96) Quais são os principais objetivos da camada de transporte?

- O objetivo primário da camada de transporte é propiciar o transporte de dados entre processos de usuários que rodam em sistemas interconectados;

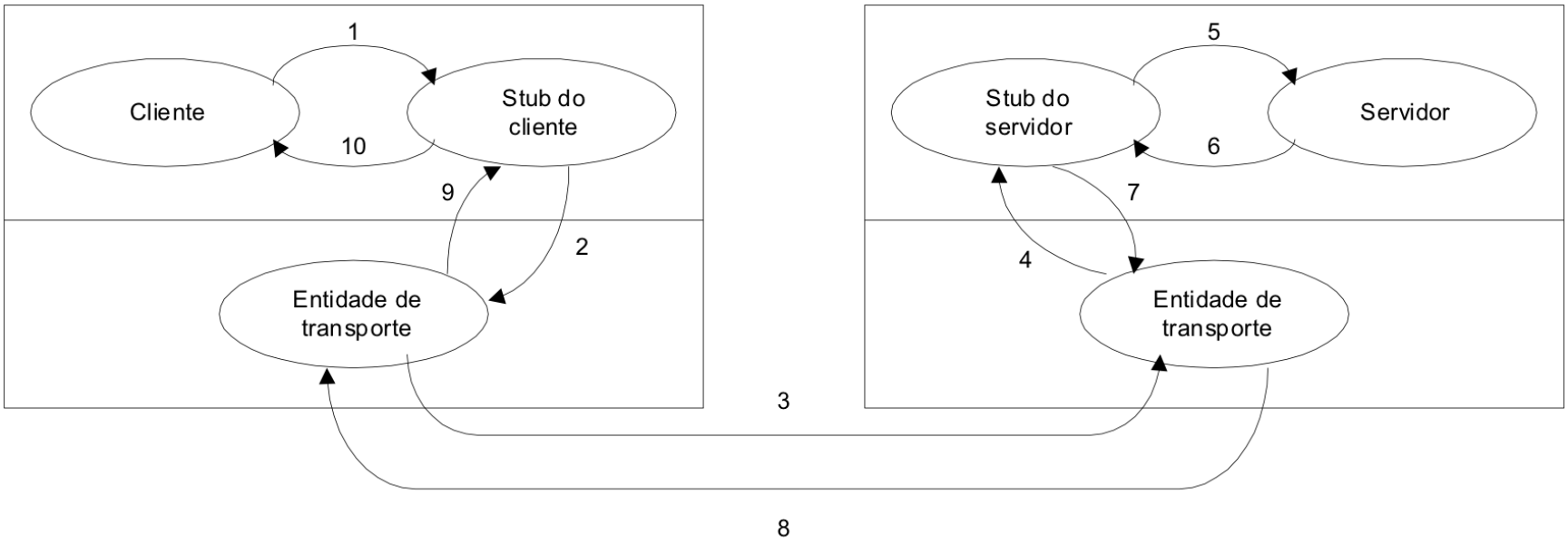
- O transporte de dados deve ser confiável e eficiente. Pois esta é a camada mais alta com esta responsabilidade, liberando as camadas superiores desta função; e

- A camada de transporte deve melhorar a qualidade dos serviços de rede, a fim de atender às necessidades e os requisitos da camada de sessão. Para isto, a camada de transporte deve ter funções de estabelecimento de conexão, endereçamento, seqüencialização, recuperação de erros e falhas, multiplexação, controle de fluxo, gerência de “buffer” e sincronização.

97) A) Quais as seqüências da invocação de primitivas para o estabelecimento “bem e mal sucedido” de uma conexão de transporte e para transferência de dados? Exemplifique através de desenhos, comentando sobre a ocorrência destas primitivas na interação das mesmas com a máquina do protocolo de transporte. B) Também mostre os desenhos, contendo os segmentos (pacotes), para estabelecer e terminar conexões (ligações) TCP, considerando a imagem do wireshark disponibilizada em aula.

98) Como você realizou o segundo trabalho prático? Considerando a experiência obtida na realização do segundo trabalho prático da disciplina apresente seus conhecimentos relacionados com a análise das camadas de aplicação, transporte e rede. Como ocorreu a interação da aplicação escolhida com a camada de transporte? Como ocorreu a interação da camada de transporte com a camada de rede? Comente sobre o conteúdo dos pacotes relacionados e identificados através do uso do Wireshark para o estabelecimento, transferênica de daos e “encerramento” das conexões.

99) Comente sobre as dez etapas necessárias para a execução de uma chamada a procedimento remoto conforme aparece na figura abaixo.



A etapa 1 consiste no programa (ou procedimento) do cliente que chama o procedimento stub encadeado no interior do seu próprio espaço de endereços. Então, o stub do cliente recolhe parâmetros e os condiciona em uma mensagem. Essa operação é conhecida como coleta de parâmetros. Depois de construída a mensagem é entregue à camada de transporte para transmissão (etapa 2). Em um sistema de LAN sem conexões, a entidade de transporte provavelmente irá apenas anexar um cabeçalho a mensagem e colocá-la na rede sem trabalho adicional (etapa 3). Quando a mensagem chega ao servidor, a entidade de transporte desse lado a entrega ao stub do servidor (etapa 4), que desagrupa os parâmetros coletados. O stub do servidor chama então o procedimento do servidor (etapa 5), passando dos parâmetros na forma padrão. Depois de completar seu trabalho, o procedimento do servidor retorna (etapa 6), da mesma maneira que qualquer outro procedimento retorna quando se encerra. Ele também pode devolver um resultado a seu chamador. Então, o stub do servidor coleta o resultado em uma mensagem e a entrega à interface de transporte (etapa 7), possivelmente fazendo uma chamada ao sistema, exatamente como na etapa 2. Depois que a resposta retorna à máquina cliente (etapa 8), ela é entregue ao stub do cliente (etapa 9). Finalmente, o stub do cliente retorna ao seu chamador, o procedimento do cliente. Qualquer valor retornado pelo servidor na etapa 6 é entregue ao cliente na etapa 10.

100) Quais as vantagens e desvantagens encontradas quando se implementa apenas a unidade funcional Kernel da camada de sessão?

A unidade funcional denominada KERNEL suporta os serviços básicos de sessão, exigidos para estabelecer uma conexão de sessão, transferir dados normais e liberar a conexão de sessão. O kernel constitui a unidade funcional mínima que deve ser implementada para que um sistema OSI possa interagir com outros OSI. A unidade kernel ajuda na verificação e validação da pilha de protocolos, permitindo realizar implementações e testes mais simples que podem ir sendo aperfeiçoados conforme necessário.

101) Quais são os serviços, SPDUs e códigos dos SPDUs da unidade funcional kernel ?

Unidade Funcional	Serviços	Cód.	SPDU
Kernel	Session Connection	CN	CONNECT
	Normal Data Transfer	AC	ACCEPT
	Ordery Release	RF	REFUSE
	U-Abort	FN	FINISH
	P-Abort	DN	DISCONNECT
		AB	ABORT
		AA	ABORT ACCEPT
		DT	DATA TRANSFER

102) Apresente o diagrama da Máquina de Estados Finita da camada de sessão a partir da comunicação entre entidades pares de sessão apresentadas na apostila (na página 197) para o sistema A e sistema B? E identifique os nomes das primitivas e UDPS envolvidos no estabelecimento e liberação de conexão e transferência de dados.

	Entidade A	**Entidade B**
Conexão	**STA1**	**STA1**
	SCONreq ↓	CN ←
	← CN	↑ SCONind
	STA2A	**STA8**
	AC ←	SCONrsp+ ↓
	↑ SCONcnf+	← AC
Transferência De Dados	**STA713**	**STA713**
	SDTreq ↓	DT ←
	← DT	↑ SDTind
	STA713	**STA713**
	DT ←	SDTreq ↓
	↑ SDTind	← DT
Desconexão	**STA713**	**STA713**
	SRELreq ↓	FN-nr ←
	← FN-nr	↑ SRELind
	STA3	**STA9**
	DN ←	SRELrsp+ ↓
	↑ SRELcnf+	← DN
	STA1	**STA1**

103) Quais são os principais objetivos e funções da camada de apresentação?

