

Capítulo 3

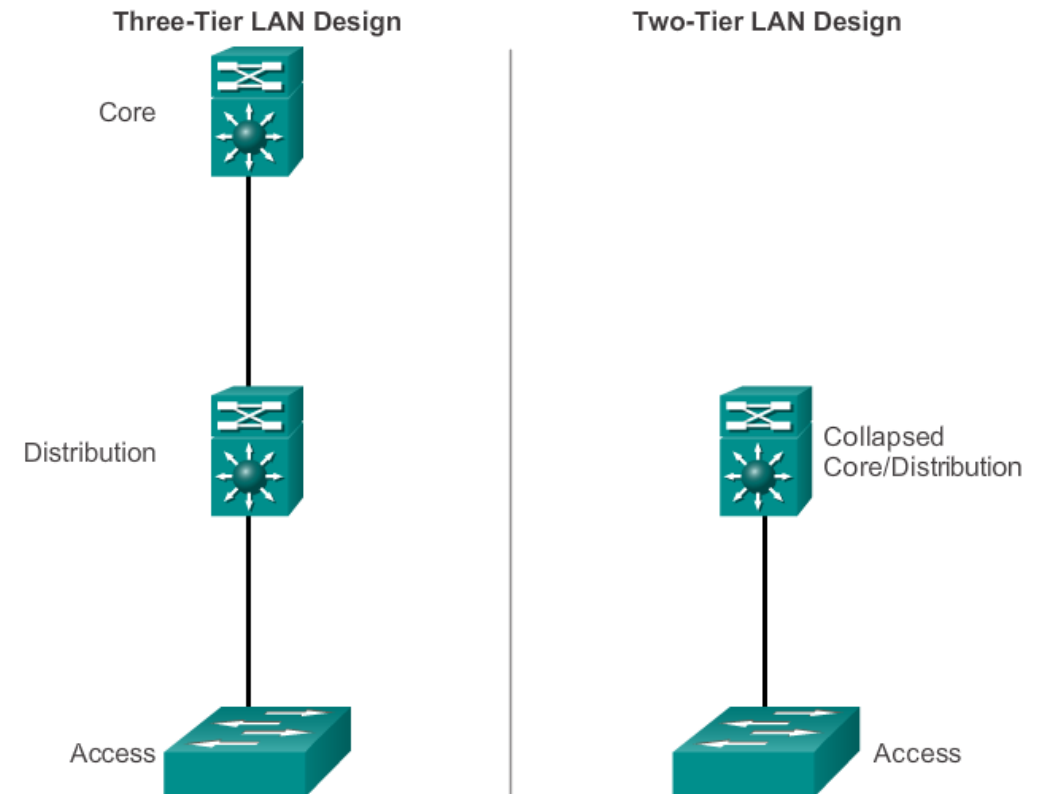
Redes numa organização

Projeto e configuração de redes

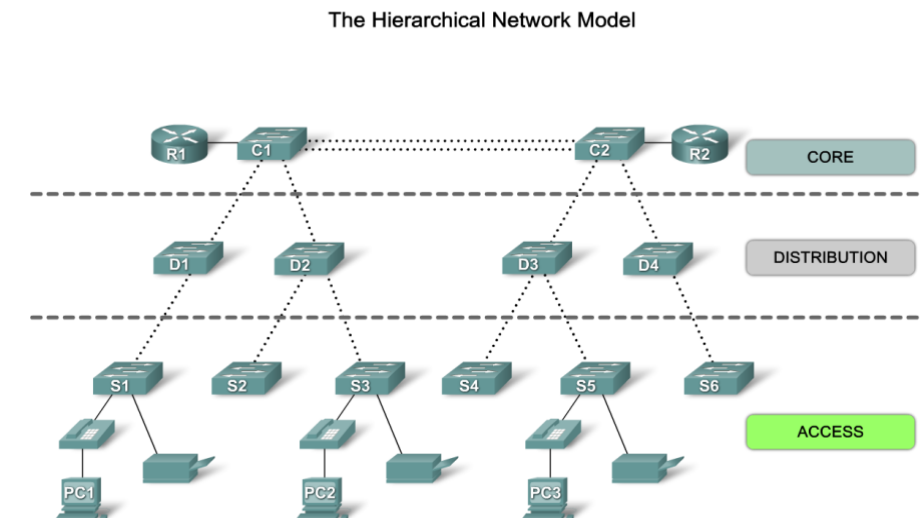
Características das LANs estruturadas através de switches

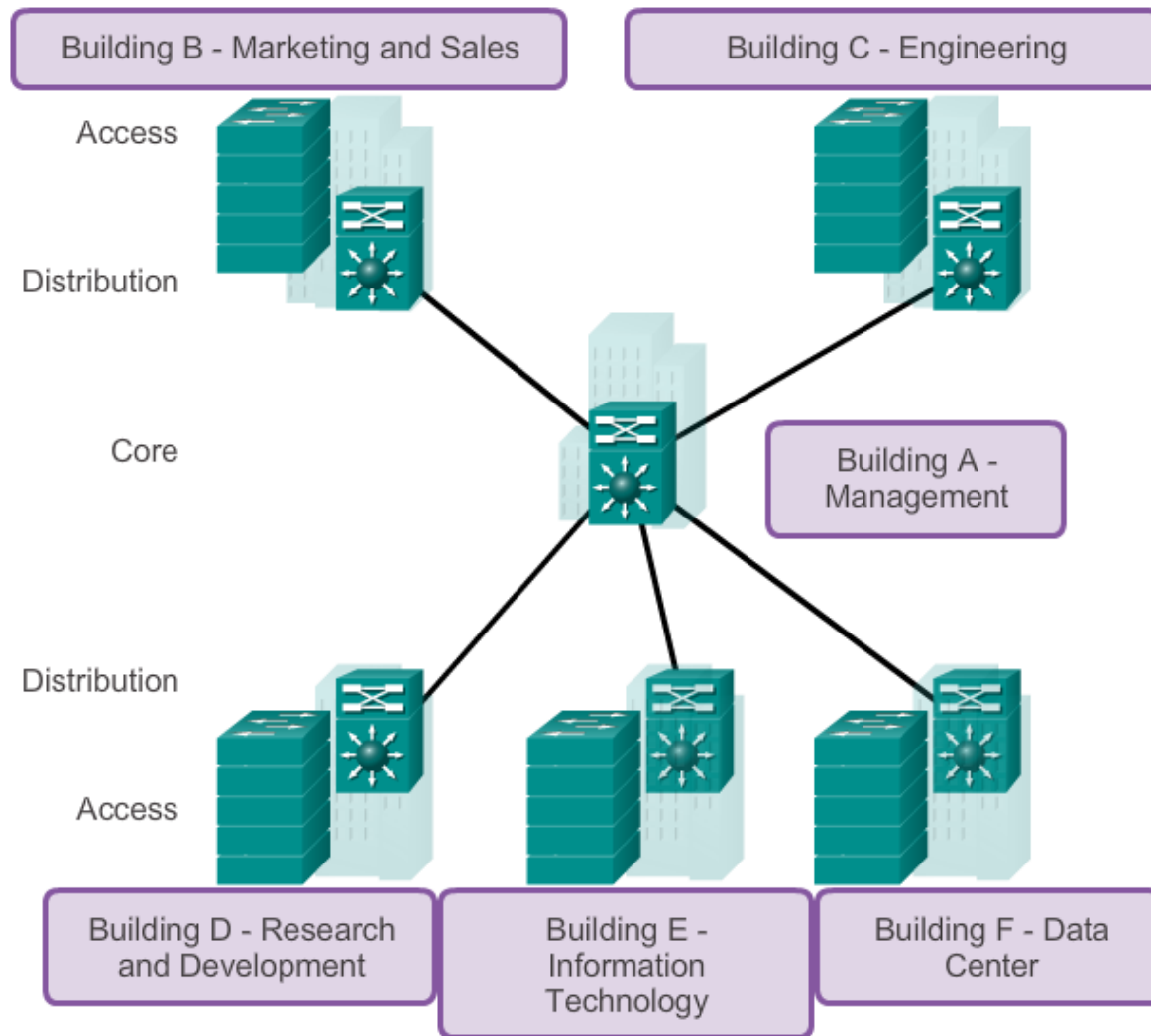
- A sobrevivência das empresas de tamanho pequeno e médio é fortemente dependente de uma LAN projetada adequadamente
 - ✓ É importante selecionar os equipamentos apropriados para suportar as especificações da rede
- Iremos estudar os princípios que são usados para projetar uma rede hierárquica

- As orientações de projeto de rede comutada são construídos sobre os seguintes princípios:
- ✓ Hierarquia
 - ✓ Modularidade
 - ✓ Resiliência
 - ✓ Flexibilidade



- O projeto de uma rede terá mais sucesso se for usado o modelo de rede hierárquico
 - ✓ Divisão da rede em camadas
 - ✓ Desempenhando cada camada funções específicas – divisão das várias funções
- O modelo hierárquico divide as funções por 3 camadas: acesso, distribuição e núcleo (core)
- A representação lógica seguinte torna fácil ver que switches executam quais funções
 - ✓ A visualização das camadas hierárquicas torna-se muito difícil quando a rede está instalada (usando a representação física)

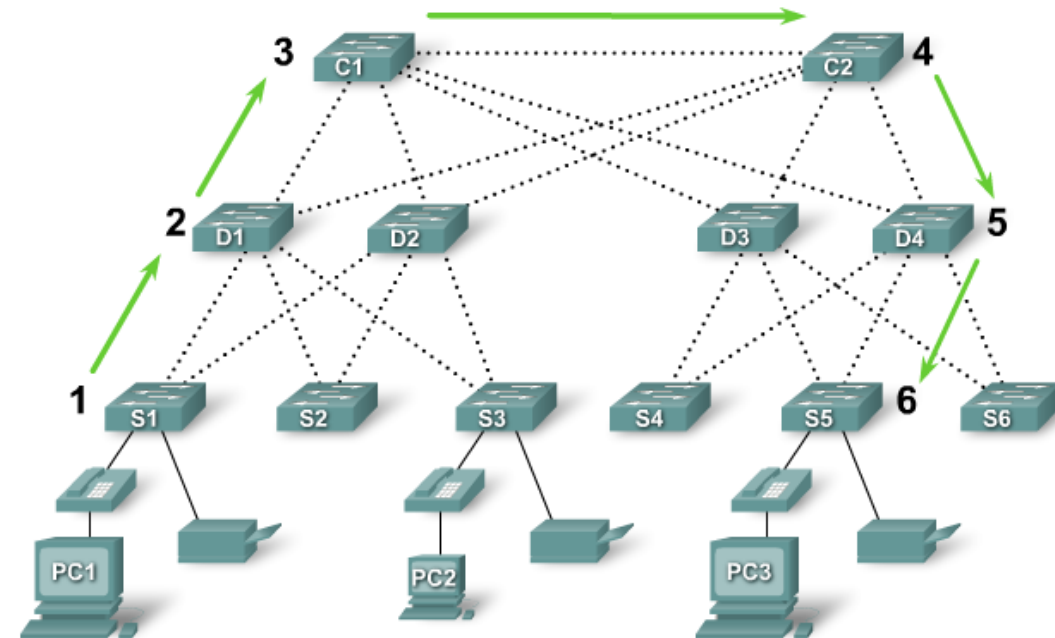




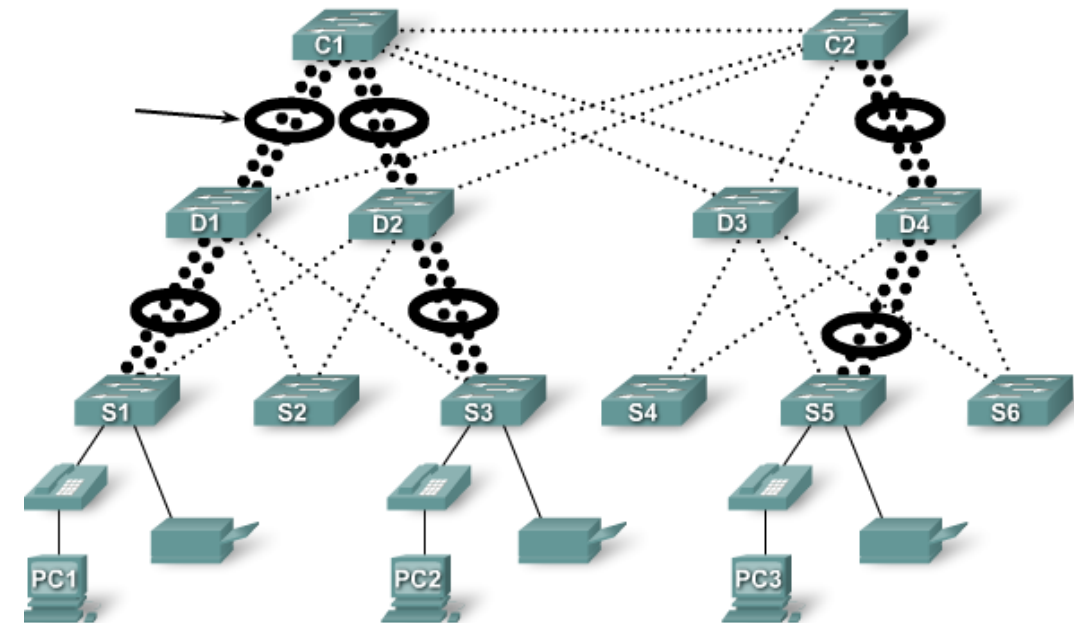
- Camada de acesso
 - ✓ Oferece um meio de ligação dos equipamentos terminais (PCs, impressoras, telefones IP) à rede
 - ✓ Pode incluir: switches, hubs, APs, etc
 - ✓ Controla quais os equipamentos que podem comunicar na rede
 - ✓ Permite a definição de LANs virtuais (VLANs)
- Camada de distribuição
 - ✓ Agrega os dados recebidos da camada de acesso
 - ✓ Controla os fluxos de tráfego usando políticas e delinea os domínios de broadcast executando funções de encaminhamento entre VLANs
- Camada de núcleo
 - ✓ Agrega o tráfego de todos os equipamentos da camada de distribuição
- Nota: Em redes pequenas é comum combinar numa única camada a camada de core e a de distribuição

