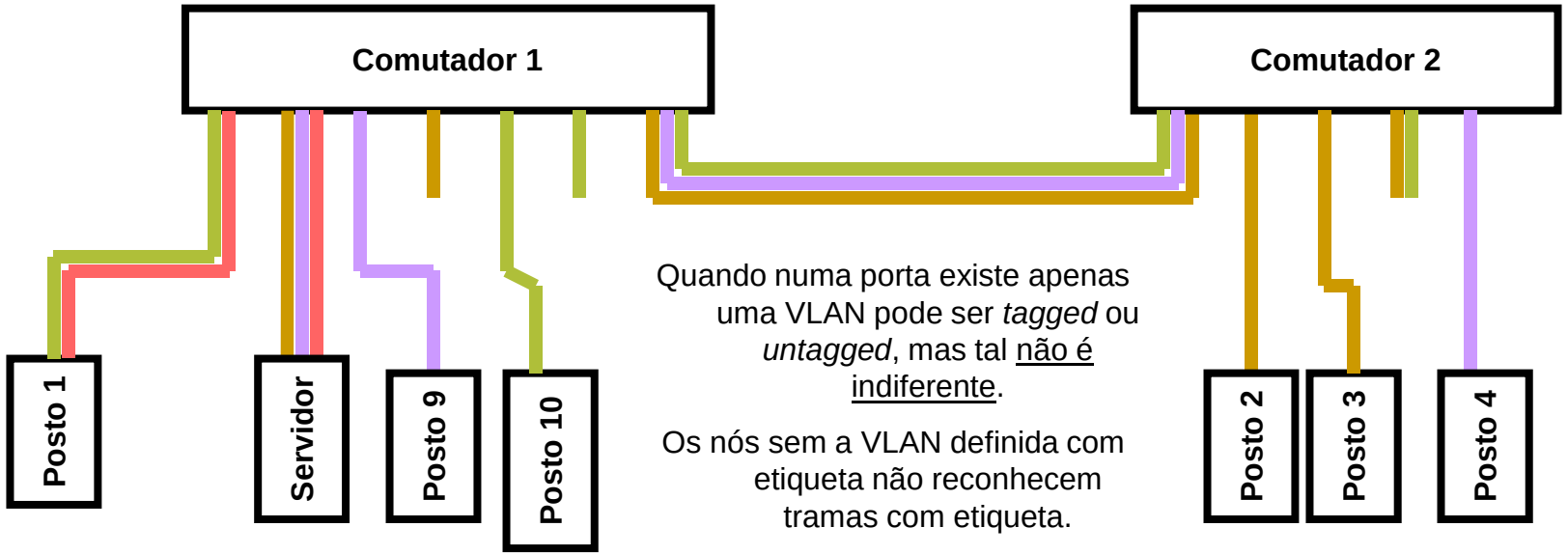
Redes Locais Virtuais - IEEE802.1Q

Uma rede local virtual (VLAN) é uma rede lógica definida sobre uma rede física. Sob todos os pontos de vista uma VLAN deve aparentar ser uma rede totalmente independente e fisicamente separada.
Há várias formas de criar redes locais virtuais. Numa mesma rede física podem etiquetar-se as tramas fazendo com que cada etiqueta (TAG) corresponda a uma rede virtual diferente. A norma IEEE802.1Q define como colocar estas etiquetas nas tramas *Ethernet II*, para o efeito usa o valor 0x8100 no campo E-TYPE e o valor original do campo E-TYPE desloca-se 4 octetos.

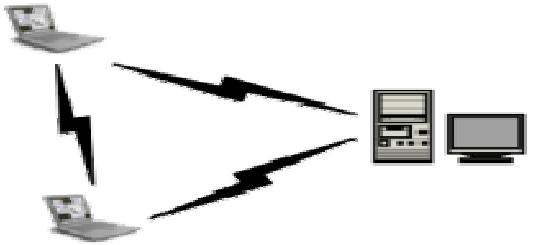


Redes Locais Virtuais - comutadores

Os comutadores podem definir VLANs sem recurso a etiquetas (*untagged*), por exemplo podem criar-se VLANs correspondentes a subconjuntos de portas do comutador. Transforma-se o comutador em vários comutadores virtuais, mas para suportar mais do que uma VLAN na mesma porta é necessário usar etiquetes, apenas uma VLAN pode ser *untagged* em cada porta. Além de VLAN baseadas em portas alguns comutadores também suportam VLAN baseadas em endereços MAC.



Redes locais sem fios (WLAN)



As redes locais sem fios representam uma evolução muito importante no sentido da acessibilidade e mobilidade por um lado e, simplificação das instalações por outro lado. As normalizações mais importantes são o IEEE 802.11 e respetivos aditamentos.

Nas primeiras versões as taxas de transmissão encontravam-se muito longe das praticadas nas redes de cabo (802.11 – 2 Mbps), atualmente já está disponível a norma 802.11n capaz de funcionar até 600 Mbps, usando múltiplos canais simultâneos (vários emissores/recetores).