- A Camada de Apresentação relaciona-se com a sintaxe e a semântica das mensagens, conversão de códigos entre máquinas e outros serviços de conversão. A principal tarefa desta camada é codificar dados estruturados de acordo com o formato interno do transmissor à um formato adequado para transmissão dos mesmos e depois decodificá-los de acordo com o exigido no equipamento destino.

- São funções da Camada de Apresentação:

Sintaxe e semântica de mensagens;

Codificação de dados;

Compatibilização das estruturas de representação de dados;

Compressão de dados, e

Segurança computacional e de redes de computadores.

104) Comente sobre os serviços de segurança e compressão de dados relacionados com a camada de apresentação.

A segurança é um assunto abrangente e inclui inúmeros tipos de problemas. Em sua forma mais simples, preocupa-se em impedir que pessoas mal-intencionadas leiam ou pior ainda, modifiquem secretamente mensagens enviadas a outros destinatários. Outra preocupação da segurança são as pessoas que tentam ter acesso a serviços remotos que não estão autorizadas a usar. Ela também lida com meios para saber se uma mensagem supostamente verdadeira é um trote. A segurança trata de situações em que mensagens legítimas são capturadas e reproduzidas, além de lidar com pessoas que tentam negar o fato de ter enviado certas mensagens [Tanenbaum 2011 e 2021].

Os problemas de segurança de redes podem ser divididos nas seguintes áreas interligadas: sigilo, autenticação, não repúdio e controle de integridade. O sigilo – também chamado confidencialidade – *está relacionado ao fato de manter as informações longe de usuários não autorizados*. É isso que costuma nos vir à mente quando pensamos em segurança de Redes. Em geral a autenticação *cuida do processo de determinar com quem você está se comunicando antes de revelar informações sigilosas ou entrar em uma transação comercial*. O não repúdio trata de assinaturas: *como provar que seu cliente realmente fez um pedido eletrônico de dez milhões de unidades de um produto com preço unitário de 89 centavos quando mais trade ele afirmar que o preço era 69 centavos?* Ou talvez ele afirme que nunca efetuou nenhum pedido. Por fim, como você *pode se certificar de que uma mensagem recebida é de fato legítima e não algo que um oponente mal-intencionado modificou a caminho ou inventou?* [Tanenbaum 2011 e 2021].

Trabalhos da equipe do LRG (Laboratório de Redes e Gerência) na área de segurança relacionados com o professor da disciplina.

Links para obter trabalhos e transparênicas:

http://www.inf.ufsc.br/~westphal/publica.html

http://www.inf.ufsc.br/~westphal/other.htm

http://www.inf.ufsc.br/~westphal/slides.htm

http://www.inf.ufsc.br/~westphal/videos.htm

http://www.inf.ufsc.br/~carlos.westphall/rgc.htm

105) Apresente o desenho e descreva os 15 passos para implementar o controle de acesso e autorização, usando “shibboleth” em uma cloud federada.

(https://www.researchgate.net/publication/321807432_Security_in_the_Context_of_Internet_of_Things_Cloud_Fog_and_Edge).

106) Comente sobre como foi realizada a implementação na prática, do cenário proposto, para obter controle de acesso e autorização, usando “Shibboleth” em uma cloud federada.

(https://www.researchgate.net/publication/321807432_Security_in_the_Context_of_Internet_of_Things_Cloud_Fog_and_Edge).

107) A) O que é ASN1? B) Quais são as suas vantagens e como o ASN1 pode ser usado? C) Observe melhor e comente sobre o uso de ASN1 no RFC 1155.

Abstract Syntax Notation One (ASN.1) *é uma notação padrão e flexível que descreve as regras e estrututras para representar, codificar, transmitir e decodificar dados em redes de computadores e telecomunicações.* As regras formais permitem representar objetos que são independentes das técnicas específicas de codificação de uma máquina. O ASN.1 é um padrão da International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), e International Telecommunication Union Telecommunication Standardization Sector ITU-T. Os dados gerados em diferentes fontes de observação devem ser transmitidos a um ou mais locais para serem processados e gerar resultados úteis. O ASN.1 juntamente com regras específicas (ASN.1 encoding) facilita a troca de dados especialmente entre os programas aplicativos em redes, descrevendo estruturas de dados de uma forma que é independente da arquitetura da máquina e linguagem de implementação [Wikipedia, 2022].

Exemplos: Na apostila e no RFC 1155.

(http://www.inf.ufsc.br/~westphal/rfc1155-SMI-colored%20by%20Westphall.pdf)

108) Explique como o ASN.1 pode ser usado para resolver o problema de transferência de dados entre um computador com bit mais significativo a direita na memória e outro computador com bit mais significativo a esquerda?

A conversão da forma de representação dos dados pode ser feita de duas maneiras: cada receptor decodifica os dados recebidos ou o transmissor e o receptor codificam os dados para um formato de transmissão e os decodificariam para sua representação particular. A primeira solução é inconveniente pois o receptor deve ser capaz de identificar as diferenças entre ele e os demais transmissores com os quais comunica-se para ser capaz de adaptar os dados recebidos. Já para a segunda solução tem-se um algoritmo mais simples: o codificador e o decodificador poderiam se basear em uma estrutura padrão para transmissão e o formato de representação interna dos dados seria irrelevante. É esse um dos objetivos da notação ASN.1 (Abstract Sintax Notation One) quando usada na camada de apresentação.

109) A) Apresente uma visão geral sobre as aplicações da camada de aplicação? B) Responda as questões de números 34 e 41.

Aplicações são a razão de ser de uma rede de computadores. Se não fosse possível inventar aplicações úteis, não haveria necessidade de projetar protocolos de rede para suportá-las. Nos últimos 40 anos, foram criadas numerosas aplicações de redes engenhosas e maravilhosas. Entre elas estão as aplicações clássicas de texto, que se tornaram populares na década de 1970 e 1980: correio eletrônico, acesso a computadores remotos, transferência de arquivos, grupos de discussão e bate-papo e também uma aplicação que alcançou estrondoso sucesso em meados da década de 1990: a World Wide Web, abrangendo a navegação na Web, busca e o comércio eletrônico. Duas aplicações de enorme sucesso também surgiram no final do milênio – mensagem instantânea com lista de amigos e compartilhamento P2P de arquivos, assim como muitas aplicações de áudio e vídeo, incluindo a telefonia por internet, transmissão e compartilhamento de vídeo, rádio via internet e televisão sobre o protocolo IP (IPTV). Além disto, a penetração crescente de acesso residencial banda larga e a onipresença de acesso sem fio estão preparando o terreno para aplicações mais modernas e interessantes no futuro [Kurose 2014 e 2021].

110) Apresente os conceitos e definições relacionados com qualidade de serviço, serviços integrados (IntServ) e serviços diferenciados (DifServ). O que é SLA? Ver exemplo de SLA no relatório do trabalho prático de INE5619.

Qualidade de Serviço (QoS) é um problema de interworking que vem sendo mais discutido que definido. Podemos definir informalmente qualidade de serviço como algo que um fluxo procura alcançar. Tradicionalmente, são atribuídos quatro tipos de características a um fluxo: confiabiliadade, atraso, jitter e lagura de banda [Forouzan, 2013].

Confiabilidade é uma característica que um fluxo precisa. A falta de confiabilidade significa perder um pacote ou confirmação, que implica na retransmissão. Entretanto, a sensibilidade dos programas aplicativos à confiabilidade não é a mesma. Por exemplo, é mais importante para o correio eletrônico, transferência de arquivos e acesso à Internet terem transmissões confiáveis que aplicações de audioconferência e telefonia [Forouzan, 2013].

Atraso origem-destino é outra característica do fluxo. Repetindo, aplicações podem tolerar atraso em diversos níveis. Nesse caso, telefonia, audioconferência, videoconferência e login remoto precisam de atraso mínimo, ao passo que o atraso na transferência de arquivos ou de e-mail é menos importante [Forouzan, 2013].