- **Escalabilidade**
 - ✓ A expansão é fácil de planear e implementar
- **Redundância – aumentar a disponibilidade da rede**
 - ✓ A ligação dos switches da camada de acesso a dois switches da camada de distribuição assegura caminhos redundantes
- **Desempenho**
 - ✓ Os dados são enviados utilizando agregação de links da camada de acesso para a camada de distribuição
 - ✓ Uma rede bem projetada pode atingir aproximadamente velocidade de fio (wire) entre todos os equipamentos
- **Segurança**
 - ✓ Os switches da camada de acesso podem ser configurados com segurança nas portas para controlar quais os equipamentos que são permitidos ligarem-se à rede
 - ✓ Na camada de distribuição é possível definir políticas de controlo de acesso – por exemplo limitar o uso de um determinado protocolo a determinados utilizadores
- **Capacidade de gestão**
 - ✓ Como cada camada executa funções específicas, se for necessário alterar as funções de um switch de uma determinada camada essa mudança poderá ser repetida em todos os switches dessa camada porque eles provavelmente executam as mesmas funções
- **Sustentabilidade**
 - ✓ Como as funções dos switches são definidas por camadas isto facilita a seleção do switch correto nas novas aquisições
 - ✓ Podem usar-se switches mais baratos na camada de acesso

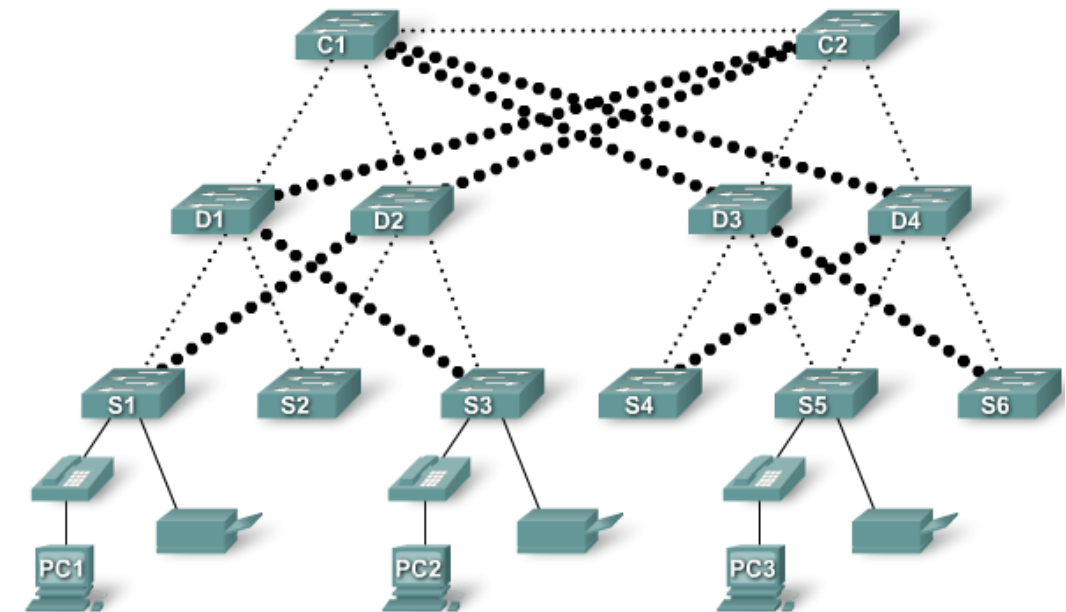
- Não é suficiente a rede estar projetada hierarquicamente para estar bem projetada
- Diâmetro da rede
 - ✓ Número de equipamentos que um pacote tem que atravessar antes de alcançar o destino – diâmetros pequenos garante que a latência entre equipamentos seja pequena e previsível
- Latência – tempo gasto por um equipamento a processar um pacote ou quadro

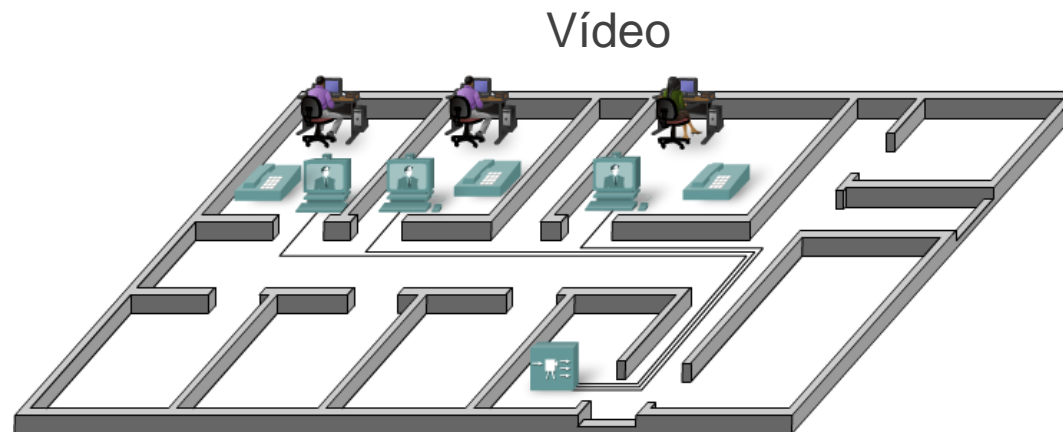
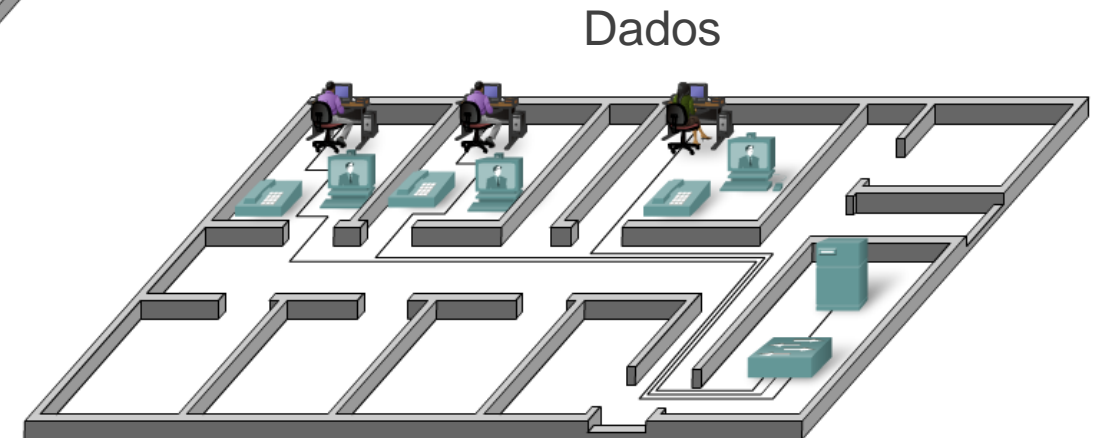
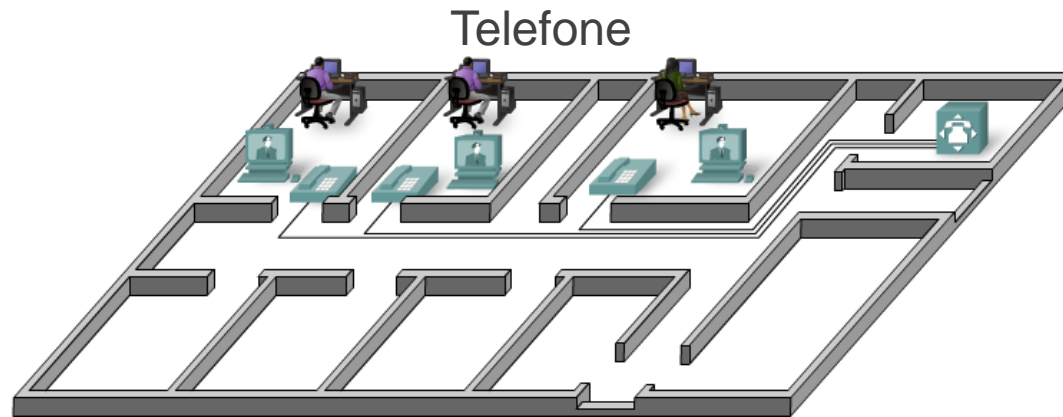


- Agregação de largura de banda (Bandwidth)
 - A agregação de ligações (links) consiste em combinar várias portas de um switch para obter maior throughput entre os switches
 - A tecnologia proprietária da Cisco, EtherChannel, permite combinar até 8 Ligações Ethernet

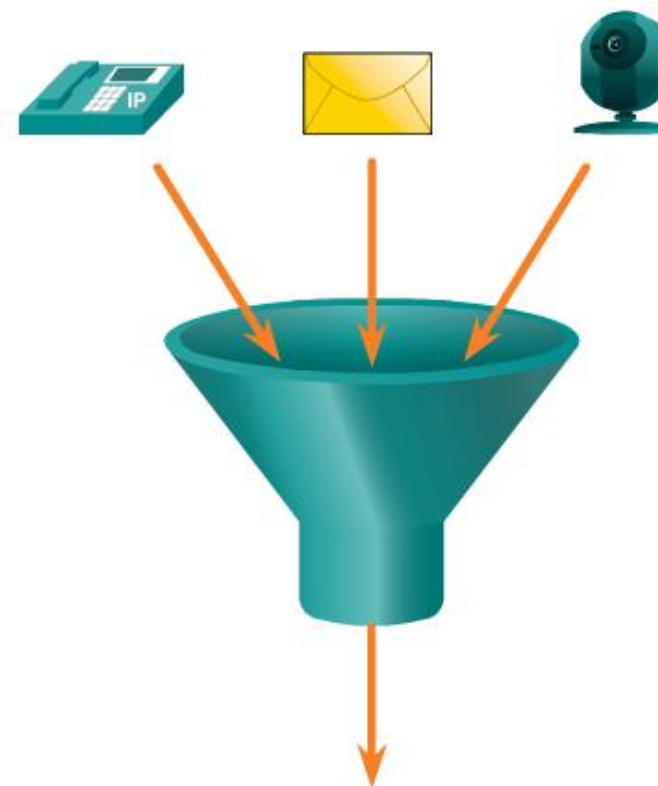


- Redundância
 - ✓ Aumenta a disponibilidade da rede
 - ✓ Pode ser oferecida por exemplo:
 - ❖ Duplicando as ligações entre os equipamentos
 - ❖ Duplicando os próprios equipamentos



