→ Redes de Computadores: Capítulo 1

RC

- A internet é composta por bilhões de dispositivos conectados (hosts = en
- Network é um conjunto de dispositivos, routers, links geridos por

- A internet possui infraestruturas que providenciam serviços para a
de programação para distribuir aplicações.
  - "Hooks" permitem que aplicações se liguem e utilizem o serviço de transporte da internet para envio/receção de dados
  - Protocolos definem o formato, ordem de mensagens enviadas e recebidas entre entidades de network assim como as ações a tomar em transmissão de mensagens e recibos

- O network edge tem hosts (clientes e servers) que enviam pacotes de dados
  - O host recebe a mensagem da aplicação e divide-a em fragmentos mais pequenos, pacotes, com comprimento de L bits
  - Transmite o pacote à taxa de transmissão R, também conhecida como taxa de transmissão do enlace, capacidade do enlace ou largura de banda do enlace

$$\text{packet transmission delay} = \frac{\text{time needed to transmit L-bit packet into Link}}{} = \frac{L \text{ bits}}{R \text{ (bits/sec)}}$$

- O internet core é uma rede de routers interligados
- Packet-switching (comutação de pacotes) os hosts divid
em pacotes. O network encaminha esses pacotes de em
origem dos pacotes até ao seu destino.

- Packet transmission delay demora L/R segundos a
- Store and forward: o pacote deve estar completo, isto é, d
antes de poder ser transmitido
- Queueing ocorre quando os pacotes chegam mais depressa do que conseguem ser enviados
  - Se o rate de chegada (bps) exceder o rate de transmissão, pacotes vão ficar em queue à espera de ser transmitidos. Os pacotes podem ser perdidos (dropped) se a memória (buffer) encher

- Forwarding (aka switching) - ação local move pacotes que estão a chegar do router's input link para um output link apropriado

- Routing - ação global determina o caminho da origem ao destino que os pacotes devem seguir

• Circuit Switching: recursos fim-a-fim são alocados para a "chamada" entre a origem e o destino. Estes recursos são dedicados, ou seja, não há partilha para garantir o desempenho. Um segmento fica livre se não for usado.

  • FDM

  • TDM

• Packet loss: os pacotes formam uma queue nos buffers à espera de serem transmitidos. O comprimento de fila aumenta quando a taxa de ~~entrada~~ chegada ao enlace excede a capacidade de enlace à saída. Ocorre perda de pacotes quando a memória para armazenar os pacotes esgota. Um pacote que chega a uma fila cheia é descartado (lost). O pacote perdido pode ser transmitido pelo nó anterior, pelo sistema terminal de origem ou, ~~em~~ não ser transmitido.

• Throughput (largura de banda útil): taxa (em bits por unidade de tempo) à qual os bits estão a ser enviados de um emissor até um recetor.

  • Rserver < Rclient => throughput = Rserver.

  • Rserver > Rcliente => throughput = Rclient

  • O throughput é limitado pela parte mais lenta. A rede até pode transportar mais, mas é aquele que estiver mais lento decide a quanto é que os bits são enviados

  • No segundo caso (Rs > Rc) ~~podemos~~ temos um bottleneck link. Mesmo que inicialmente o remetente tente enviar a Rs, a rede só consegue entregar os dados a Rc. O resto é descartado ou fica em queue.

• Traceroute: fornece uma medida de atraso desde a origem até cada router ao longo do caminho fim a fim da internet até ao seu destino

• Do
datagra

• Fragmen

→ Redes de Computadores: Capítulo 4

- O transporte de segmentos de um host de envio para um host receção
  - Sender encapsula os segmentos em datagramas e passa-os à link layer
  - Receiver entrega os segmentos à transport layer protocol
- Os router examinam o cabeçalho de todos os datagramas IP que o atravessam e movem os datagramas do input porto para output porto para transferir os datagramas ao longo do caminho fim-a-fim

- Forwarding: mover pacotes do input link do router para o output link apropriado
- Routing: determina o caminho que deve ser seguido pelos pacotes de uma determinado origem até um determinado destino

- Data plane: função local, por router. Determi... router input port é encaminhado (forwarded) para...
- Control Plane: determina como um datagrama é rot... desde a origem até ao destino. Duas abordagens ... implementados nos routers: software defined network