Jitter é a variação no atraso entre pacotes pertencentes ao mesmo fluxo. Por exemplo, se quatro pacotes partirem nos instantes 0, 1, 2, 3 e chegarem aos instantes 20, 21, 22, 23, todos terão o mesmo atraso, 20 unidades de tempo. Por outro lado, se os pacotes chegarem aos instantes 21, 23, 21 e 28, eles terão atrasos diferentes: 21, 22, 19 e 24. Para aplicações de áudio e vídeo, o primeiro caso é completamente aceitável; o segundo caso, não [Forouzan, 2013].

Lagura de Banda – Aplicações diferentes requerem diferentes lagura de banda. Em videoconferência, precisamos transmitir milhões de bits por segundo para atualizar uma tela colorida, ao passo que o número total de bits em uma mensagem de e-mail talvez nem chegue à casa de um milhão [Forouzan, 2013].

Serviços Integrados – Entre 1995 e 1997, a IETF dedicou um grande esforço à criação de uma arquitetura para streaming de multimídia. Este trabalho resultou em mais de duas dezenas de RFCs, começando com as RFCs 2205 a 2212. O nome gernério deste trabalho é serviços integrados. Ele teve como objetivo as aplicações de unicast e multicast. Um exemplo do primeiro tipo de aplicação é um único usuário que recebe um streaming de vídeo transmitido por um site de notícias. Um exemplo do outro tipo de aplicação é um conjunto de estações de televisão digital que transmitem seus programas sob a forma de fluxos de pacotes IP para muitos receptores situados em diversos locais [Tanenbaum 2011 e 2021].

RSVP – Resource reSerVation Protocol – A parte principal da arquitetura de serviços integrados visível aos usuários da rede é o **RSVP**, descrito nas RFCs 2205-2210. Esse protocolo é empregado para fazer as reservas; outros protocolos são usados para transmitir os dados. O RSVP permite que vários transmissores enviem os dados para vários grupos de receptores, torna possível aos receptores individuais mudar livremente de canais e otimiza o uso da largura de banda ao mesmo tempo que elimina o congestionamento [Tanenbaum 2011 e 2021].

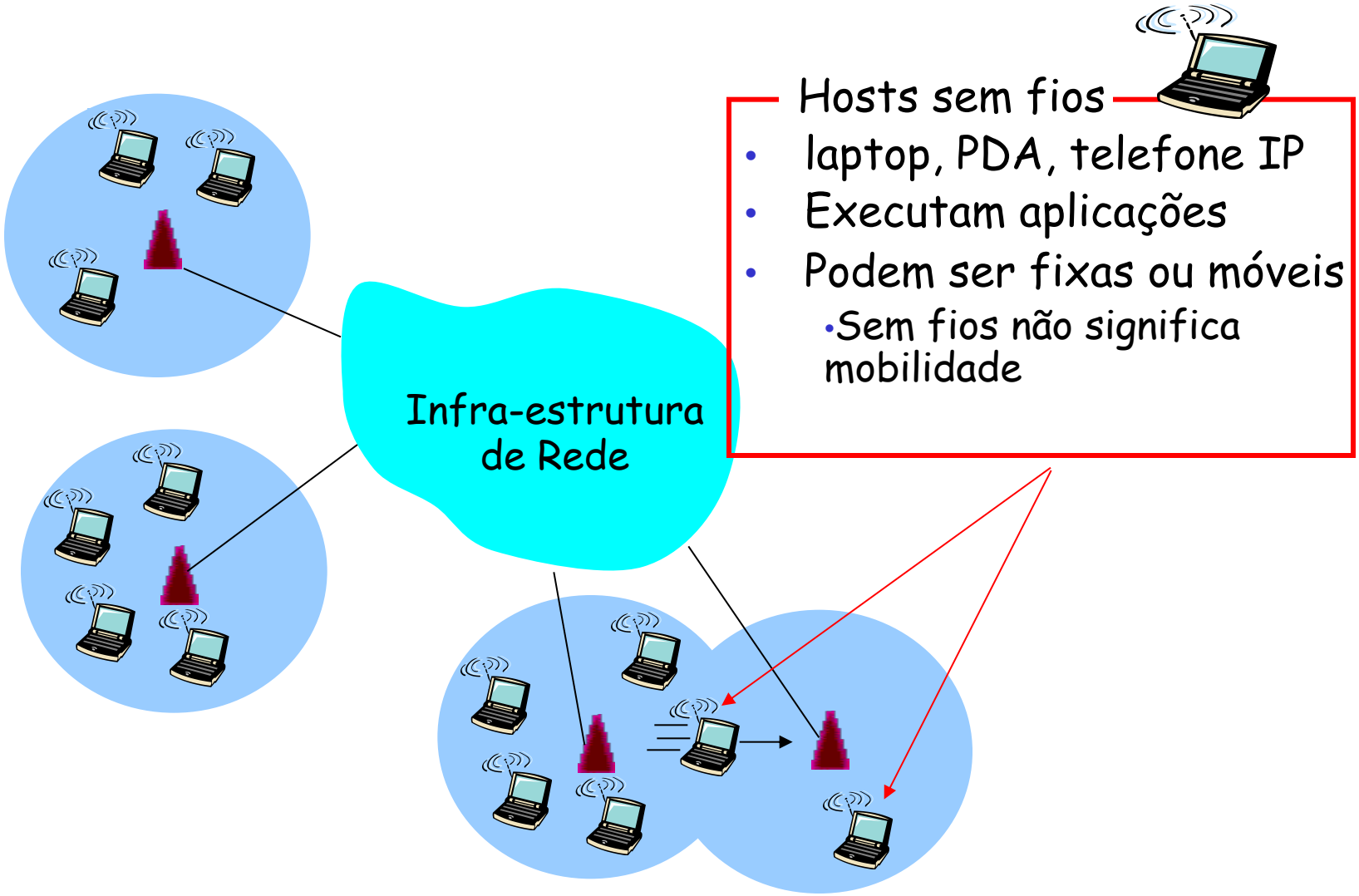
Serviços Diferenciados – A IETF também criou uma abordagem mais simples para oferecer qualidade de serviço, uma estratégia que pode ser implementada em grande parte no local em cada roteador, sem configuração antecipada e sem ter que envolver todo caminho. Essa aboradagem é conhecida como qualidade de serviço **baseada em classe** (em vez de baseada em fluxo). A IETF padronizou uma arquitetura para ela, chamada arquitetura de **serviços diferenciados**, descrita nas RFCs 2474, 2475 e várias outras [Tanenbaum 2011 e 2021].

Os Serviços Diferenciados (Differentiated Services – DS) podem ser oferecidos por um conjunto de rotedores que formam um domínio administrativo. A administração define um conjunto de classes de serviços com regras de encaminhamento correspondentes. Se um cliente fizer a assinatura para DS, seus pacotes que entrarem no domínio serão marcados com a classe a que pertencem. Essa informação é executada no campo *differentiated services* dos pacotes IPv4 e IPv6. As classes são definidas como **comportamento por hop**, pois correspondem ao tratamento que o pacote receberá em cada roteador, e não uma garantia pela rede [Tanenbaum 2011 e 2021].