Mais penalizador do que a taxa de transmissão é o facto de haver um retorno aos primórdios das redes locais com o meio de transmissão partilhado e um mecanismo de controlo de acesso ao meio do tipo CSMA.

O meio de transmissão sem fios partilhado torna impossível o controlo de acesso físico de utilizadores. Coloca ainda mais problemas de segurança do que as redes de meio partilhado de cabo.

802.11 - modulação

Embora a norma 802.11 original tivesse prevista uma implementação alternativa baseada em luz infravermelha, todas as evoluções posteriores usam exclusivamente rádio frequência na banda 2,4 GHz ou 5,7 GHz (micro-ondas).

Tratando-se de sinais analógicos por natureza, a transmissão de dados recorre a técnicas de modulação. As técnicas de modulação usadas atualmente são bastante complexas, usando vários sinais em simultâneo com combinações múltiplas PSK e ASK. Foram desenvolvidas na fase final da evolução dos modems de linha telefónica, para as linhas DSL e para as redes de telemóvel.

A norma 802.11 e respetivos aditamentos definem várias técnicas alternativas de modulação, que conduzem a várias taxas de transmissão. Cabe aos nós tentar as várias técnica para obter a melhor taxa possível. Geralmente as opções de menor taxa são mais fiáveis com sinal de baixa intensidade.

A gama de frequências usadas (micro-ondas) e as restrições quanto à potência de emissão (100 mW) produzem alcances muito reduzidos, especialmente no interior de edifícios onde é normalmente inferior a 50 metros.

802.11 – CSMA/CA

O maior problema das redes locais sem fios é o facto de usarem um meio de transmissão partilhado que só pode ser usado por um nó de cada vez.

>> Mesmo que o mecanismo de controlo de acesso ao meio (MAC) seja 100% eficaz, sob tráfego elevado a taxa nominal é dividida pelo número de nós.
>> As transmissões são *half-duplex*, um nó não pode emitir e receber ao mesmo tempo.

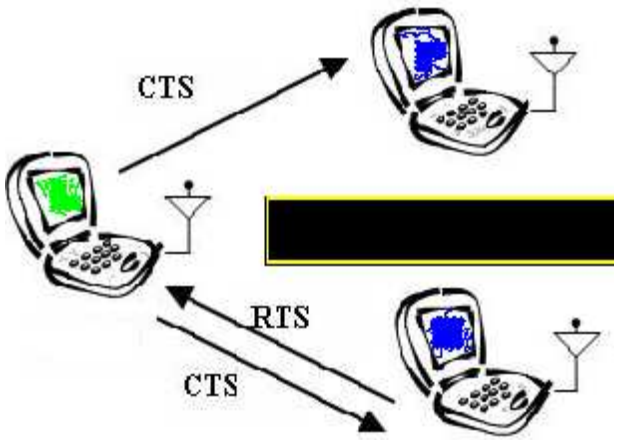
A receção de sinal em simultâneo com a emissão não é possível devido ao elevado custo, por isso o protocolo CSMA/CD não pode ser usado (não é possível detetar as colisões).

Em alternativa usa-se o CSMA/CA (*Collision Avoidance*), que tenta evitar colisões obrigando os nós a esperar que o meio esteja livre durante um dado período de tempo antes de poderem emitir.
Esta técnica não elimina as colisões, quando elas ocorrem, esse facto tem de ser detetado pelo emissor, para esse efeito sempre que um nó recebe uma trama válida envia ao emissor uma trama ACK.

IEEE 802.11 RTS/CTS

A técnica CSMA/CA pode ser combinada com RTS/CTS, esta técnica só é usada para o envio de pacotes com tamanho superior ao parâmetro *RTSThreshold* definido em cada nó.

A técnica RTS/CTS consiste no envio pelo emissor de uma trama *Request to Send* ao recetor, eventualmente o recetor responde com *Clear to Send* que indica que está pronto a receber.



Os outros nós quando recebem um RTS ou um CTS ficam impossibilitados de emitir durante algum tempo.

A técnica RTS/CTS é especialmente eficaz no modo infraestrutura em que existe um dispositivo central, o AP (*Access Point*) pelo qual todas as comunicações passam. Numa WLAN sem AP todos os nós podem receber pacotes para retransmitir a outros nós. Este modo de funcionamento, sem AP, é conhecido por *ad-hoc*.