- O modelo best-effort não oferece garantias em ... ou ordem de entrega; banda larga disponível para o fluxo fornece fim
  - É um mecanismo bastante simples; a provisão adequada de largura de banda permite que aplicações em tempo real tenham um desempenho "suficientemente bom" na maioria dos vezes; serviços distribuídos na application-layer permite fornecer serviços a partir de múltiplas localizações; o controlo do congestionamento de serviços "elásticos" ajuda a manter o desempenho

- Network-links têm um MTU (maximum transfer unit) - o maior tamanho possível de uma trama de link-level frame
- Datagramas IPs grandes são fragmentados dentro da rede, um datagrama pode tornar-se vários sempre que necessário, os seus fragmentos apenas são agrupados quando chegam ao destino.
  - Os campos do cabeçalho IP (identifier, flags, fragment offset) são usados para identificar e ordenar fragmentos relacionados

- O endereço IP é um identificador de 32-bit associado a cada host ou router interface

- Não é obrigatória a implementação de mecanismos de controlo de fluxo e de erros na troca de pacotes de dados
- A mesma tecnologia de ligação não é suficiente para permitir comunicação em redes físicas distintas - é necessário encaminhamento a nível 3 (IP)

- Parte do endereço identifica o network (ou subnet) e outra parte identifica o host único. Subnet part - dispositivos no mesmo subnet com bits de grande ordem comuns; Host-part - bits de baixa ordem que

- Endereço IP baseado em classes (Classful) é o esquema original baseado no RCF 791. Os primeiros bits identificam a classe dos endereços (hardcoded)

  - as classes têm capacidades de endereçamento diferentes

- Endereços IP sem classes (Classless) não consideram os bits iniciais para a identificação de classe, é usado uma máscara de rede de 32 bits para determinar o endereço de rede. Permite agregação o que aumenta a eficácia do routing (CIDR). A agregação reduz o tamanho das tabelas de routing ao agrupar conjuntos de endereços de rede adjacentes

- Subnet é uma interfaces de dispositivos que conseguem chegar uns aos outros sem passar por um router interveniente.
  - Permite uma melhor organização do espaço de endereçamento
  - Permite estabelecer níveis hierquicos para o routing
  - Reduz o espaço de endereçamento para interfaces de host, pois alguns dos endereços iniciais não podem ser usados com o mesmo fim
  - Requer uma gestão adicional do endereçamento

- No Dinamic Host Configuration Protocol (DHCP), o objetivo é o host obter dinamicamente um endereço IP do network server quando se junta à rede.
  - Pode renovar o endereço que está a utilizar
  - Permite a reutilização de endereços
  - Suporta utilizadores moveis que saem e entram na rede
- O host envia uma mensagem de DHCP discover em broadcast; o DHCP responde com uma DHCP offer; o host pede um endereço IP, DHCP request; o DHCP envia um endereço IP, DHCP ack (podemos saltar os dois primeiros passos se um cliente quiser usar (re-usar) um endereço IP antigo)
- O DHCP pode fornecer mais do que apenas o endereço IP atribuido: o endereço do router de primeiro salto (first hop) para o cliente; nome e endereço IP do server DNS; máscara de rede

- Routers e hosts mantêm uma tabela de IP forwarding que inclui:
  - 1ª coluna - IP network destino
  - 2ª coluna - O endereço IP da interface host do próximo salto
  - 3ª coluna - netmask
  - última coluna - Id de interface da interface local de link layer
  - outras colunas (dependem do SO e da implementação) - flags, volume de tráfego, métricas, etc
- O encaminhamento de pacotes para o próximo salto é decidido baseado no endereço IP de destino do pacote depois de ser aplicado a máscara correspondente.

- Considera o endereço IP a.b.c.d/n como X.Y (endereço de host)
  - A netmask n é usada para extrair o endereço do network (ou sub-net) X
  - Procura na tabela de encaminhamento a entrada que mais corresponde a X. Se X é local, entrega a X.Y caso contrário, usa X para determinar o próximo salto.
  - Se X não estiver na tabela, a rota de entrada (default ou 0.0.0.0) é usada uma vez que corresponde a todos os destinos possíveis.
- A rota de entrada default tem uma prioridade mais baixa que as outras entradas da tabela. Permite reduzir o tamanho da tabela de encaminhamento ao custo de menos controlo

- O Static Routing é baseado em routes definidos manualmente ou pré-definidos num ficheiro de configuração
  - Reduz o network tráfego já que nenhuma publicidade de routes acontece
  - Esquema simples que não é capaz de acomodar mudanças na topologia do network.
- O Dynamic routing, o router envia publicidade aos vizinhos
  - Aumenta o network tráfego devido aos anúncios periódicos ou link changes
  - Esquema flexível capaz de adaptar a mudanças na topologia do network ou falhas no router