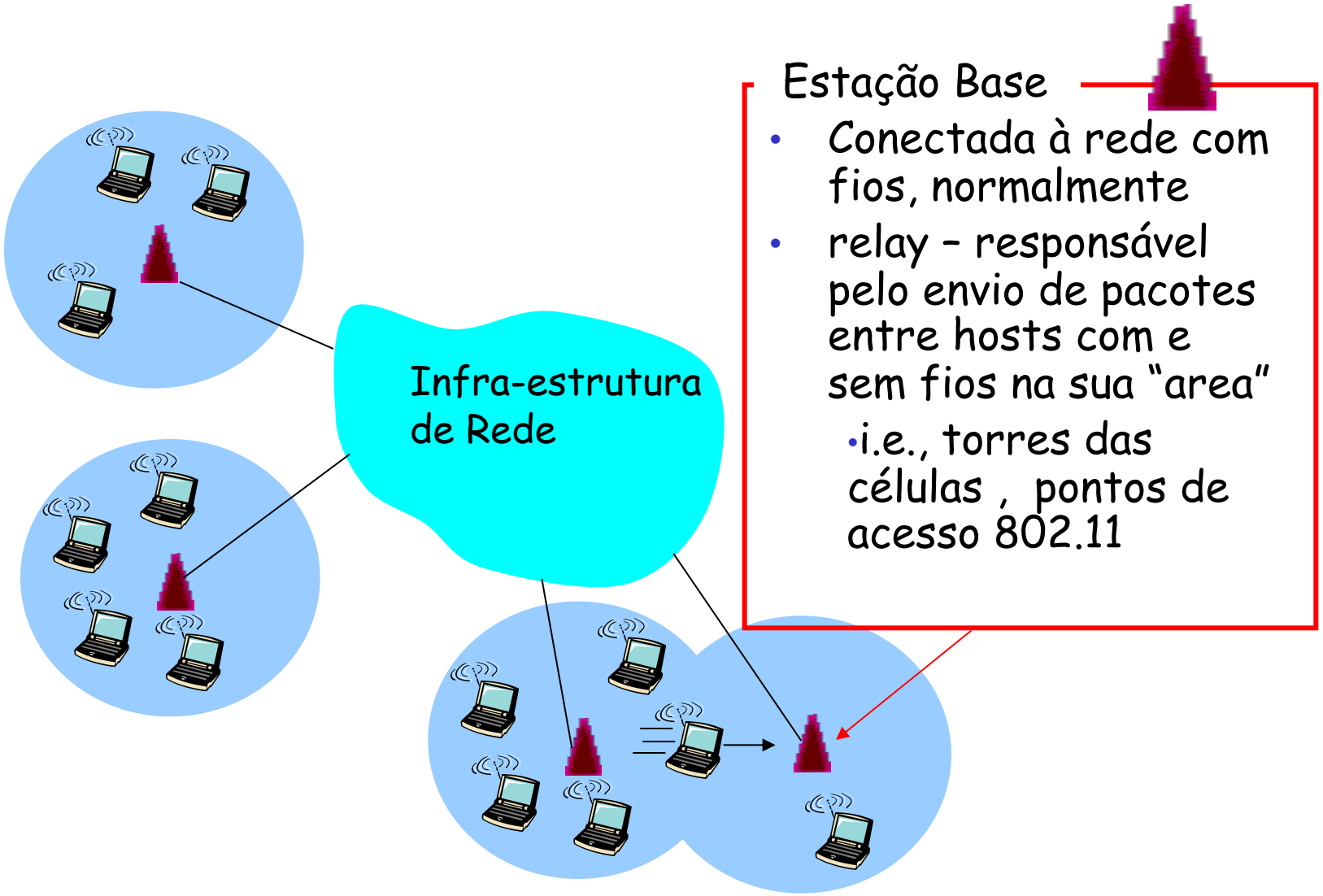
111) Considerando o protocolo IEEE 802.11: A) Explique como funcionam os tipos de redes infraestruturada e ad hoc; e
B) Descreva o funcionamento do CSMA/CA.

As redes 802.11 são compostas de clientes, como notebooks e telefones móveis, e infraestrutura chamada **pontos de acesso**, ou **APs** (**Access Points**), que são instalados nos prédios. Os pontos de acesso também são chamados de **estações-base**. Os pontos de acesso se conectam à rede com fios, e toda comunicação entre os clientes passa por um ponto de acesso. Também é possível que os clientes no alcance do rádio falem diretamente, como dois computadores em um escritório sem um ponto de acesso. Este arranjo é chamado de **rede ocasional** (ou **rede ad hoc**) [Tanenbaum 2011 e 2021].

Elementos de uma Rede Sem Fio



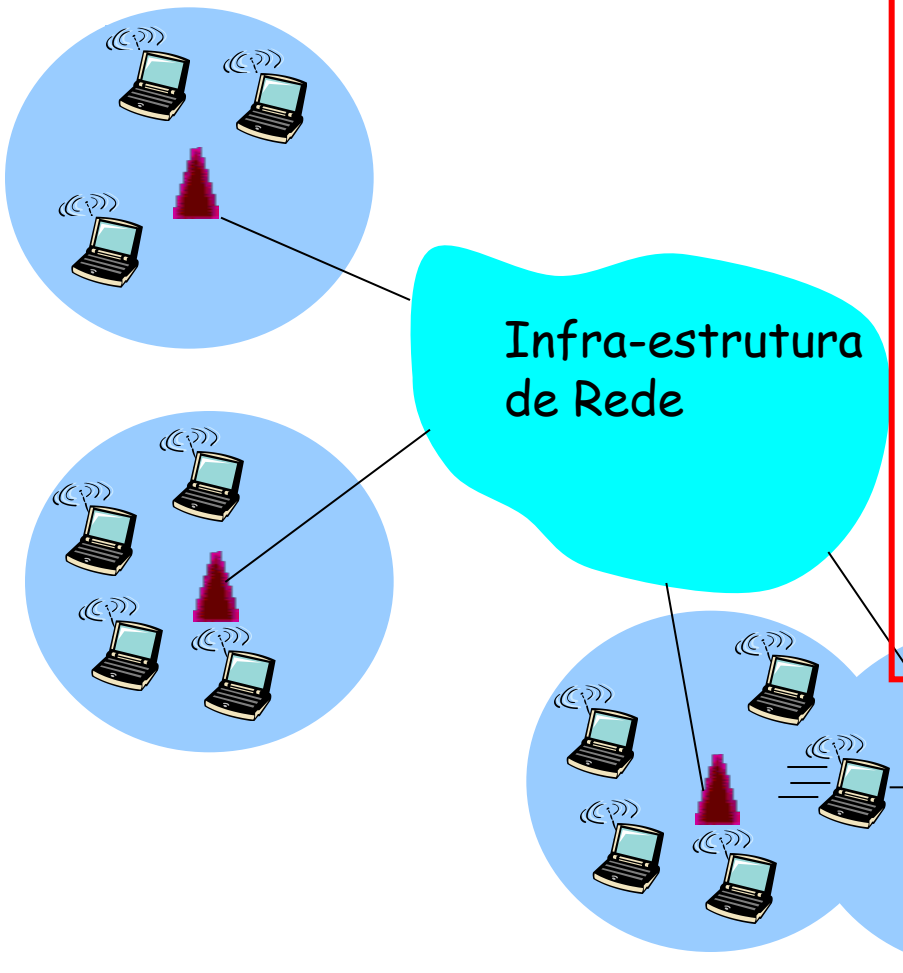
Elementos de uma Rede Sem Fio



Estação Base

- Conectada à rede com fios, normalmente
- relay – responsável pelo envio de pacotes entre hosts com e sem fios na sua "area"
  - i.e., torres das células , pontos de acesso 802.11