802.11 – modo infraestrutura

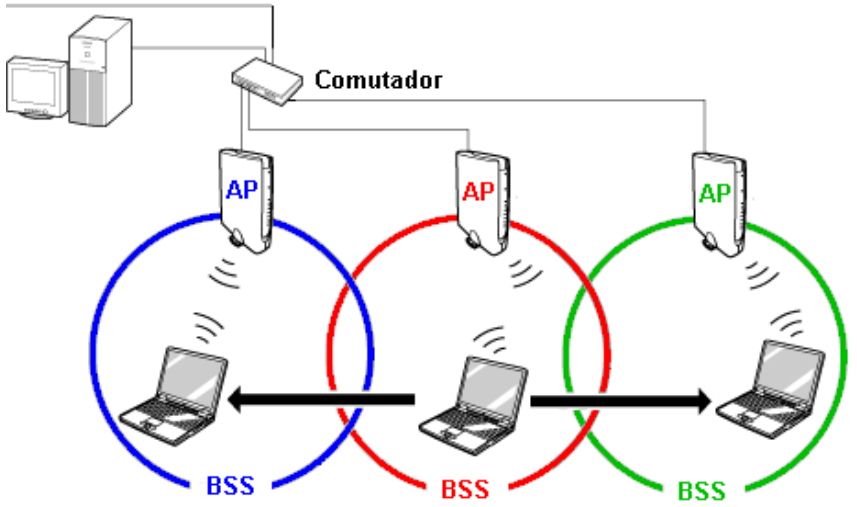
O modo de infraestrutura envolve a existência de um dispositivo central pelo qual todas as comunicações passam, pode-se considerar que se trata de uma topologia em estrela, embora sem fios.

O modo de infraestrutura tem grandes vantagens, uma delas é que a técnica RTS/CTS passa a ser muito eficaz porque apenas o AP pode responder aos RTS enviando o CTS.

802.11 – células

No modo de infraestrutura a rede é dividida em zonas de cobertura designadas de BBS (*Basic Service Set*) e também conhecidas por células. Cada célula é controlada por uma *base station*, também conhecida por AP (*Access Point*). Cada célula tem um identificador único (BBSID).

Um conjunto de células, pode fazer parte de uma mesma infraestrutura conhecida por ESS (*Extended Service Set*), o ESS é identificado por um nome com até 32 caracteres designado de SSID, todas as células de um ESS usam o mesmo SSID (*Service Set Identifier*) .



Nestas condições os nós de rede sem fios podem circular livremente entre os BSS do mesmo ESS sem perderem acesso à rede. A passagem transparente de célula em célula é conhecida por *roaming*.

802.11 - segmentação

A divisão de uma zona de cobertura em células reduz os efeitos negativos do meio de transmissão partilhado ao reduzir essa partilha a apenas uma célula. Aumentando o número de células (APs) garante-se que cada célula vai conter um menor número de nós, atenuando os efeitos negativos da partilha do meio de transmissão.

O número de células deve ser o necessário para garantir a cobertura total da área pretendida, mas além disso deve garantir também que o número de nós em cada célula não é muito elevado.

Não é disparate numa sala de 20 m^2 ter instalados dois ou até mais APs, tudo depende do número de postos de trabalho e da eficiência pretendida. Com APs instalados próximos uns dos outros é necessário ter a preocupação de usar canais afastados para evitar sobreposições.
A interligação de APs via ligação sem fios (*wireless distribution system*) é possível, mas deve ser evitada pois não proporciona o isolamento de meios partilhados como é desejável.

802.11 – tramas

O funcionamento das redes 802.11 é bastante complexo, envolvendo nós de diferentes funções e diversa informação de controlo específica, por isso o formato de trama é também bastante complexo, por exemplo as tramas 802.11 contêm 4 endereços MAC.

Apesar destas complexidades internas a ligação direta a redes locais com fios (Ethernet) é simples pois o formato de endereços é igual e os dados e campos de controlo podem ser transportados diretamente entre tramas 802.11 e tramas 802.3. Esta é uma missão do AP.

Na realidade foi realizado um grande esforço para manter a compatibilidade direta com as tramas 802.3. Por vezes (elevada taxa de erros) é conveniente usar tramas 802.11 muito pequenas, mas as tramas 803.3 podem chegar aos 1518 octetos. Para resolver o problema os nós 802.11 são capazes de fragmentar uma trama em segmentos e reagrupar esses segmentos.

802.11 – segurança

Tratando-se de uma rede com meio de transmissão partilhado a segurança é desde logo muito precária, uma vez que o meio está livremente acessível (dentro de determinada área) os problemas são ainda maiores.

Controlo de acesso

Os APs implementam diversas forma de controlo de acesso como parte do processo de entrada de um nó na célula. A autenticação pelo endereço MAC do nó não é segura, alternativas mais sólidas são a autenticação de utilizador ou a utilização de uma chave pré-partilhada (PSK).

Confidencialidade

Para garantir a confidencialidade é obrigatório recorrer à criptografia que é suportada pelo AP. Para esse efeito é necessário que o AP e o nó possuam uma mesma chave secreta. Esta pode ser pré-partilhada e nessa caso funciona também como autenticação ou pode ser gerada durante o processo de autenticação do utilizador. Uma outra alternativa consiste na utilização de criptografia de chave pública.