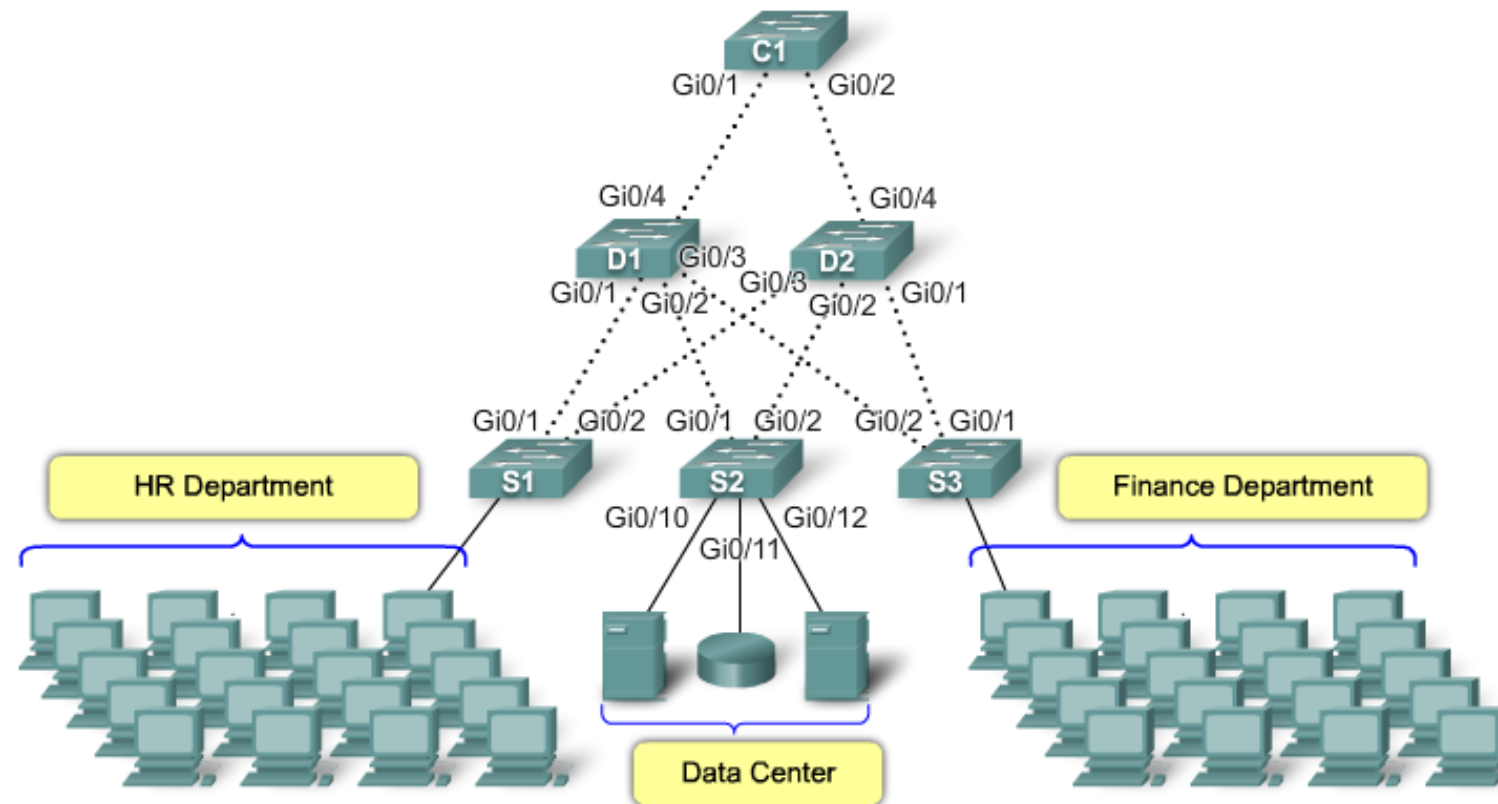


- A colaboração é uma necessidade
- Para suportar a colaboração, as redes empregam soluções convergentes
- Estas incluem os serviços de dados, tais como sistemas de voz, telefones IP, gateways de voz, suporte de vídeo e videoconferência

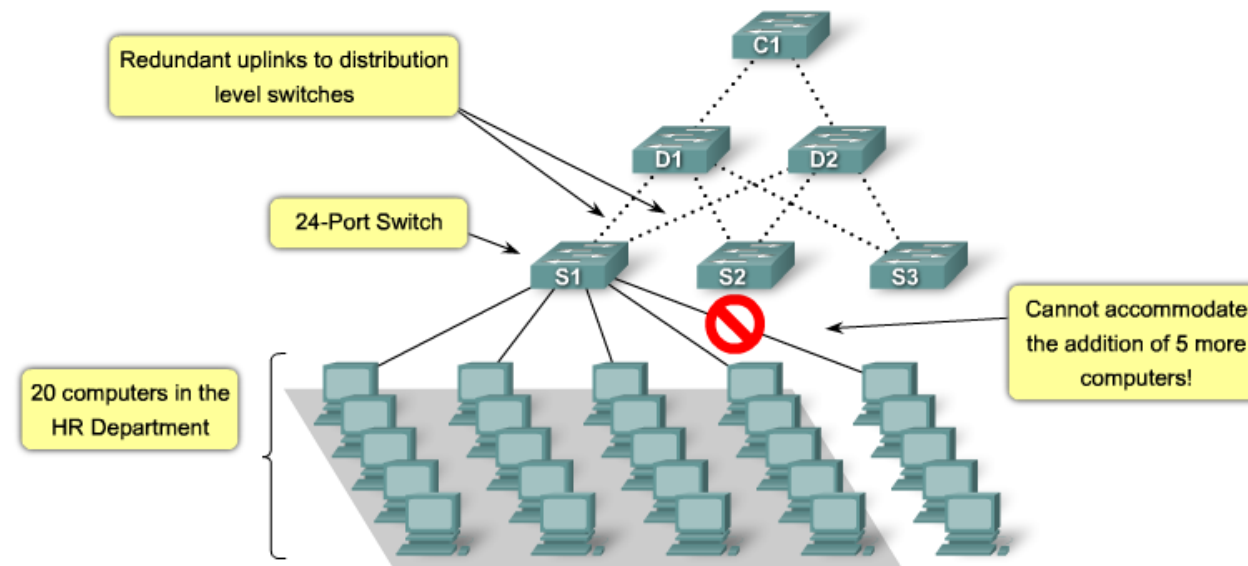


- Processo de integração de voz e vídeo numa rede de dados
- Existiu como ideia muito tempo sem ser aplicada
 - ✓ Exigiam novos equipamentos
 - ✓ Os novos equipamentos eram caros
- Nas redes convergentes passa a existir apenas uma rede para gerir
- É necessário implementar apenas uma infraestrutura

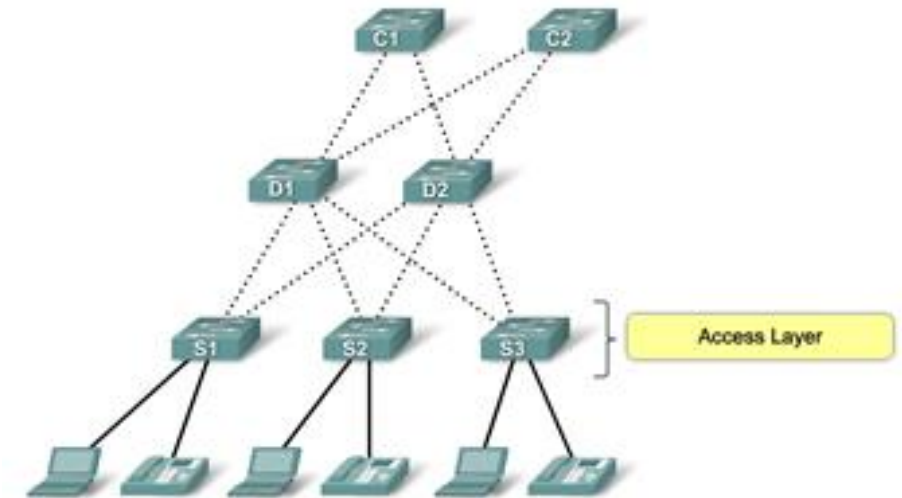
- Mostra como todos os switches são interligados e eventuais pormenores adicionais



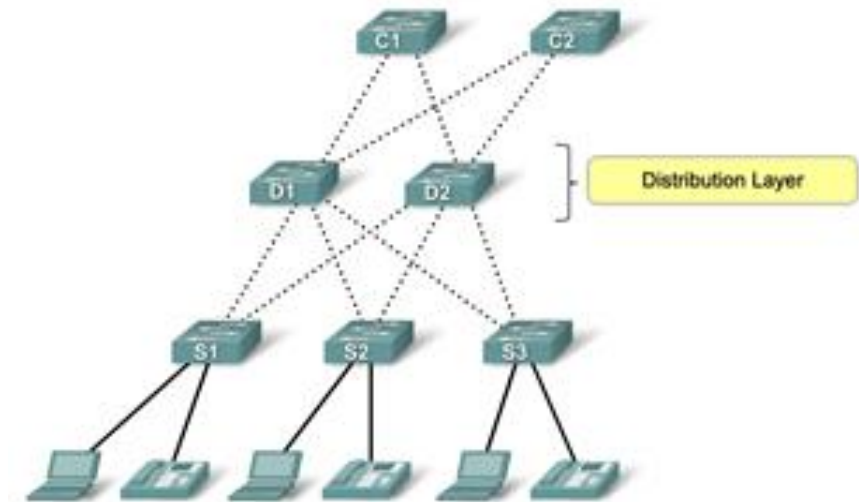
- Em geral os utilizadores finais são agrupados de acordo com os seus cargos porque o seu tipo de acesso a recursos e aplicações é semelhante
- Um projeto de rede bom deve ter em conta não apenas as necessidades atuais (em termos de número de portas e necessidades de tráfego) mas também ter em conta o crescimento



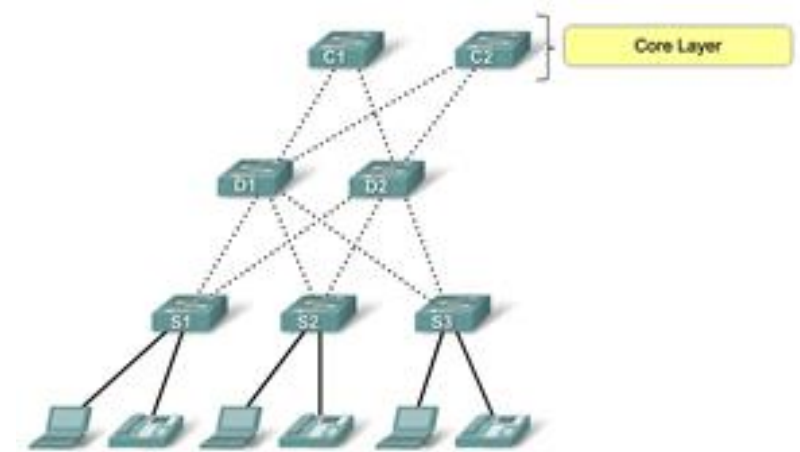
- Segurança nas portas
- Configuração de VLANs
- Fast Ethernet/Gigabit Ethernet
- Power over Ethernet (PoE)
- Agregação de ligações
- Configurações de Qualidade de Serviço (QoS)



- Políticas de segurança/Listas de controlo de acesso
- Taxas de encaminhamento grandes
- Gigabit Ethernet/10 Gigabit Ethernet
- Componentes redundantes
- Agregação de ligações
- Configurações de Qualidade de Serviço (QoS)



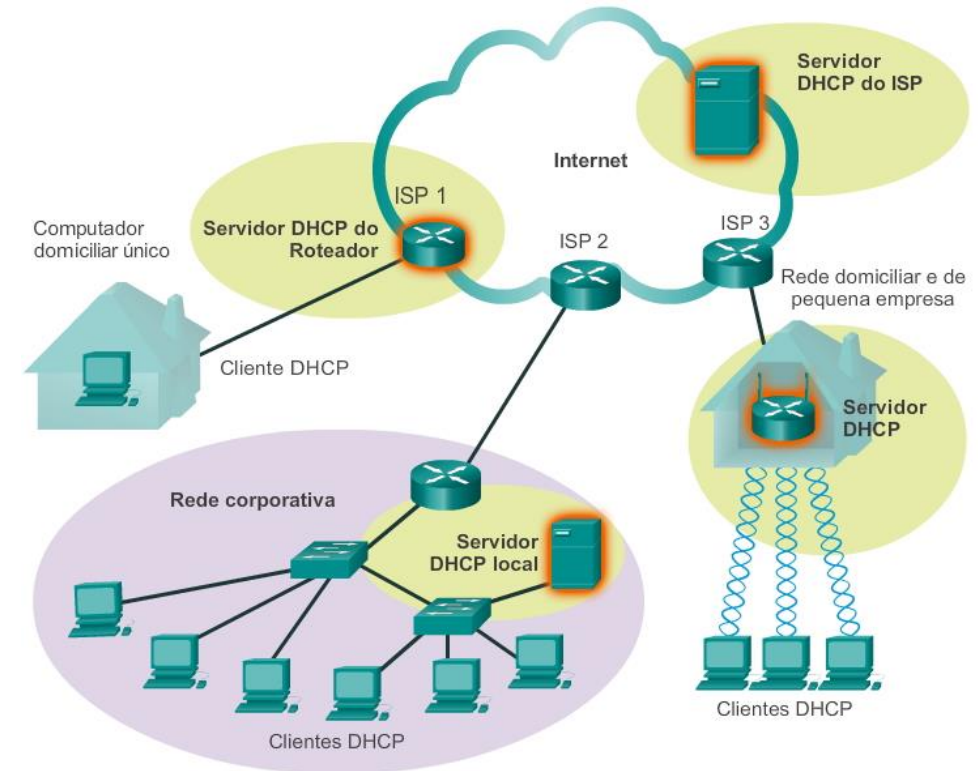
- Suporte para funções Camada 3
- Taxas de encaminhamento muito grandes
- Gigabit Ethernet/10 Gigabit Ethernet
- Componentes redundantes
- Agregação de ligações
- Configurações de Qualidade de Serviço (QoS)



Viver com as limitações do IPv4

Endereçamento dinâmico usando DHCPv4 e DHCPv6

- O DHCP permite que um host obtenha um endereço IP de forma dinâmica
- O servidor DHCP é contactado e o endereço é solicitado - escolhe o endereço de uma lista configurada de endereços chamada pool e "arrenda-o" ao host por um período definido
- O DHCP é utilizado por hosts de uso geral, como dispositivos de utilizador final e o endereçamento estático, é usado em dispositivos de rede, como gateways, switches, servidores e impressoras