- O processo de encaminhamento em redes IP permite que um pacote de dados se aproxime, da interface de destino, sendo que a decisão de encaminhamento é tomada em todos os equipamentos de rede por onde o pacote passa tendo em consideração o conjunto de endereços de rede ou sub-rede de destino

- NAT: todos os dispositivos da rede local partilham um endereço IPV4 do ponto de vista exterior
  - todos os datagramas que saiem da network local têm o mesmo endereço NAT IP de origem, mas diferentes números de portos de origem
  -
- Todos os dispositivos numa rede local têm um endereço IP "privado" de 32-bit que apenas pode ser usado na network
  - Só é preciso um endereço IP do provedor ISP para todos os dispositivos
  - Podemos mudar o endereço de host em network local sem notificar o mundo exterior
  - Podemos mudar de ISP sem mudar os endereços da network local
  - Dispositivos dentro da rede local não são diretamente endereçáveis ou visíveis para o mundo exterior

- Um NAT router deve:
  - datagramas de saída: substituir o endereço IP de origem pelo endereço NAT IP
  - lembrar-se de todos os pares de tradução (IP → NAT IP)
  - datagramas de entrada: substituir o NAT IP address nos campos de destino com o correspondente endereço IP guardado na tabela NAT.

——— // ———

- O protocolo IPv4 funciona como modelo "best effort" e orientado a pacotes. Cada fragmento tem o seu próprio cabeçalho IP e um campo "fragment offset" que indica a posição da carga útil no pacote original e um bit "more fragments" para indicar se ainda vem mais fragmentos. A reconstrução completa só é feita no destino, mas deve ser conduzida num router.

- O TCP é um protocolo de transporte da pilha TCP/IP que funciona na camada 4 (transporte) do OSI

- O protocolo ICMP opera no nível protocolo de rede ainda que as mensagens ICMP sejam encapsulados em pacotes IP

→ Redes de Computadores - Capítulo 6

- A link layer (camada de ligação) tem a responsabilidade de transferir o datagrama de um nó (host/router) para outro nó ficamente adjacente através de um link (canal de comunicação (com ou sem fios) (redes locais LANs)).

> • Os PDUs a este nível chamam-se tramas ou frames

- Um datagrama é transferido por protocolos de ligação diferente em diferentes ligações. Cada protocolo de ligação fornece diferentes serviços

- A implementação da link layer é obrigatória em todos os dispositivos (host) que pretendem ligar-se à rede. É implementado on-chip ou na network interface card (NIC). Este conecta-se aos sistemas bases do host. É uma combinação de hardware, software e firmware

- Quando dois infraestruturas comunicam, o lado emissor encapsula o datagrama numa trama (frame) e adiciona bits de verificação de erro, transferência fiável de dados, controlo de fluxo
O lado recetor verifica erros, transferência fiável, controlo de fluxos, extrai o datagrama e passa-o para a camada superior no lado recetor

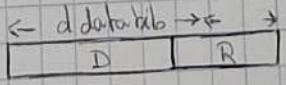
> • Este nível protocolar define mecanismos e funcionalidades em processos de comunicação direta entre interfaces por forma a serem suportados vários tipos de tecnologias e ligação físicos de interligação

- Os protocolos podem não detetar alguns erros (
e correção de erros
- O parity checking pode detetar e transmitir

- Internet checksum tenta detetar erros mas
do UDP segmento como uma sequência de 16 bit inteiros; o segmento é adicionado para obter o checksum e é colocado no campo de checksum do UDP. O receiver computa o checksum do segmento recebido e verifica se é igual → se for igual não há erros, senão for igual, há erros.

- Cyclic Redundacy check (CRC) - deteção de erros mais poderoso. O sender computa r CRC bits, R de forma a que <D,R> seja divisível por G. O receiver sabe G e se o resto der ≠0 → erro!