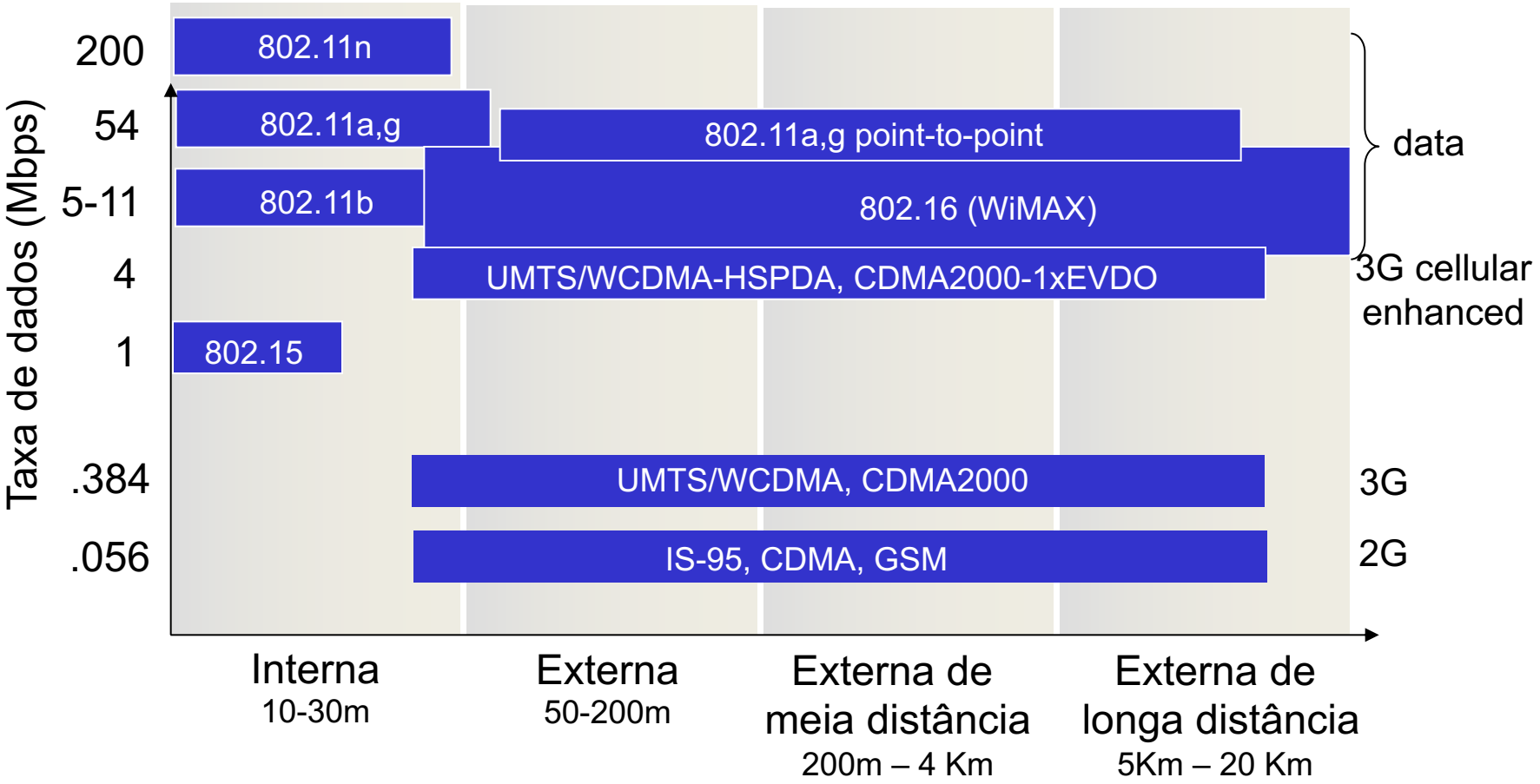
Elementos de uma Rede Sem Fio



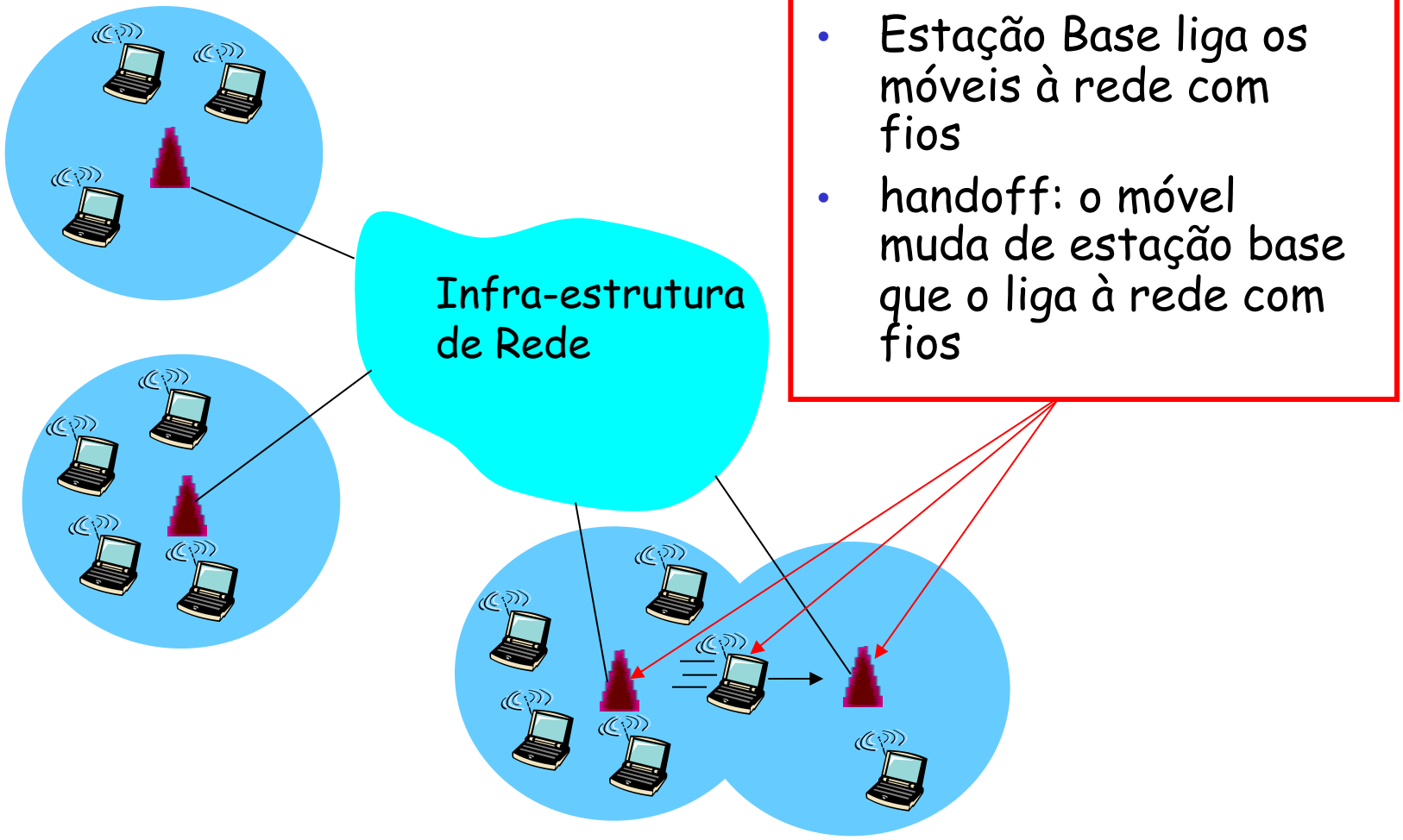
ligação sem fios

- Tipicamente usado para ligar as estações móveis à estação base
- Também usado como ligação de backbone
- Acesso ao link coordenado por protocolos múltiplos
- Variação nas taxas de dados e distância de transmissão