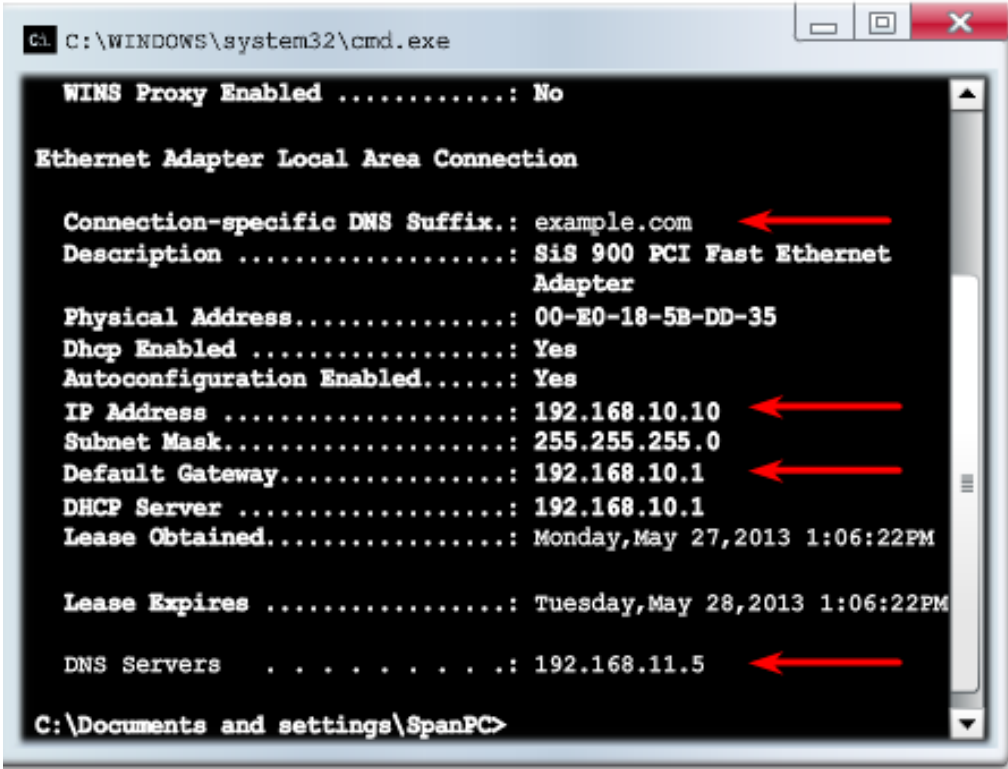
- Dynamic Host Configuration Protocol (DHCP) é um protocolo de rede que fornece endereçamento IP automático e outras informações para os clientes:
 - ✓ Endereço IP
 - ✓ Máscara de sub-rede (IPv4) ou comprimento de prefixo (IPv6)
 - ✓ Endereço do default gateway
 - ✓ Endereço do servidor DNS
- Disponível tanto para IPv4 como para IPv6
- Este capítulo explora as funcionalidades, configuração e resolução de problemas tanto para DHCPv4 como para DHCPv6

- DHCPv4 utiliza três métodos diferentes de atribuição de endereços
 - ✓ Atribuição Manual - O administrador atribui um endereço IPv4 pré-alocado ao cliente, e DHCPv4 envia apenas o endereço IPv4 ao dispositivo.
 - ✓ Atribuição automática - DHCPv4 atribui automaticamente um endereço IPv4 estático permanentemente a um dispositivo, selecionando-o a partir de uma pool de endereços disponíveis. Não há empréstimo temporário.
 - ✓ Atribuição dinâmica - DHCPv4 atribui dinamicamente, ou empresta, um endereço IPv4 de uma pool de endereços por um período limitado de tempo escolhido pelo servidor, ou até que o cliente não precisa mais do endereço. O método mais utilizado.

- Um router Cisco executando o software Cisco IOS pode ser configurado para funcionar como um servidor DHCPv4. Para configurar o DHCP
 - ✓ Excluir endereços da pool.
 - ✓ Configure o nome da pool de DHCP
 - ✓ Configurando tarefas específicas -. Definir a gama de endereços e máscara de sub-rede. Use o comando default-router para definir o default gateway. Itens opcionais que podem ser incluídos na pool - servidor dns e nome de domínio (domain-name)
- Para desativar o dhcp - no service dhcp

```
R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1(config)# ip dhcp excluded-address 192.168.10.254
R1(config)# ip dhcp pool LAN-POOL-1
R1(dhcp-config)# network 192.168.10.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.10.1
R1(dhcp-config)# dns-server 192.168.11.5
R1(dhcp-config)# domain-name example.com
R1(dhcp-config)# end
R1#
```


- Comando para verificar a configuração do DHCP
- show running-config | section dhcp
- No PC – executar o comando ipconfig / all



```
C:\WINDOWS\system32\cmd.exe

WINS Proxy Enabled .....: No

Ethernet Adapter Local Area Connection

Connection-specific DNS Suffix.: example.com
Description .....: SiS 900 PCI Fast Ethernet Adapter
Physical Address.....: 00-E0-18-5B-DD-35
Dhcp Enabled .....: Yes
Autoconfiguration Enabled.....: Yes
IP Address .....: 192.168.10.10
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.10.1
DHCP Server .....: 192.168.10.1
Lease Obtained.....: Monday, May 27, 2013 1:06:22PM

Lease Expires .....: Tuesday, May 28, 2013 1:06:22PM

DNS Servers . . . . .: 192.168.11.5

C:\Documents and settings\SpanPC>
```

- Usar o comando `ip helper-address ip_address` para habilitar um router para enviar broadcasts DHCPv4 para o servidor DHCPv4. Agindo como um router relay

```
R1(config)# interface g0/0
R1(config-if)# ip helper-address 192.168.11.6
R1(config-if)# end
R1# show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is 192.168.11.6
<Output omitted>
```



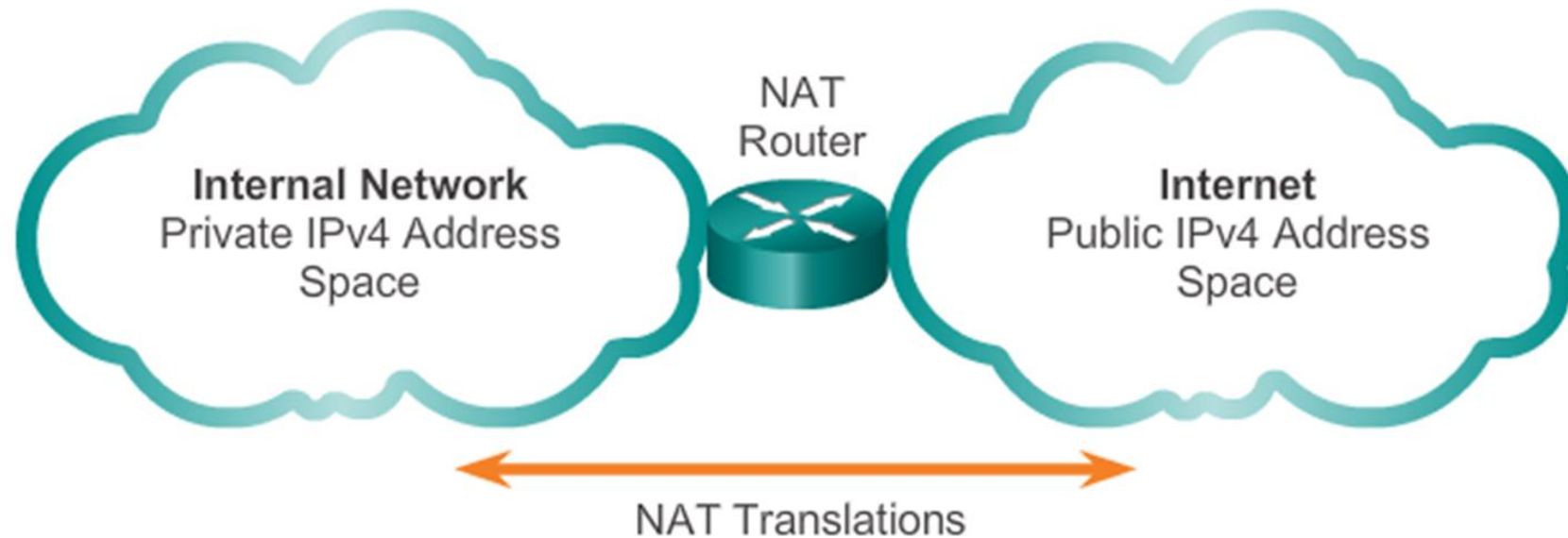
```
SOHO(config)# interface g0/1
SOHO(config-if)# ip address dhcp
SOHO(config-if)# no shutdown
SOHO(config-if)#
*Jan 31 17:31:11.507: %DHCP-6-ADDRESS_ASSIGN: Interface
GigabitEthernet0/1 assigned DHCP address 209.165.201.12, mask
255.255.255.224, hostname SOHO
SOHO(config-if)# end
SOHO# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 209.165.201.12/27
  Broadcast address is 255.255.255.255
  Address determined by DHCP
  <Output omitted>
```

➤ 10.2.2.7 - Servidores DHCP e DNS

Viver com as limitações do IPv4

Funcionamento e configuração do protocolo NAT (Network Address Translation)

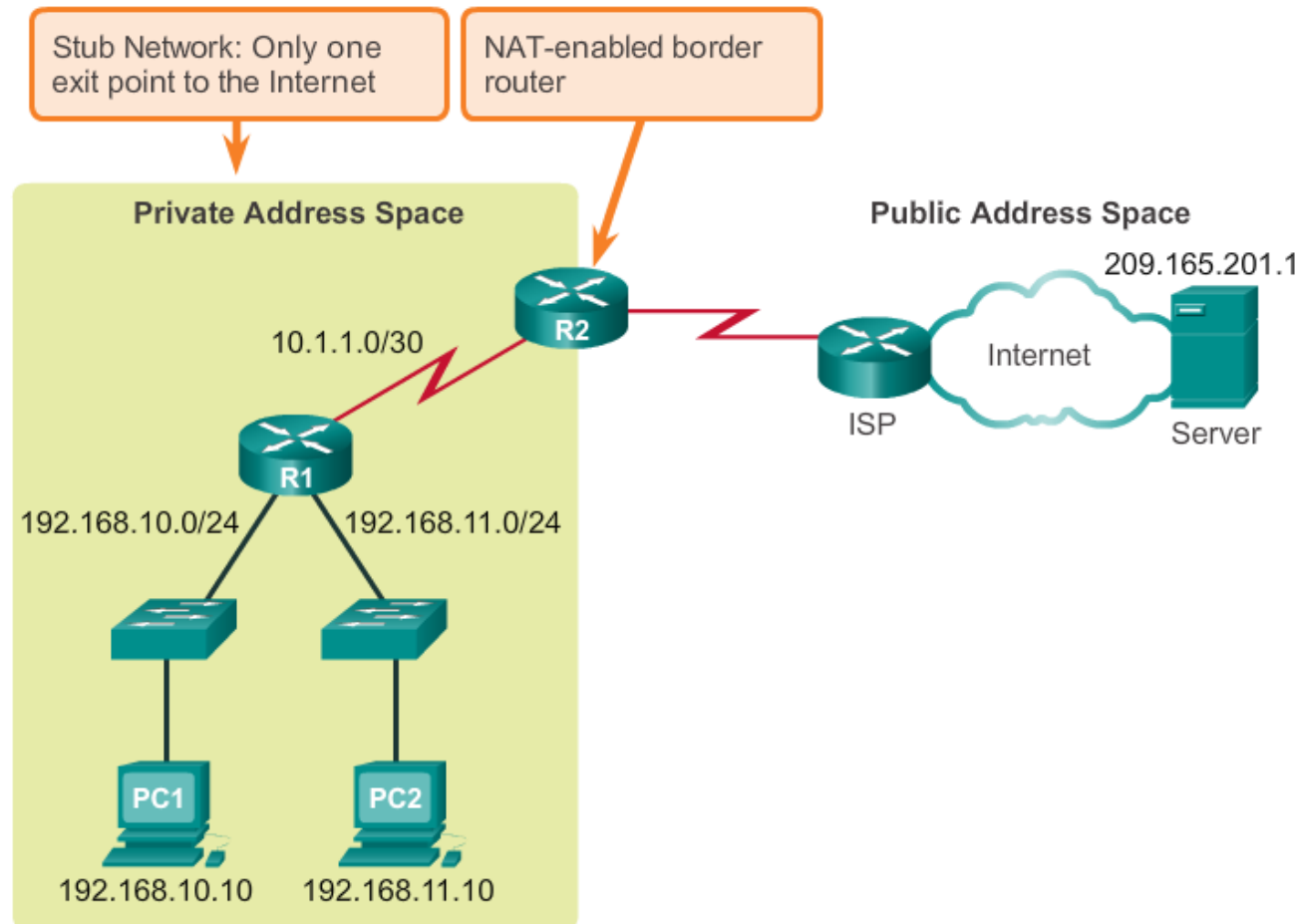
- O espaço de endereços IPv4 não é grande o suficiente para fornecer endereços para todos os dispositivos que precisam de estar ligados à Internet
- Endereços privados de Rede estão descritos no RFC 1918 e foram planeados para serem usados dentro de uma organização
- Os endereços privados não são encaminhadas pelos routers da Internet, isso só acontece com endereços públicos
- Os endereços privados podem aliviar a escassez IPv4 mas como não são encaminhados pelos routers, para isso acontecer eles precisam em primeiro lugar de ser traduzidos.
- NAT é o processo usado para realizar essa tradução