  - D: data bits
  - G: bit pattern of n+1 bits



$<D,R> = D * 2^r$ XOR R

- Multiple Acess Protocol
  - Canal de broadcast partilhado único
  - dois ou mais transmissões simultâneas por nodos podem causar interferência → ocorre uma colisão e um nó recebe dois ou mais sinais ao mesmo tempo
  - é utilizado um algoritmo distribuido para determinar como os nodos partilham o canal, i.e. determinar quando cada nodo pode transmitir
  - A comunicação sobre partilha de canal tem de usar o próprio canal, não existe nenhum canal out-of-band para coordenação

- os endereços MAC do layer 2 são de maior comprimento do que os endereços IPv4

- Os protocolos Mac têm três classes principais:
  - dividir o canal em partes mais pequ... luxo
  de um nodo: channel partitioning
  - acesso aleatório: o canal não é dividi... -se dos colisões
  - Taking turns: os nodos "tomam" turnos, ... os maiores

- TDMA (time division multiple acess) - o acesso aos canais é em "rondas", cada um recebe um slot de comprimento fixo, aqueles que não forem usados

- FDMA (frequency division multiple acess) - o espetro do canal é dividido em bandas de frequência, cada um com uma faixa de frequência fixa, tempo de transmissão não utilizado nos outros

- Unslotted ALOHA: mais simples, sem sincronização. Quando um nodo tem um quadro para enviar, transmite imediatamente; a probabilidade de colisão aumenta na ausência de sincronização (eficiência 18%)
- Slotted ALOHA: todos os frames têm o mesmo tamanho, o tempo é dividido em slots de tamanho igual os nodos começam apenas a transmitir no início de um slot, estão sincronizados, uma colisão é detetada por todos os nodos (eficiência 37%)
  - Quando um nodo obtem uma nova frame transmite-a no proximo slot
    - se não houver colisão o nodo pode enviar a frame no proximo slot
    - se houver colisão o nodo retransmite a frame em cada slot subsequente com a probabilidade p de sucesso.

• Vantagens: um único nó pode transmitir continuamente à taxa total do canal; altamente descentralizado (apenas os slots nos nodos é que precisam de estar sincronizados); simples

• Desvantagens: colisões desperdiçam slots (slots ociosos)

• CSMA simples: se o canal for detetado como ocioso transmite o quadro inteiro, se o canal for detetado como ocupado adia a transmissão; não se interrope os outros!

• CSMA/CD: as colisões são detetadas em pouco tempo, as transmissões em colisão são suspensas que reduz o desperdício do canal; a deteção de colisões é fácil em ligações com fio e difícil em ligações sem fio; o convencional educado

• Ainda podem ocorrer colisões no CSMA mesmo que este escute o meio. Atrasos de propagação significa que dois nodos podem não se ouvir ao começar a transmitir. Quando há colisões, o tempo de transmissão do pacote inteiro é desperdiçado. A distância e o atraso de propagação são importantes em determinar a probabilidade de colisão

• O CSMA/CD reduz a quantidade de tempo desperdiçado nas colisões porque a transmissão é abortada assim que a colisão é detetada.

• As metodologias de partilha do meio de transmissão com deteção de portadora (CSMA) são utilizados tanto em tecnologias de rede-com-fios como em tecnologias de Redes-sem-fios.

• Algoritmo Ethernet CSMA/CD

1. Ethernet recebe o datagrama da network layer (camada
2. Se a ethernet escuta o canal:
   - Vazio (Silencioso) começa a transmitir o fram
   - Ruidoso espera que fique silencioso e a
3. ~~Se detetar outra transmissão enquanto~~
3. Se transmitir a frame inteira sem colisões - feito!
4. Se detetar outra transmissão enquanto está a enviar: aborta e envia jam signal.
5. Depois de abortar, inicia binary (exponential) backoff:
   - Depois da m-ésima colisão, escolhe um K aleatório entre $\{0, 1, 2, \ldots 2^m - 1\}$

a ethernet espera K * 512 bit times e retorna ao passo 2.

- mais colisões → maior intervalo de backoff

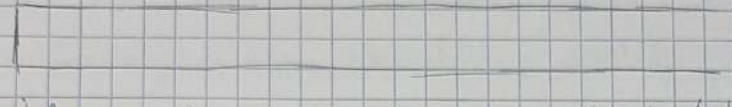
- Taking turns" MAC protocols
  - Partilham o canal de forma eficiente e justa sobre alta carga mas é ineficiente sob baixa carga; há atraso no canal, a largura de banda 1/N é alocada mesmo que tenha apenas 1 nó ativo
  - Os protocolos MAC de acesso aleatórios eficientes sobre baixa carga, um único nó pode utilizar o canal mas sob alta carga há sobre carga de colisões
- Polling - o controlador centralizador convida outros nós a transmitir por turnos. Preocupações: sobrecarga de polling, latência, ponto único de falha (bluetooth usa polling)
- Token passing: a mensagem de token de controlo é passada explicitamente de um nó para outro (sequencialmente). O nó só transmite enquanto detem o token. Preocupações: sobrecarga de token, latência e ponto único de falha