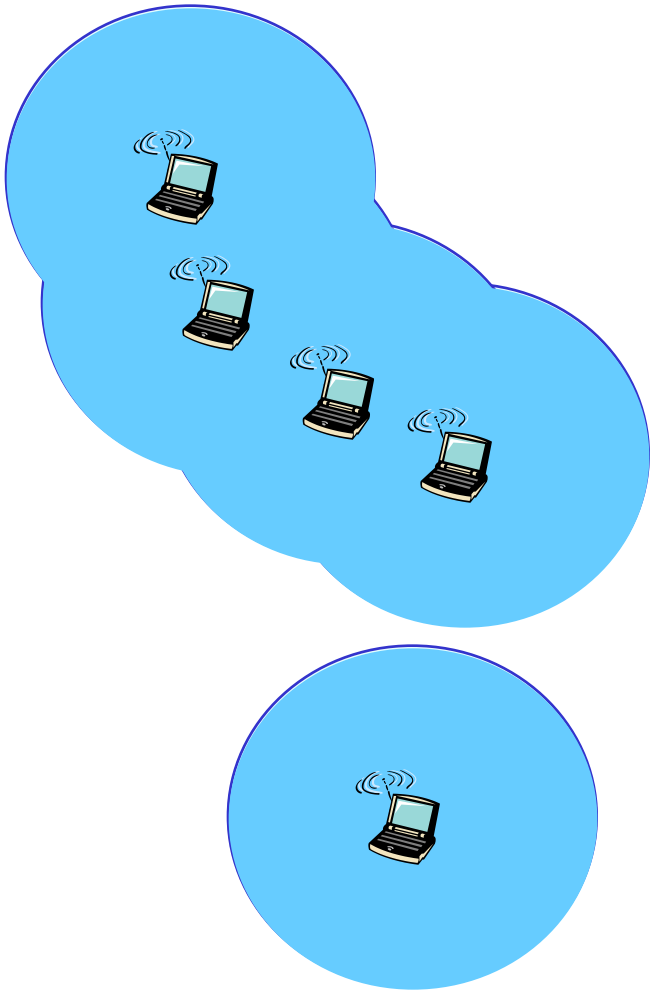
Características dos diferentes enlaces sem fio



Elementos de uma Rede Sem Fio



Elementos de uma Rede Sem Fio



Modo ad hoc

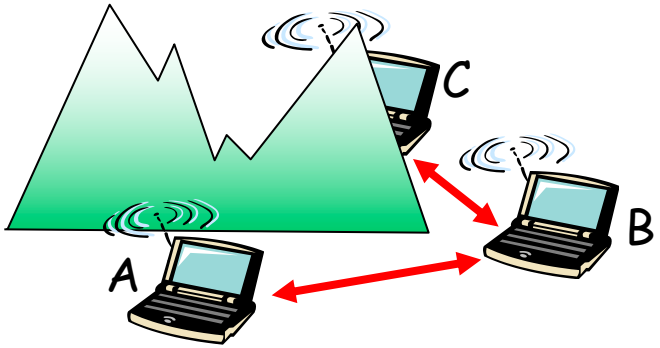
- Sem estações de base
- Os nós podem apenas transmitir para outros nós dentro da sua área de cobertura
- Os nós organizam-se em rede: encaminham através de si próprios

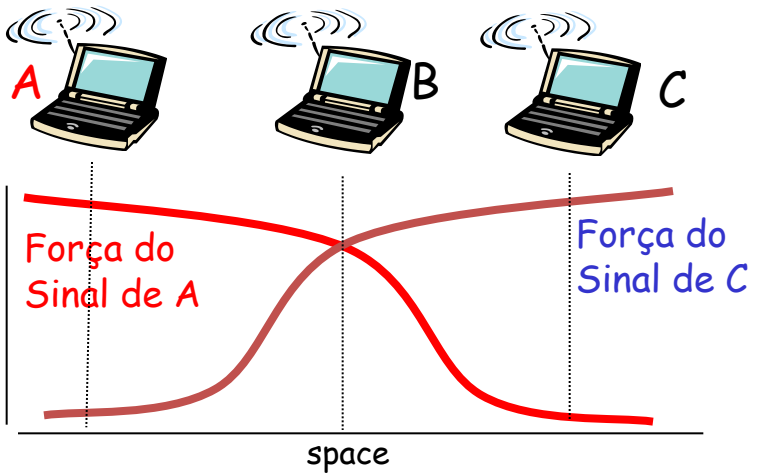
Taxonomia

	Salto único	Saltos múltiplos
Infra-estructura (i.e., APs)	host liga-se à estação de base (WiFi,WiMAX, celular) que se liga à Internet	O host pode ter que passar por vários nós relay sem fios para se ligar à Internet: *mesh net*
Sem Infra-estructura	Sem estação de base nem Ligação à Internet (Bluetooth, redes adhoc)	Sem estação de base, sem ligação à Internet. Pode ter que usar relays para atingir um dado nó sem fios na MANET, VANET

Características

- **Força decrescente do sinal**
- **Interferência com outras fontes: frequências partilhadas com outros dispositivos como telefones; interferência com motores**
- **Terminal escondido**
  - **B interfere entre A e C**
- **Atenuação do sinal**
  - B, A ouvem um ao outro
  - B, C ouvem um ao outro
  - A, C não se ouvem e interferem em B





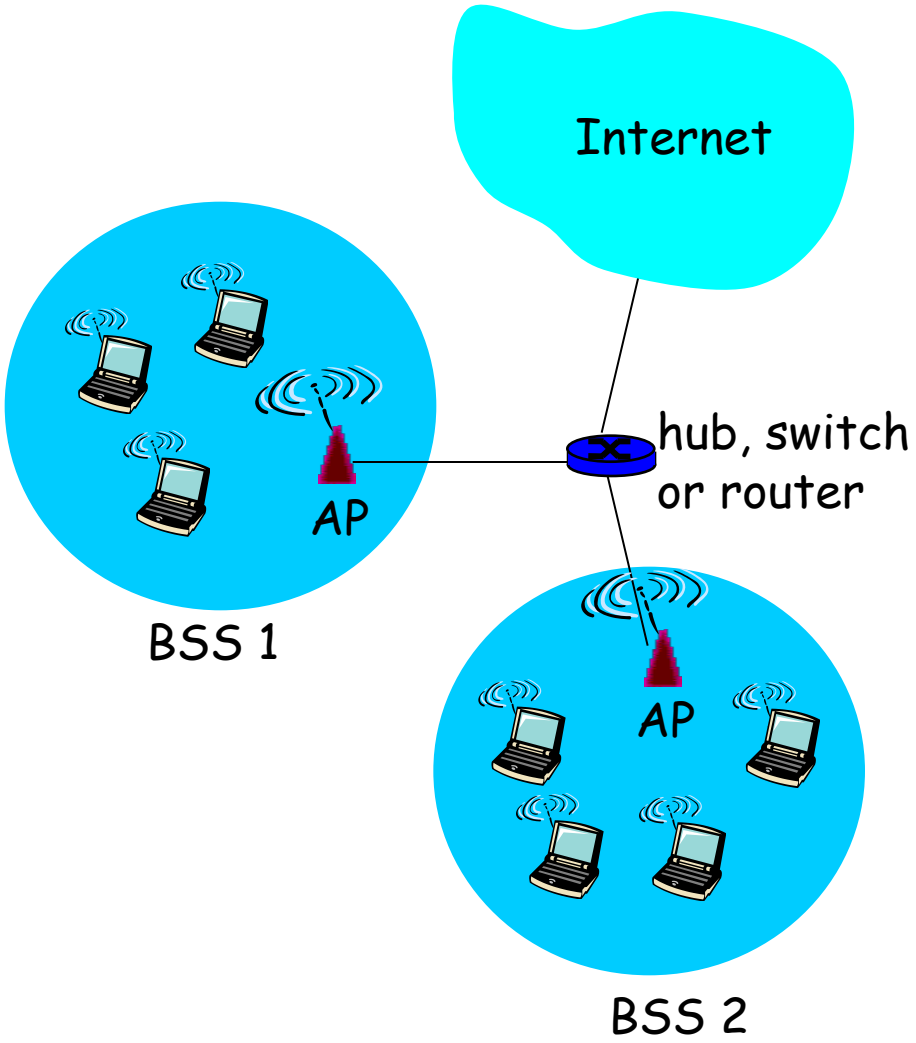
Redes Locais sem fios IEEE 802.11

- 802.11b (1999)
  - –2.4-5 GHz espectro sem licença
  - –Até 11 Mbps
  - –direct sequence spread spectrum (DSSS) na camada física
    - Todos os hosts usam o mesmo código de "chipping"
- 802.11ac (Dez 2013)
  - – 5 GHz
  - – Até 780 Mbps
- 802.11ad (Dez 2012)
  - – 60 GHz
  - – Até +- 7 Gbps

- 802.11a (1999)
  - –5-6 GHz
  - –Até 54 Mbps
- 802.11g (2003)
  - –2.4
  - –Até 54 Mbps
- 802.11n (2009): antenas múltiplas
  - –2.4-5 GHz
  - –Até 150 Mbps

- Todas usam CSMA/CA para acesso múltiplo
- Todas têm versões com estação base e para redes ad-hoc

Arquitetura da LAN 802.11



- Cada host sem fios se comunica com uma estação de base
  - Estação de Base = Ponto de Acesso (AP)
- Conjunto básico de serviço (BSS) ("célula") no modo infra-estrtutura contém:
  - Hosts sem fios
  - Pontos de Acesso (AP): Estações de Base

Arquitetura da LAN 802.11

BSS

- Cojunto básico de serviço (BSS) em modo Ad hoc contém:
  - Hosts sem fios

Transparências de números 26 a 36 (Direitos autorais de J. F Kurose e K. W. Ross).