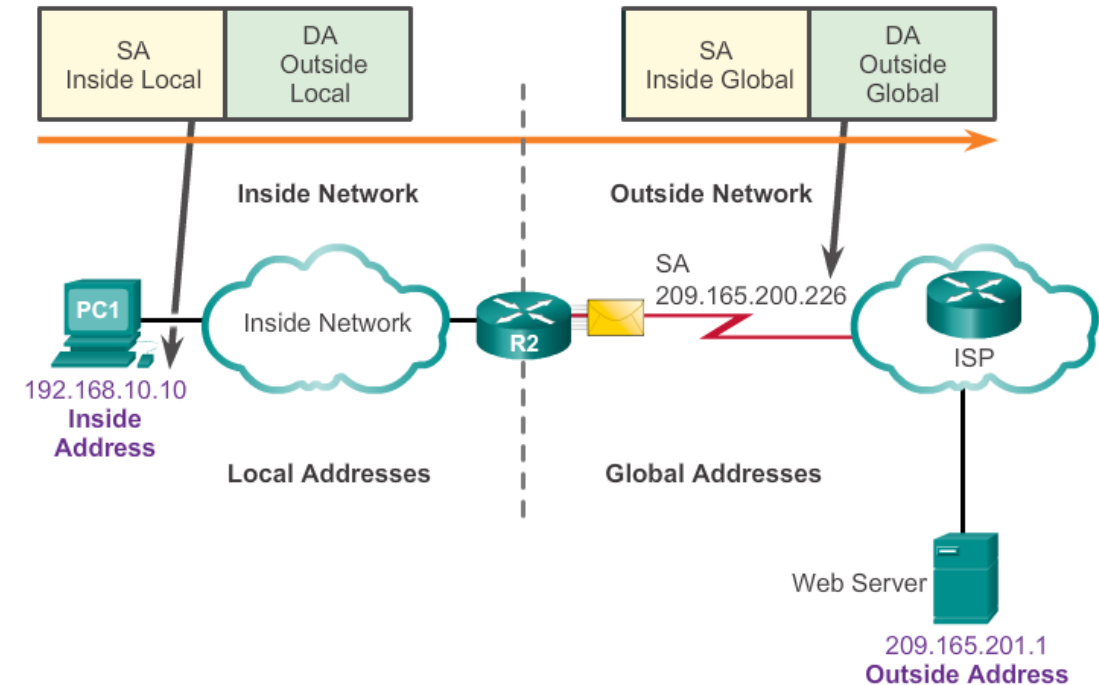
Private Internet addresses are defined in RFC 1918:

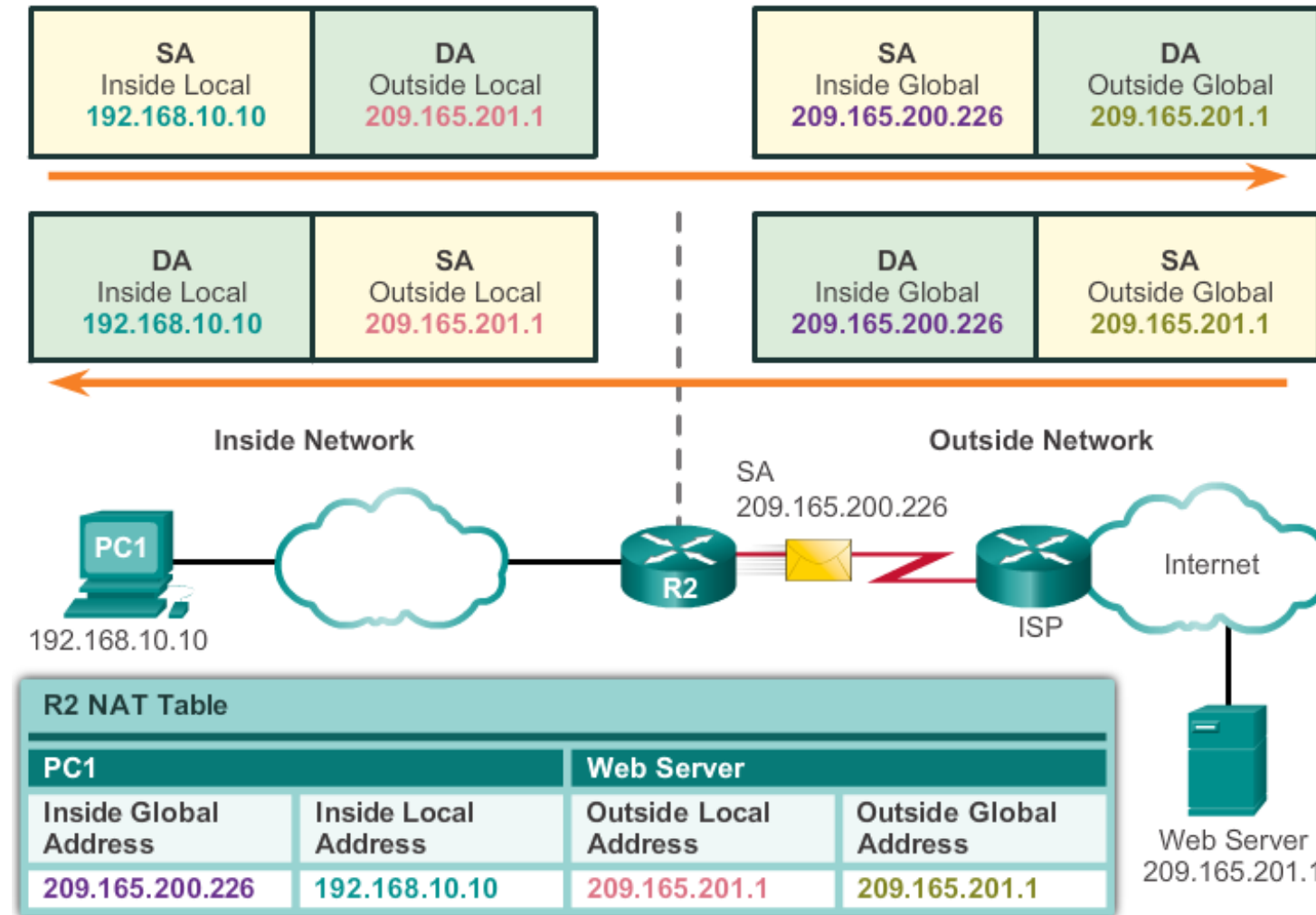
Class	RFC 1918 Internal Address Range	CIDR Prefix
A	10.0.0.0 - 10.255.255.255	10.0.0.0/8
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16

- NAT é um processo utilizado para traduzir os endereços de Rede
- A principal utilização de NAT é preservar endereços IPv4 públicos
- Normalmente implementado em dispositivos de rede de fronteira, tais como firewalls ou routers
- Isto permite que as redes usem endereços privados internamente, apenas traduzidos para endereços públicos, quando necessário
- Aos dispositivos dentro das organizações podem ser atribuídos endereços privados e funcionarem com endereços que são únicos localmente.
- Quando o tráfego precisa ser enviado / recebido de / para outras organizações na Internet, o router fronteira traduz os endereços para endereços públicos e únicos globalmente



- Na terminologia do NAT, a rede interna é o conjunto de dispositivos que utilizam endereços privados. Redes externas são todas as outras redes
- ✓ NAT inclui 4 tipos de endereços:
 - ✓ Endereço local interno
 - ✓ Endereços global interno
 - ✓ Endereço local externo
 - ✓ Endereço global externo

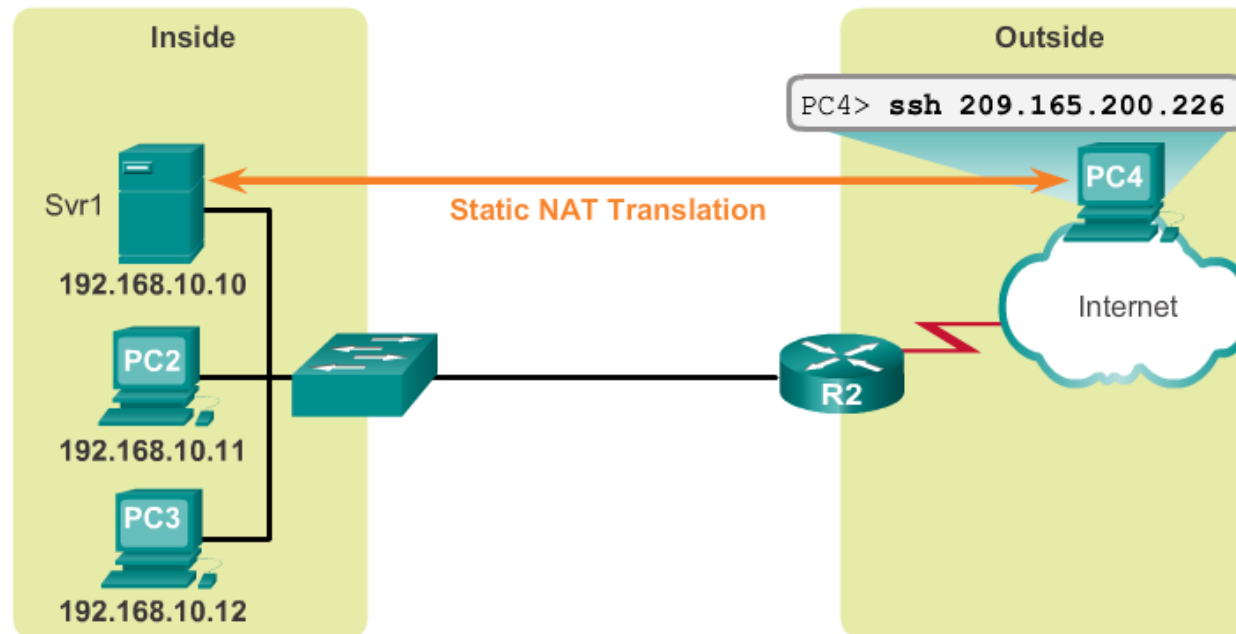




- NAT estático utiliza um mapeamento um-para-um entre os endereços locais e globais
- Esses mapeamentos são configurados pelo administrador da rede e mantem-se constantes
- NAT estático é particularmente útil quando os servidores na rede interna devem ser acessíveis a partir da rede externa
- Um administrador de rede pode aceder por SSH para um servidor na rede interna utilizando no cliente SSH o endereços global interno

Static NAT

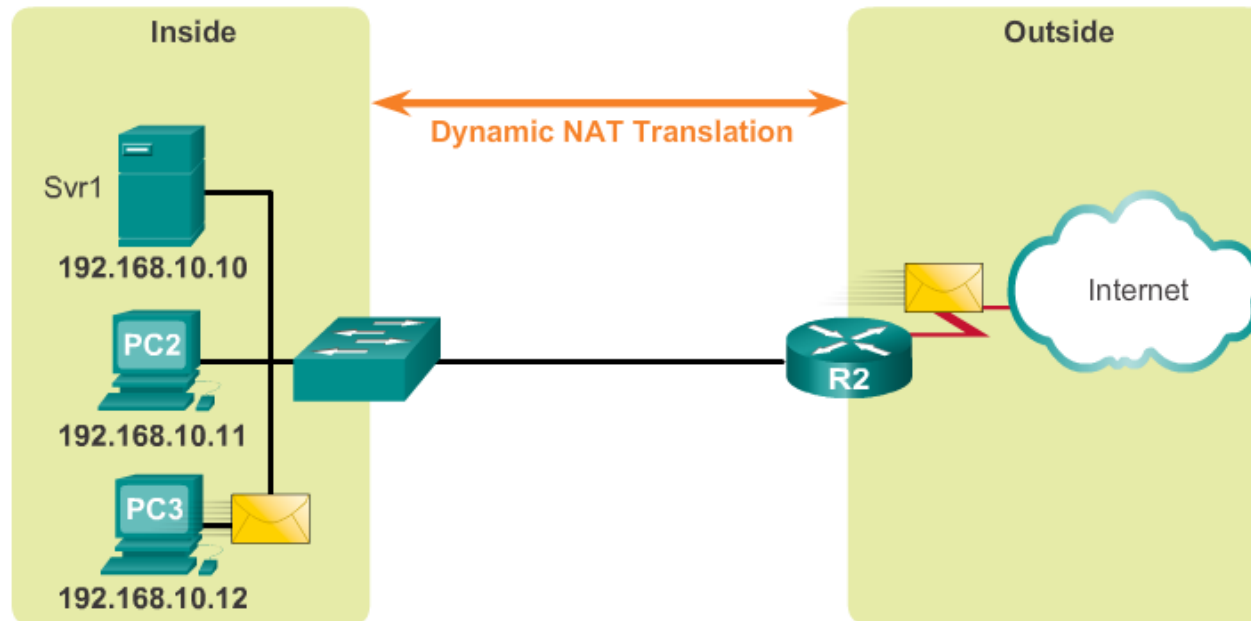
Static NAT Table	
Inside Local Address	Inside Global Address - Addresses reachable via R2
192.168.10.10	209.165.200.226
192.168.10.11	209.165.200.227
192.168.10.12	209.165.200.228