---

- MAC (ou LAN ou físico ou Ethernet) Adress é usado localmente para transferir uma trama (frame) de uma interface para outra interface à qual está fisicamente ligada. Tem 48bits (notação hexadecimal)
- Cada interface tem um endereço MAC único de 48bits. A atribuição dos endereços MAC é gerida pelo IEEE
É um endereço flat (portabilidade) pode mover-se de uma LAN para outra sem alterar o endereço

- ARP (Address Resolution Protocol) é um protocolo da camada de ligação (link layer) que serve para mapear um endereço IP (network layer) para um endereço MAC numa rede local (LAN)

- Ethernet
  - bus - todos os nodes no mesmo domínio de colisão (podem colidir entre si)
  - switched - um switch (da link layer) no centro, cada "fala" com um pacote (Ethernet frame) (nodes não colidem uns com os outros)
- A interface de envio encapsula o datagrama IP numa trama Ethernet



  - preambulo é usado para sincronizar o receiver, sender clock rates (7 bytes com o padrão 10101010 e seguidos de 1 com o padrão 10101011)
  - endereços. 6 bytes para o endereço MAC de origem, 6 bytes para o endereço MAC de destino
    - se o adaptador receber uma frame com endereço de destino a combinar ou com endereço de broadcast (e.g. ARP packet), passa a data em frame ao network layer protocol. Caso contrário, descarta o frame
  - type: indica protocolo da camada superior (principalmente IP) usado para demultiplex no receiver.
  - CRC - cyclic redundacy check at receiver, se for detetado um erro a frame é dropped.
- A Ethernet é ~~sem ligação~~ = fiável e ~~sem ligação~~ (connectionless)
  - connectionless: não é estabelecido ligação entre NICs de envio e de receção
  - unreliable: NICs de envio não enviam ACKs ou NAKs para o NIC de envio
    - data em dropped frames só é recuperada se o host inicial tiver um protocolo alto como TCP caso contrário é dropped e perdida.
  - Ethernet MAC protocol: unslotted CSMA/CD com binary backoff

- Ethernet switch
- O switch é um dispositivo link-layer atua de forma ativa na rede
  - Guarda e encaminha frames Ethernet
  - Examina endereços MAC recebidos, seletivamente encaminha os frame para um ou mais outgoing links a frame é para ser encaminhado em segmento utiliza CSMA/CD para aceder ao segmento
  - é transparente, o host não tem conhecimento dos switches
  - plug and play, self-learning (switches não precisam de ser configurados)
- Hosts têm uma ligação dedicada e direta ao switch
  - O switch armazena em buffer os frames.
  - O protocolo Ethernet usado em cada incoming link então não há colisões, full duplex e cada link tem o seu próprio domínio de colisão
  - Trocas de A para A' e de B para B' podem ser transmitidos simultaneamente sem colisões, mas A para A' e C para A' não pode acontecer simultaneamente
  - Cada switch tem a sua própria switch table, cada entrada tem:
    - MAC adress do host, interface to reach host, time stamp
- O switch aprende qual host pode ser alcançado a partir de determinados interfaces
  - Quando uma frame é recebida o switch aprende a localização de quem a enviou e guarda a informação numa switch table
- Quando uma frame é recebida por um switch:
  1. Regista o link de entrada e o MAC adress do host que enviou
  2. Procura na tabela o MAC adress do destino
  3. If } encontrou a entrada para o destino

     then }
     if } o destino está no mesmo segmento de onde a frame veio
     then drop frame
     else encaminha a frame para a entrada indicada na tabela
     } else flood /* encaminha o quadro para todos os interfaces exceto para aquela de onde veio */

- Switches vs routers
  - ambos são store and forward
    - routers: network layer device
    - switches: link layer devices
  - ambos têm forwarding tables
    - routers: computa a tabela com algoritmos de routing, IP addresses
    - switches: aprende a forwarding table com flooding e MAC adresses

- VLANs
  - VLANs - switches com suporte para VLAN podem ser configurados para definir multiplos LANs virtuais sobre uma única infraestrutura de VLAN física