802.11 Canais e Associações

- **802.11b: espectro 2.4GHz-2.485GHz dividido em 11 canais com diferentes frequências**
  - AP admin escolhe a frequência para o AP
  - Possível interferência: escolha do mesmo canal que um AP vizinho !

- **host: deve *associar-se* a um AP**
  - Varre os canais, ouvindo os quadros de orientação (*beacon frames)* contendo o nome do AP (SSID) e endereços MAC
  - Seleciona um AP para se associar
  - Pode autenticar-se (vários protocolos)
  - Tipicamente usa o DHCP para obter um endereço IP na subrede do AP

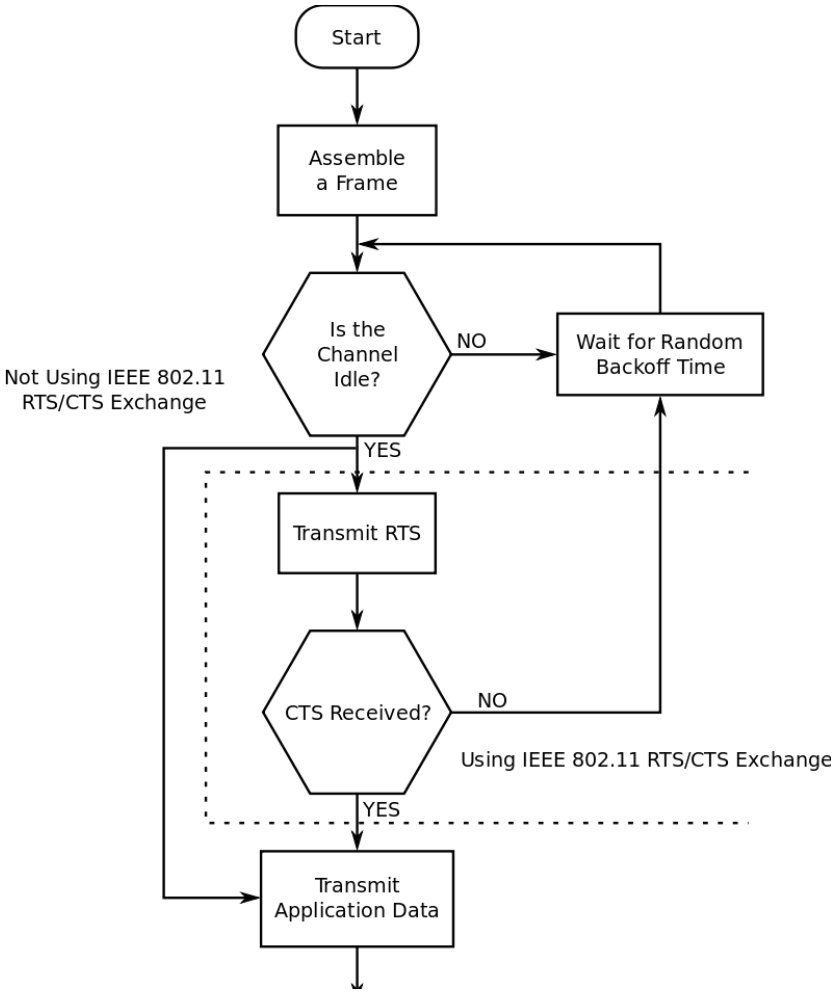
Carrier sense multiple access with collision avoidance (**CSMA/CA**)

é um método de transmissão que possui um grau de ordenação maior que o seu antecessor (CSMA/CD) e possui também mais parâmetros restritivos, o que contribui para a redução da ocorrência de colisões em uma rede (máquina interligadas através de uma rede identificam uma colisão quando o nível de sinal aumenta no interior do cabo). *Antes de transmitir efetivamente um pacote, a estação avisa sobre a transmissão e em quanto tempo a mesma irá realizar a tarefa. Dessa forma, as estações não tentarão transmitir, porque entendem que o canal está sendo usado por outra máquina [Wikipedia, 2022].*

Alguns detalhes do CSMA/CA

É uma forma eficaz de administrar e ordenar o tráfego de pacotes em rede de computadores tendo um impacto relevante no sentido de diminuir as colisões, entretanto é conveniente ressaltar que apenas transmitir a intenção de trafegar pacotes aumenta o fluxo, impactando, desta forma, no desempenho da rede. *Os dispositivos de uma rede (WLAN) devem sentir o meio para verificar a alimentação (estímulo de RF acima de um certo limite) e esperar até que o meio esteja livre antes de transmitir. O CSMA/CA Utiliza um recurso chamado "solicitar para enviar" / "livre para enviar" (RTS/CTS) [Wikipedia, 2022].*

Algoritmo simplificado do CSMA/CA [Wikipedia, 2020]