- NAT dinâmico utiliza uma pool de endereços públicos e atribui-os de forma a que o primeiro a chegar será o primeiro a ser servido
- Quando um dispositivo interno solicita acesso a uma rede externa, NAT atribui dinamicamente um endereço IPv4 público disponível na pool para esse acesso
- NAT dinâmico requer que estejam disponíveis endereços públicos suficientes para satisfazer o número total de sessões simultâneas

Dynamic NAT

IPv4 NAT Pool	
Inside Local Address	Inside Global Address Pool - Addresses reachable via R2
192.168.10.12	209.165.200.226
Available	209.165.200.227
Available	209.165.200.228
Available	209.165.200.229
Available	209.165.200.230

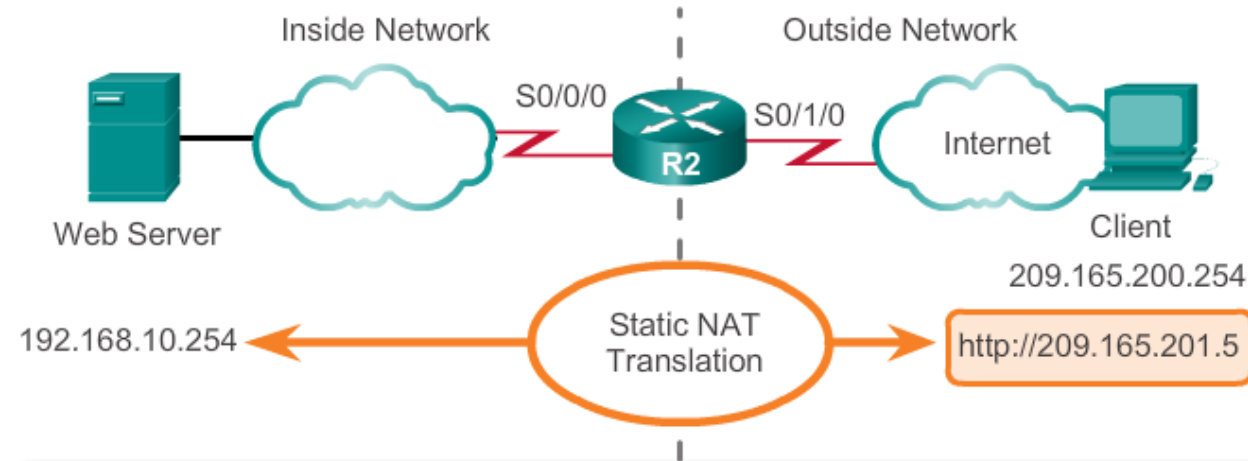


- PAT mapeia vários endereços IPv4 privado num endereço IPv4 público único ou num número de endereços inferior
- PAT usa o par endereço IP e porto de origem para rastrear que tráfego pertence a que cliente interno
- PAT também é conhecido como NAT overload
- Utilizando também o número do porto, PAT é capaz de transmitir os pacotes de resposta para o dispositivo interno correto
- O processo PAT também permite verificar se os pacotes que chegam foram solicitados, acrescentando assim um grau de segurança à sessão

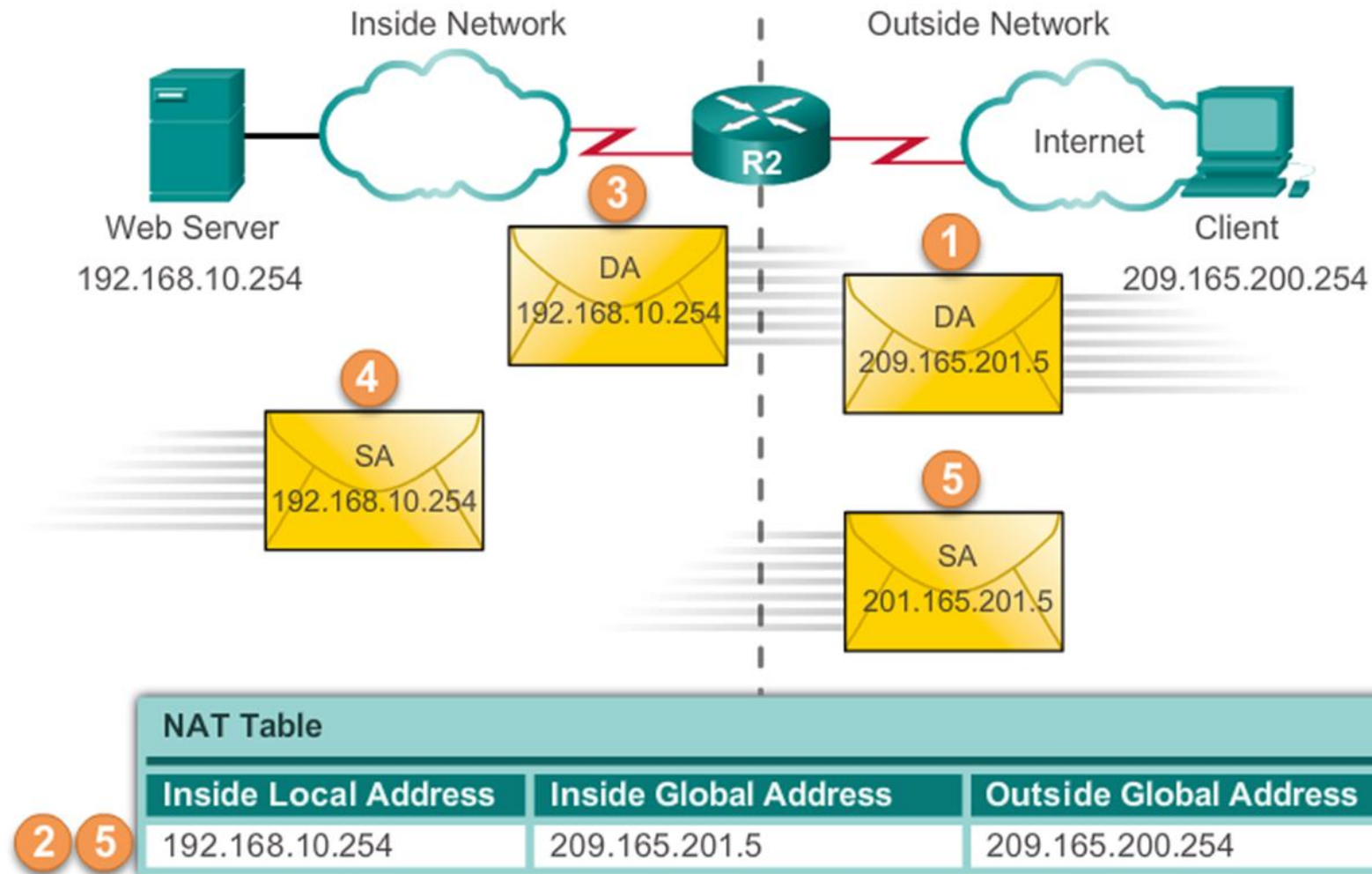
- NAT traduz endereços IPv4 na razão de 1:1 entre endereços IPv4 privados e endereços IPv4 públicos
- PAT modifica tanto o endereço como o número do porto
- NAT encaminha os pacotes de entrada para o destino interno, referindo-se ao endereço IPv4 de entrada fornecido pelo host na rede pública
- Com PAT, há geralmente apenas um ou poucos endereços IPv4 mostrados publicamente
- PAT também é capaz de traduzir protocolos que não utilizam números de porto, como o ICMP. Cada um desses protocolos são suportados de forma diferente por PAT

- Há duas tarefas básicas quando se pretende configurar traduções de NAT estático:
 - ✓ Criar o mapeamento entre os endereços locais internos e os endereços locais externos
 - ✓ Definir quais interfaces pertencem à rede interna e quais pertencem à rede externa

Example Static NAT Configuration



```
Establishes static translation between an inside local address and  
an inside global address.  
R2(config)# ip nat inside source static 192.168.10.254 209.165.201.5  
  
R2(config)# interface Serial0/0/0  
R2(config-if)# ip address 10.1.1.2 255.255.255.252  
Identifies interface serial 0/0/0 as an inside NAT interface.  
R2(config-if)# ip nat inside  
R2(config-if)# exit  
  
R2(config)# interface Serial0/1/0  
R2(config-if)# ip address 209.165.200.225 255.255.255.224  
Identifies interface serial 0/1/0 as the outside NAT interface.  
R2(config-if)# ip nat outside
```



The static translation is always present in the NAT table.

```
R2# show ip nat translations
Pro Inside global  Inside local  Outside local  Outside global
--- 209.165.201.5  192.168.10.254  ---          ---
R2#
```

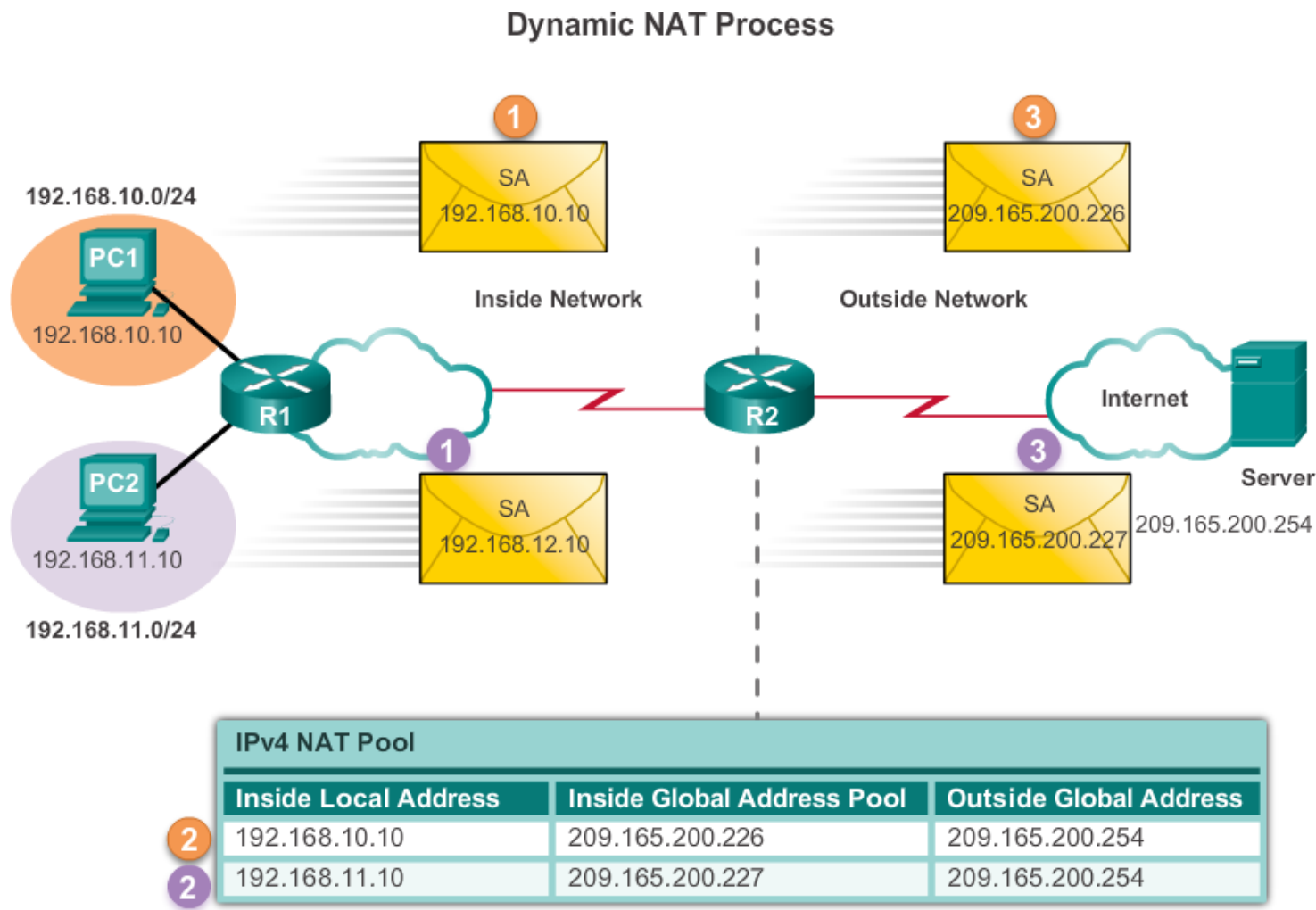
The static translation during an active session.