- Um comutador (switch) interliga vários portos (links) numa topologia em estrela que emula o comportamento duma topologia clássica de barramento partilhado (bus)

Redes de Computadores: Capítulo 7

- **Base station**
  - tipicamente conectada a uma rede com fios
  - responsável por enviar pacotes entre network com fios e hosts sem fios na "área"

- **Wireless link**
  - tipicamente usado para conectar dispositivos móveis à base station e também como um backbone link
  - protocolo de acesso múltiplo coordena o link de acesso
  - vários transmission rates e distâncias e bandas de frequência

- **Infrastructure mode**
  - A base station conecta os dispositivos móveis à rede com fios
  - handoff: o dispositivo móvel muda de base station que fornece a conexão à rede com fios

- **Ad Hoc mode**
  - no base stations
  - nodes só podem transmitir para outros nodes dentro de cobertura da ligação
  - nodes organizam-se numa rede e roteiam entre si

- O sinal de rádio (wireless) perde potência à medida que se propaga

- **multipath propagation**: o sinal de rádio reflete-se em objetos como o chão, construções, chega ao destino a tempos ligeiramente diferentes.
  - **Coherence time**: quantidade de tempo que o bit está presente no canal para ser recebido.
    - Influência a ~~mais~~ transmission rate máxima já que coherence times não consegam overlap
    - Inversamente proporcional à frequência e à velocidade do recetor

- Interferência de outras fontes nas frequências da rede wireless como motores e outros aparelhos
- O SNR (signal-to-noise ratio) quanto maior mais fácil é extrair sinal do ruído
- SNR vs BER tradeoff: dada uma camada física aumentar a potência → aumenta o SNR → diminui o
-
- O SNR pode mudar com a mobilidade adaptado ~~fisicamente~~ dinamicamente à camada física

- 802.11 LAN Architecture
- Um wireless host comunica com uma base station (base station = access point (AP))
- Basic Service Set (BSS) (aka "cell") no infrastructure mode contém:
  - wireless host
  - access point (AP): base station
  - ad hoc mode: hosts only
- Extended Service Set (ESS) inclui uma ou mais BSS

- 802.11: channels
- Espetro é dividido em canais a diferentes frequências
  - Pode haver interferência se o canal escolhido for o mesmo

- 802.11: Association
- O host ao chega deve associar-se a um AP
  - Scans channels e ouve os beacon frames que contem APs chamado SSID e o seu Mac Address
  - Seleciona o AP com quem se associar e performa uma autenticação antes da associação

depois (tipicamente) corre DHCP para colocar o IP dentro da subnet do AP

- Passive scanning
  - Beacon frames enviados pelo AP → é enviado um association request frame do H1 para um AP selecionado → Association response frame enviado do AP para H1

- Active Scanning
  - Probe request frame broadcast transmitido pelo H1 → Probe Response frames enviados pelos APs → Association Request frame enviada do H1 para o AP selecionado → Association Response frame enviado do AP selecionado para o H1

- As frames Wi-fi podem conter até quatro campos de endereço mac

- 802.11: multiplexação
- É complicado detetar colisões no ar então escolhe-se evitar as colisões com o protocolo CSMA/CA (Collision Avoidance)
- 802.11 Sender
  - Se o canal estiver silencioso por o DIFS então transmite a frame completa (sem CD)
    - se não houver nenhum ACK após ela, aumenta o intervalo de Random backoff
    - caso contrário, transmissão bem sucedida
  - Se sentir o canal ocupado então começa um random backoff time
    - tempo decresce enquanto o canal estiver idle
    - quando o tempo acaba volta a sentir o canal
- 802.11 Receiver
  - Se a frame for recebida OK devolve o ACK depois do SIFS (ACK necessário devido ao problema do terminal escondido)

- O sender reserva o canal para data frames com pequenos pacotes de reserva
  - O sender envia um pequeno request-to-send (RTS) para a base station (bs) com CSMA (RTSs podem colidir uns com os outros mas eles são pequenos)
  - A base station (BS) broadcasta clear-to-send (CTS) em resposta ao RTS
  - CTS é ouvido por todos os nodos. O Sender transmite a data frame e os outros estações ~~dele~~ não transmitem

- Quando nas redes Wi-Fi (802.11) são usados frames RTC e CTR, o débito máximo de informação diminui substâncialmente ainda que diminuam eventuais colisões
- Se dois APs estiverem a operar canais diferentes então não interferem um com o outro mesmo que estejam ao alcance um do outro