CSMA/CA

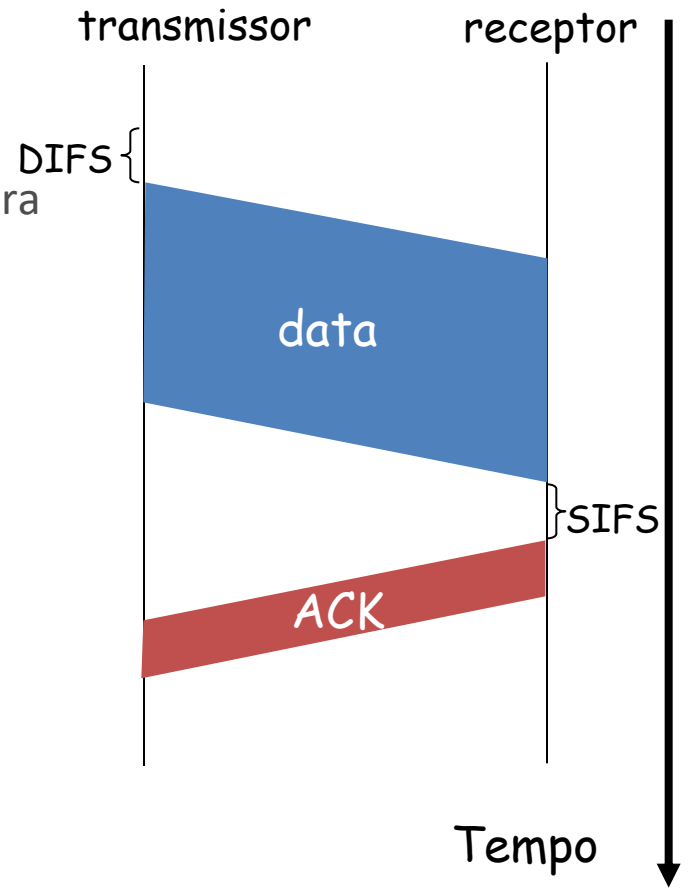
Transmissor 802.11

1 Se percebe o canal inativo durante o tempo DIFS então
Transmite o quadro completo (sem CD)

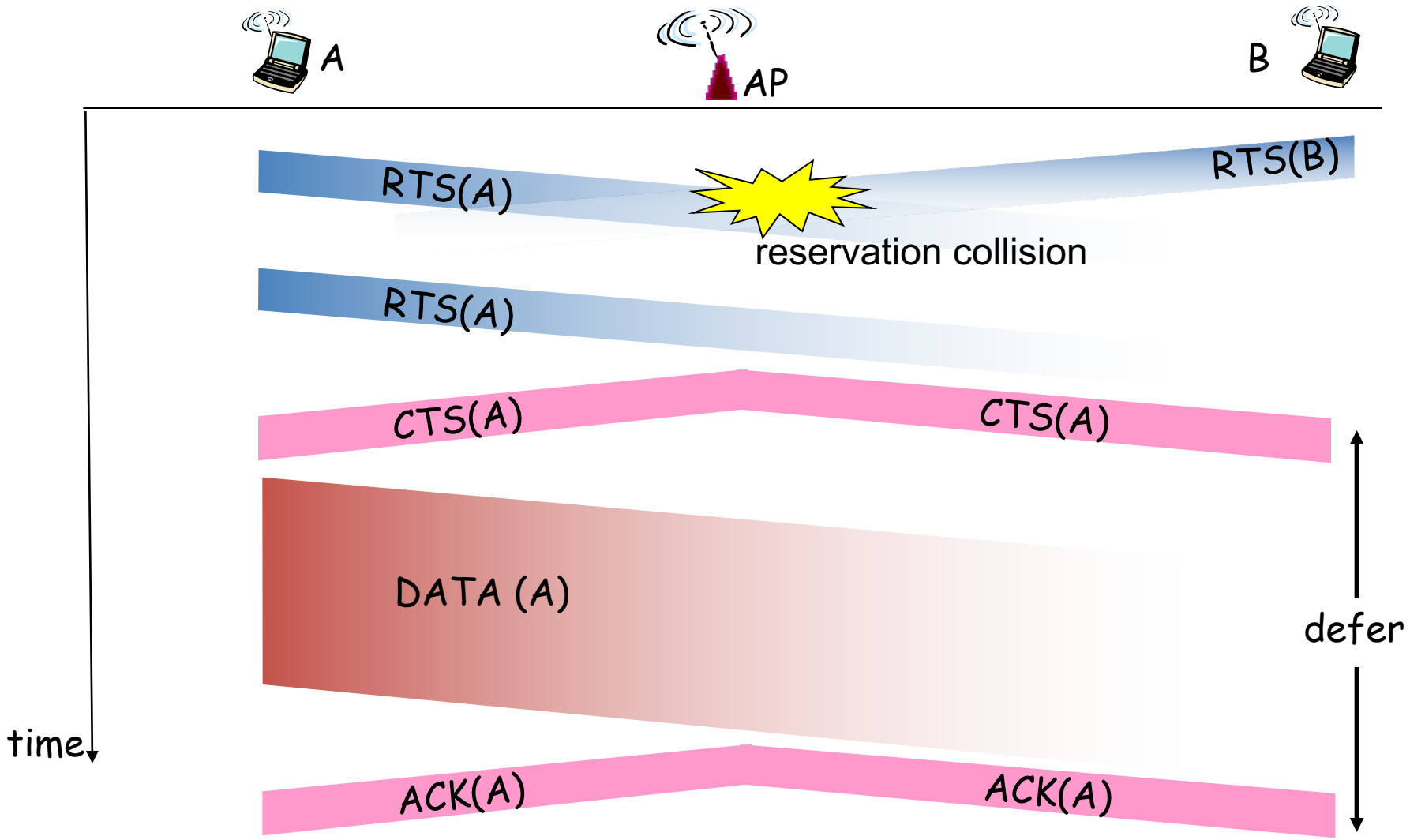
2 Se o canal estiver ocupado então
espera um tempo aleatório de backoff
O temporizador faz uma contagem decrescente à espera do canal inativo
Transmite quando o tempo termina
Se não tiver confirmação (ACK), aumenta o intervalo aleatório do tempo de backboff, e repete o passo 2

Receptor 802.11

- Se o quadro recebido estiver OK
devolve o ACK após o tempo SIFS (ACK é necessário por causa do problema do terminal escondido)



Collision Avoidance: RTS-CTS exchange



Applets do livro do Kurose

- http://wps.aw.com/aw_kurose_network_3/21/5493/1406348.cw/index.html
- http://media.pearsoncmg.com/aw/aw_kurose_network_2/applets/csma-ca/withouthidden.html
- http://media.pearsoncmg.com/aw/aw_kurose_network_2/applets/csma-ca/withhidden.html

112) Para obter mais informações sobre “Redes Sem Fios” identifique, no You Tube, os vídeos mais interessantes, atualizados e confiáveis sobre este assunto. Depois utilize estas informações para responder as questões de números 113 a 121.

Exemplos de alguns links

Redes sem fio

https://www.youtube.com/watch?v=YGejGIhLu8E&list=PLkJNjFf6dJTIzs5LY1YR0Bhy6vDgjDdN4

Segurança de redes sem fio: WEP, WPA, EAP, WPA2

https://www.youtube.com/watch?v=WkRMIXW_J7Y

802.11a, 802.11b, 802.11g, 802.11n, 802.11ac

https://www.youtube.com/watch?v=lcG6FVd-WAA

Wireless Networking English Tutorial

https://www.youtube.com/watch?v=3Bh4PcO2YJE

Tutorial Wireless Technology

https://www.youtube.com/watch?v=vH8xbva1H40

Evolução da Telefonia Móvel do 1G ao 5G

https://www.youtube.com/watch?v=WlgmLqXg8SQ

Exemplos de alguns links

From 1G to 4G & Towards 5G - Evolution Of Communication
https://www.youtube.com/watch?v=2nsEAw_SirQ
1G,2G,3G & 4G Best Explanation & Comparision
https://www.youtube.com/watch?v=Rjluns-AEnc
What is 1G, 2G, 3G, 4G, 5G of Cellular Mobile Communications
https://www.youtube.com/watch?v=CI9No9Ci9Ro
Olhar Digital - 5G Tudo que precisamos saber até 2020
https://www.youtube.com/watch?v=BNGhGBPt95Y
Primeira Transmissão 5G no Brasil com Tecnologia Nacional
https://www.youtube.com/watch?v=bxUcRNrCy0k
O 5G brasileiro da Inatel - Futurecom
https://www.youtube.com/watch?v=GI2IwujT39E

Exemplos de alguns links

Everything You Need to Know About 5G
https://www.youtube.com/watch?v=GEx_d0SjvS0
Fundamentals of 5G Mobile Communication
https://www.youtube.com/watch?v=7y75iBuW_6s
What Is 5G? & How 5G Will Change The World!
https://www.youtube.com/watch?v=LhECDSuXRDs
Introduction to 5G Mobile Communication Technology
https://www.youtube.com/watch?v=XC9Yx62vR9Q
5G Network Architecture by Andy Sutton (IET 2018 Turing)
https://www.youtube.com/watch?v=aGEAQJ7U1tA
What will the future of 5G bring? - BBC Click
https://www.youtube.com/watch?v=5hfZxsGcWB4

113) Quais são os tipos de redes sem fio locais (Wireless LAN) padronizadas?

114) Quais são as características, vantagens e desvantagens das Redes Sem Fios (Wireless LAN)?

115) Explique sobre os problemas do “terminal oculto” e “atenuação do sinal” em Redes Sem Fio.

116) Defina os elementos da topologia (BSS, STA, DS e ESS) da rede sem fios IEEE 802.11.

117) Comente sobre varredura passiva e ativa no IEEE 802.11.

118) Como foi resolvido o problema de segurança no IEEE 802.11, usando WEP, WPA, EAP, WPA2?

118) Descreva sucintamente as características de cada protocolo de Redes sem Fio (802.11a, 802.11b, 802.11g, 802.11n, 802.11ac) - 802.11 Wireless Wi-Fi.

120) Descreva sucintamente as características de cada geração da telefonia móvel (1G, 2G, 3G, 4G, 5G e 6G).

121) Estude e comente também sobre outras redes sem fio como: Redes de Sensores, RFID, IEEE 802.15.4 (Zigbee), IEEE 802.16 (WiMAX) e Bluetooth.