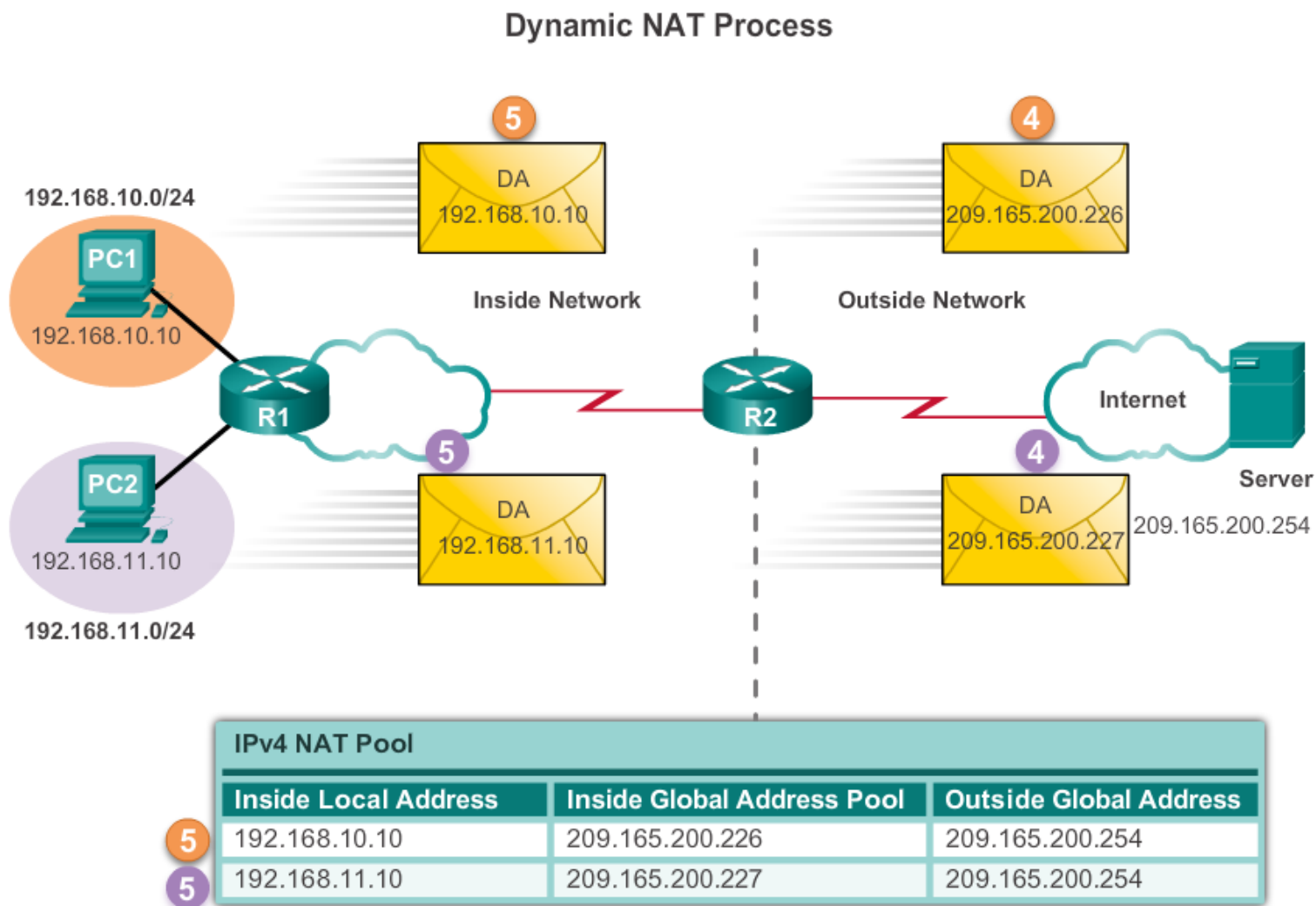
```
R2# show ip nat translations
Pro Inside global  Inside local  Outside local  Outside global
--- 209.165.201.5  192.168.10.254  209.165.200.254  209.165.200.254
R2#
```

- A pool de endereços IPv4 públicos (pool de endereços globais internos) está disponível para qualquer dispositivo na rede interna numa base primeiro a chegar, primeiro a ser servido
- Com o NAT dinâmico, um endereço interno é traduzido para um endereço externo
- A pool deve ser grande o suficiente para acomodar todos os dispositivos no interior
- Um dispositivo não será capaz de comunicar a quaisquer redes externas se não houver qualquer endereço disponível na pool

Dynamic NAT Configuration Steps

Dynamic NAT Configuration Steps	
Step 1	<p>Define a pool of global addresses to be used for translation.</p> <pre>ip nat pool name start-ip end-ip { netmasknetmask prefix-length prefix-length }</pre>
Step 2	<p>Define a standard access list permitting the addresses that should be translated.</p> <pre>access-list access-list-number permit source [source-wildcard]</pre>
Step 3	<p>Establish dynamic source translation, specifying the access list and pool defined in prior steps.</p> <pre>ip nat inside source list access-list- number pool name</pre>
Step 4	<p>Identify the inside interface.</p> <pre>interface type number ip nat inside</pre>
Step 5	<p>Identify the outside interface.</p> <pre>interface type number ip nat outside</pre>



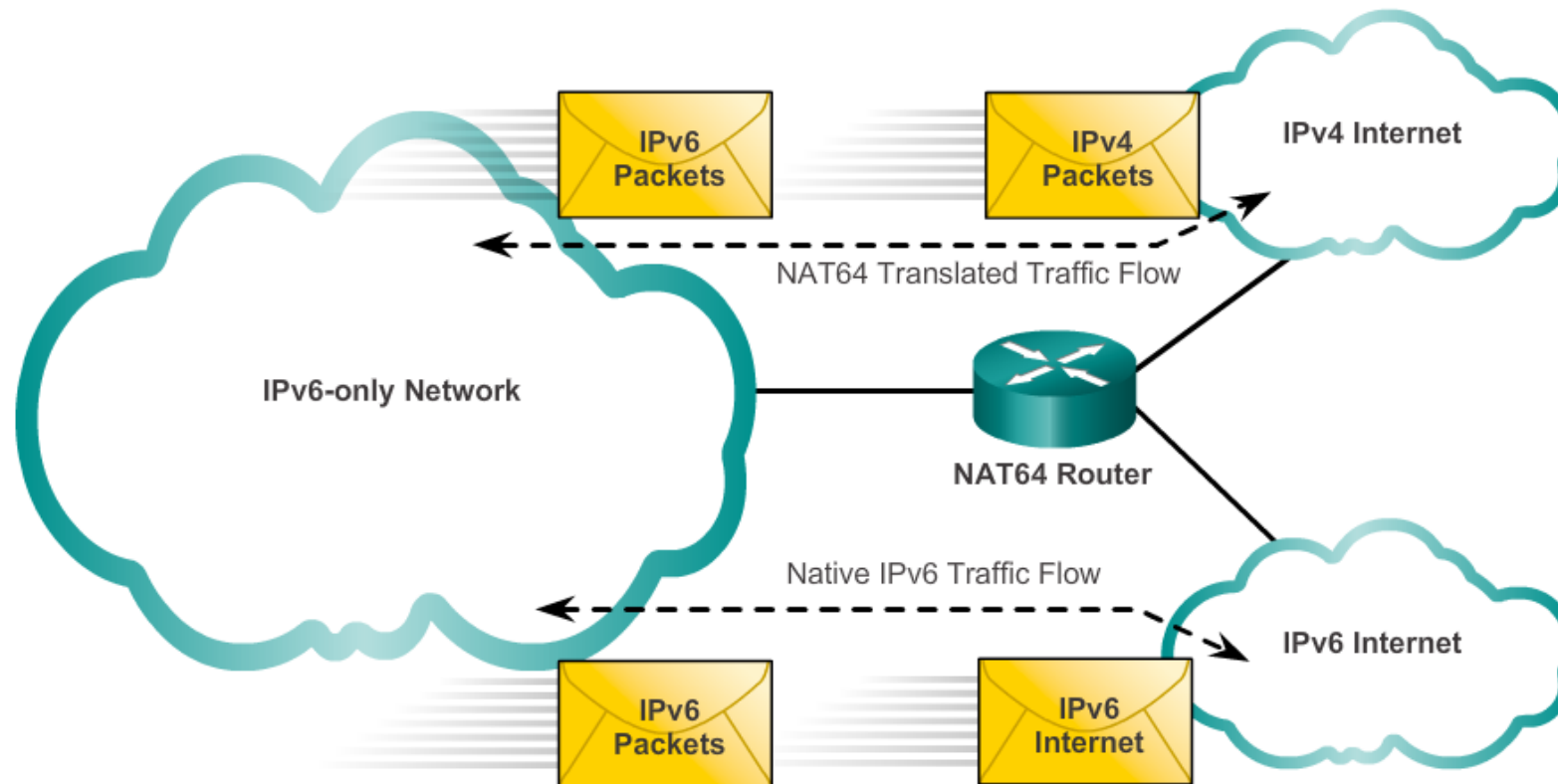


Verifying Dynamic NAT with show ip nat translations

```
R2# show ip nat translations
Pro Inside global      Inside local  Outside local  Outside global
--- 209.165.200.226    192.168.10.10 ---          ---
--- 209.165.200.227    192.168.11.10 ---          ---
R2#
R2# show ip nat translations verbose
Pro Inside global      Inside local  Outside local  Outside global
--- 209.165.200.226    192.168.10.10 ---          ---
      create 00:17:25, use 00:01:54 timeout:86400000, left
23:58:05, Map-Id(In): 1,
      flags:
none, use_count: 0, entry-id: 32, lc_entries: 0
--- 209.165.200.227    192.168.11.10 ---          ---
      create 00:17:22, use 00:01:51 timeout:86400000, left
23:58:08, Map-Id(In): 1,
      flags:
none, use_count: 0, entry-id: 34, lc_entries: 0
R2#
```

- NAT é uma solução para a escassez de endereços IPv4
- IPv6 com um endereço de 128 bits oferece 340 undecillion de endereços
- Não há um problema de limitação do espaço de endereçamento em IPv6
- IPv6 torna a tradução NAT público-privado do IPv4 desnecessária por projeto
- No entanto, o IPv6 implementa uma forma de endereços privados e é implementada de forma diferente do que acontece com IPv4

- IPv6 também utiliza NAT, mas num contexto muito diferente
- No IPv6, o NAT é usado para fornecer uma comunicação transparente entre IPv6 e IPv4
- NAT64 não se destina a ser uma solução permanente. Ele foi criado para ser um mecanismo de transição
- Network Address Translation - Protocol Translation (NAT-PT) foi outro mecanismo de transição para IPv6 baseado em NAT mas é agora obsoleto pelo IETF
- NAT64 é agora recomendado



Redes locais sem fios, incluindo configuração e segurança

- Numa rede com fios a mudança física de postos de trabalho de funcionários implica instalação de novas ligações à rede
- Para evitar estas alterações as redes sem fios são de cada vez mais frequentes, devido à sua grande flexibilidade e custos reduzidos
- WLAN (IEEE 802.11) são muitas vezes extensões da rede Ethernet (IEEE 802.3)
- WLAN usam frequências de rádio (radio frequencies - RF)
 - ✓ RF não estão limitadas a um cabo, o que torna os dados acessíveis a toda a gente que possa receber sinais RF, por esta razão as questões relativas a confidencialidade são aqui mais preocupantes
 - ✓ A utilização de RF semelhantes pode causar interferências entre elas
 - ✓ À medida que a distância à fonte de sinal aumenta o sinal pode mesmo deixar de ser detetado
 - ✓ A regulamentação das bandas de RF varia de país para país

- Os utilizadores da rede precisam de aceder à rede à medida que se deslocam
- Os utilizadores mudam frequentemente de localização dentro da instituição
- Nas WLAN cada cliente utiliza um adaptador wireless para ter acesso à rede através de um dispositivo wireless, tal como um router wireless ou um AP

➤ WPAN

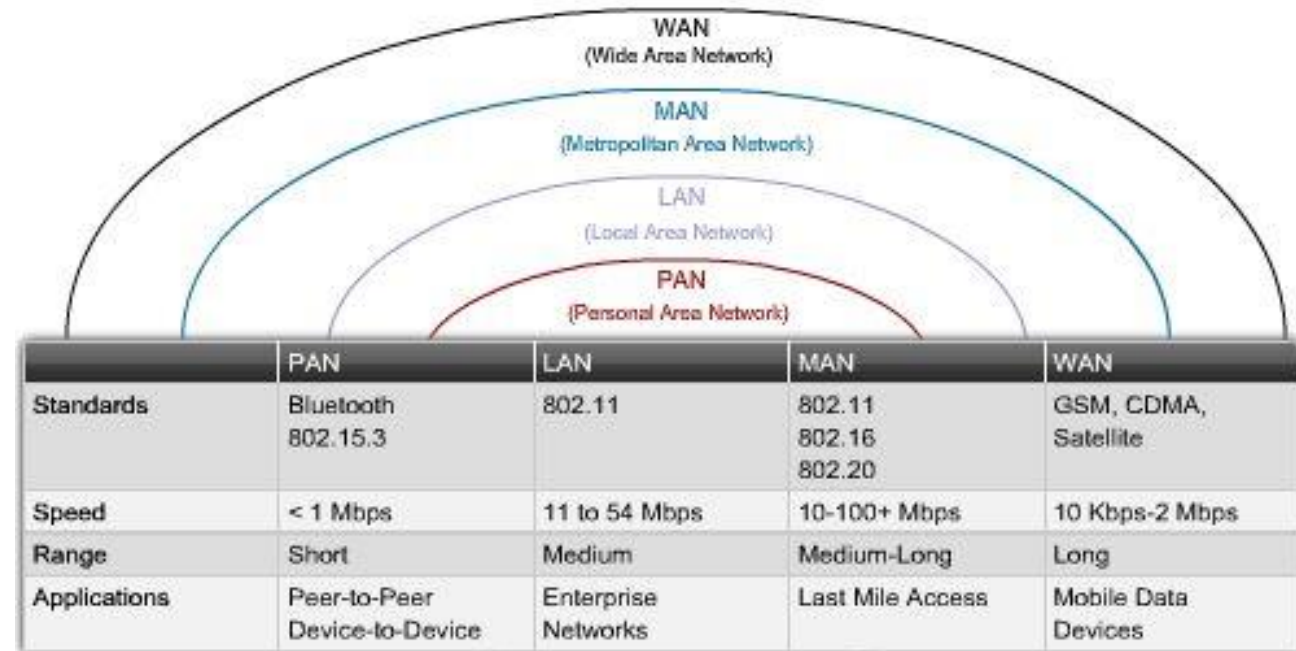
- ✓ É a rede sem fios mais pequena
- ✓ Usada para ligar vários periféricos tais como ratos, teclados PDAs a um computador

➤ WLAN

- ✓ Frequentemente usada para estender a rede LAN
- ✓ Usam RF de acordo com os padrões IEEE 802.11

➤ WWAN

- ✓ Oferecem cobertura de áreas extremamente grandes
- ✓ Um exemplo é a rede celular telefónica

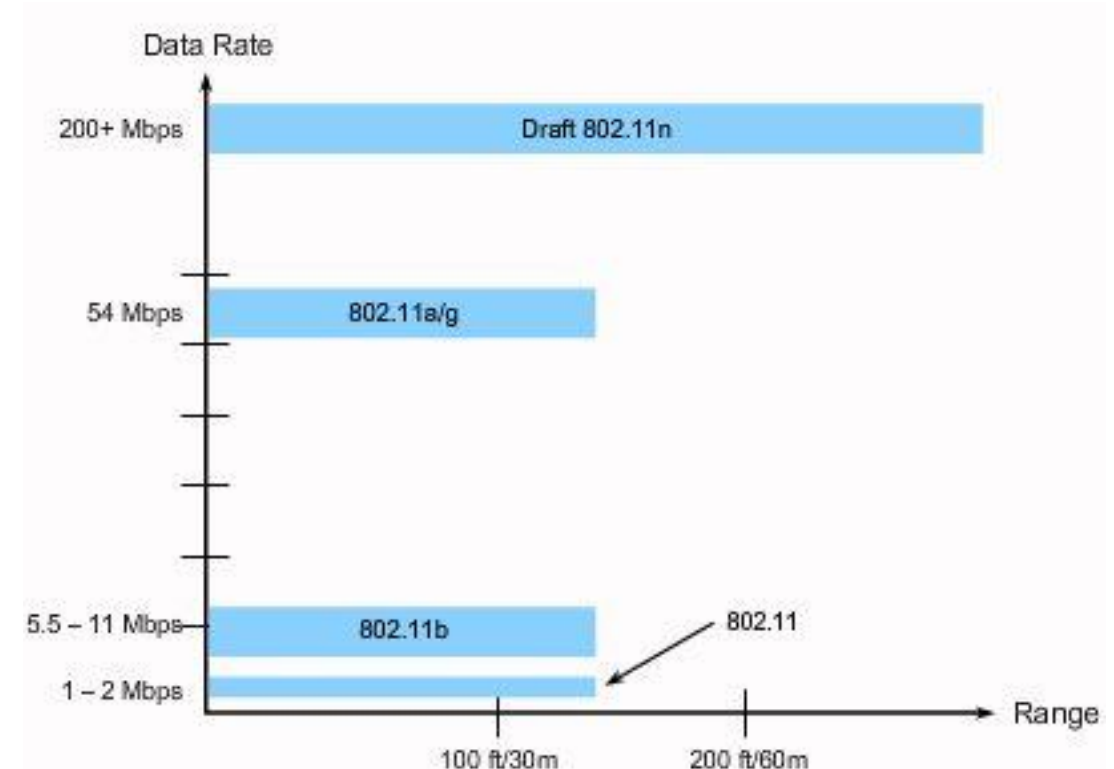


Comparing a WLAN to a LAN

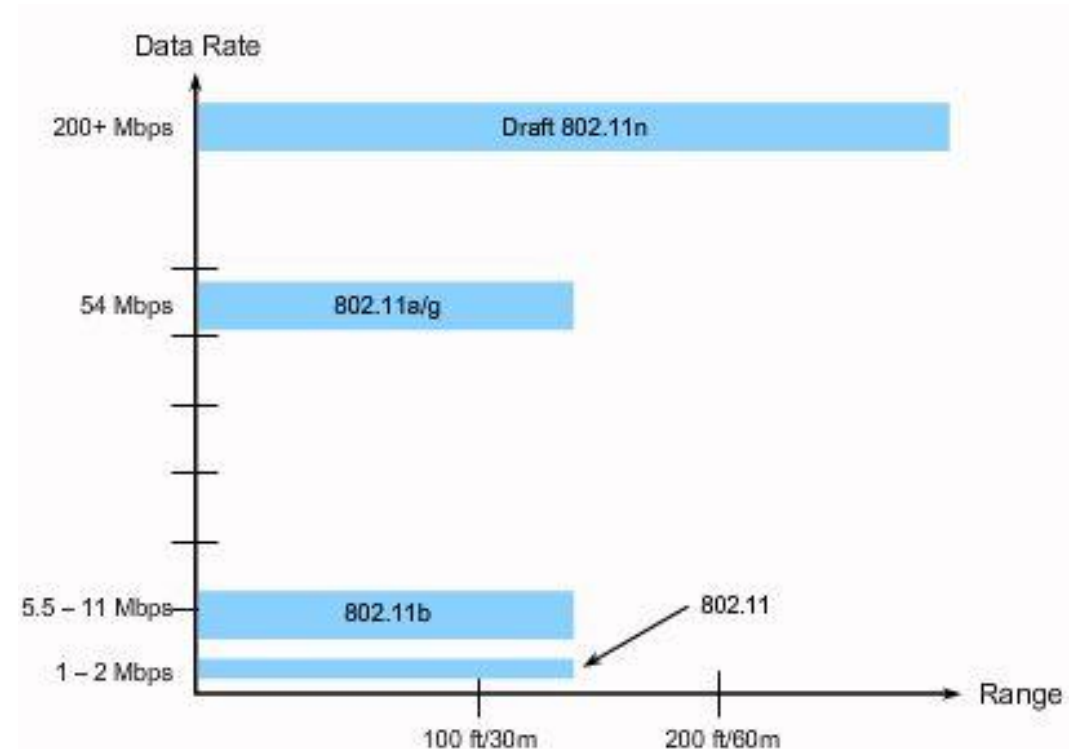
Characteristic	802.11 Wireless LAN	802.3 Ethernet LANs
Physical Layer	Radio Frequency (RF)	Cable
Media Access	Collision Avoidance	Collision Detection
Availability	Anyone with a radio NIC in range of an access point	Cable connection required
Signal Interference	Yes	Inconsequential
Regulation	Additional regulation by local authorities	IEEE standard dictates

- O formato dos quadros nas redes WLAN é diferente do formato dos quadros na rede Ethernet
- As normas especificam:
 - ✓ O espectro de RF usado
 - ✓ Taxa de transmissão
 - ✓ Como é que a informação é transmitida
 - ✓ Etc.
- A organização responsável por criar os padrões wireless é o IEEE
- Os padrões IEEE 802.11 são os padrões relativos à WLAN
- Wi-Fi Alliance
 - ✓ Responsável por garantir a interoperabilidade entre equipamentos wireless de diferentes fabricantes

- 802.11a
 - ✓ RF de 5 GHz
 - ✓ Não é compatível com RF de 2,4 GHz, ou seja com equipamentos 802.11 b/g/n
 - ✓ Alcance menor que o alcance da 802.11 b/g
 - ✓ Relativamente cara de implementar comparada com as outras
- 802.11b
 - ✓ Primeira tecnologia a usar os 2,4 GHz
 - ✓ Taxa de transmissão máxima de 11 Mbps
 - ✓ Alcance de aproximadamente 46 m indoors/96 m (300 ft) outdoors



- 802.11g
 - ✓ Tecnologia de 2,4 GHz
 - ✓ Taxa de transmissão máxima de 54 Mbps
 - ✓ Mesmo alcance que a 802.11 b
 - ✓ Compatibilidade com a 802.11 b
- 802.11n
 - ✓ A mais recente
 - ✓ Tecnologia de 2,4 GHz
 - ✓ Maior alcance e taxa de transferência
 - ✓ Compatível com equipamentos 802.11 g e 802.11 b

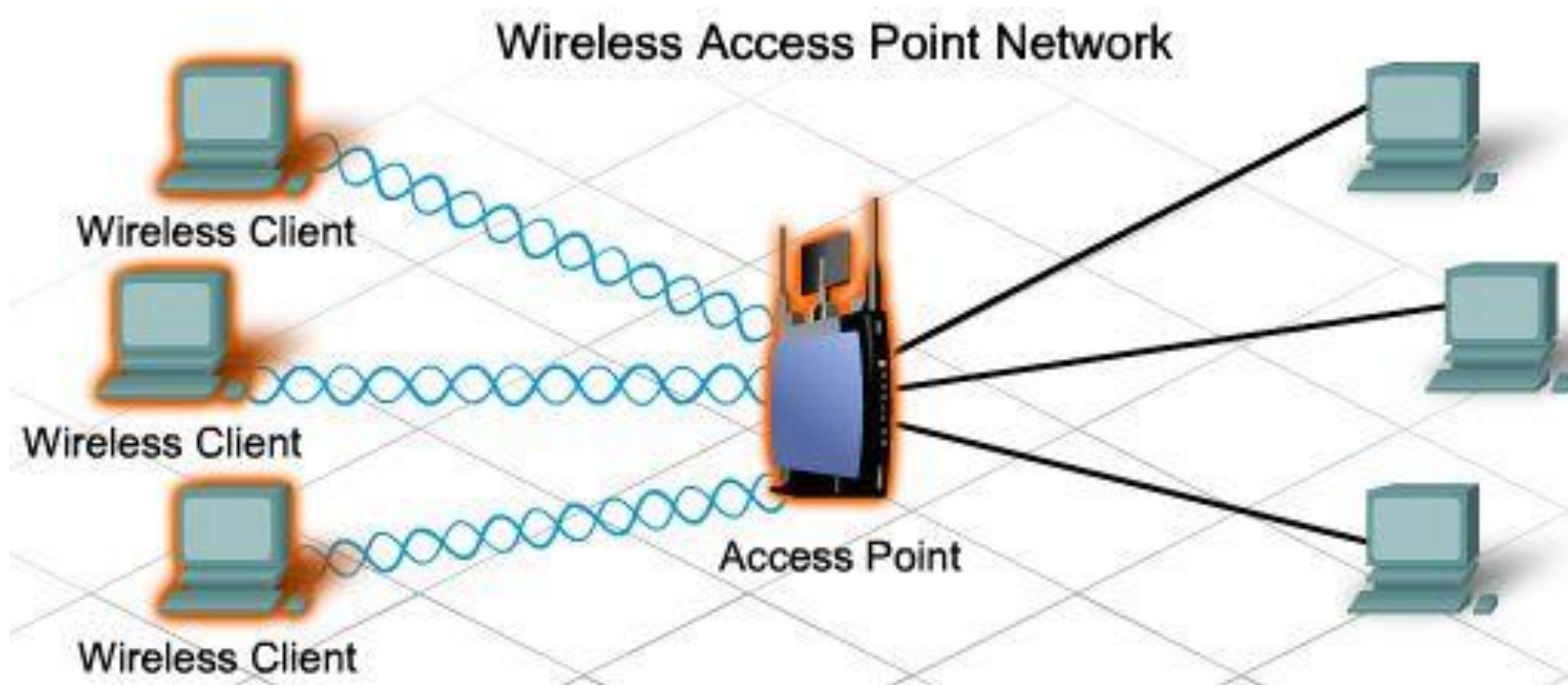


- É importante que todos os equipamentos na WLAN utilizem a mesma norma ou pelo menos uma compatível

Padrão IEEE	Velocidade Máxima	Frequência	Compatível com Versões Anteriores
802.11	2Mb/s	2,4GHz	—
802.11a	54Mb/s	5GHz	—
802.11b	11Mb/s	2,4GHz	—
802.11g	54Mb/s	2,4GHz	802.11b
802.11n	600Mb/s	2,4GHz e 5GHz	802.11a/b/g
802.11ac	1,3Gb/s (1300 Mb/s)	5GHz	802.11a/n
802.11ad	7Gb/s (7000Mb/s)	2,4GHz, 5GHz e 60 GHz	802.11a/b/g/n/ac

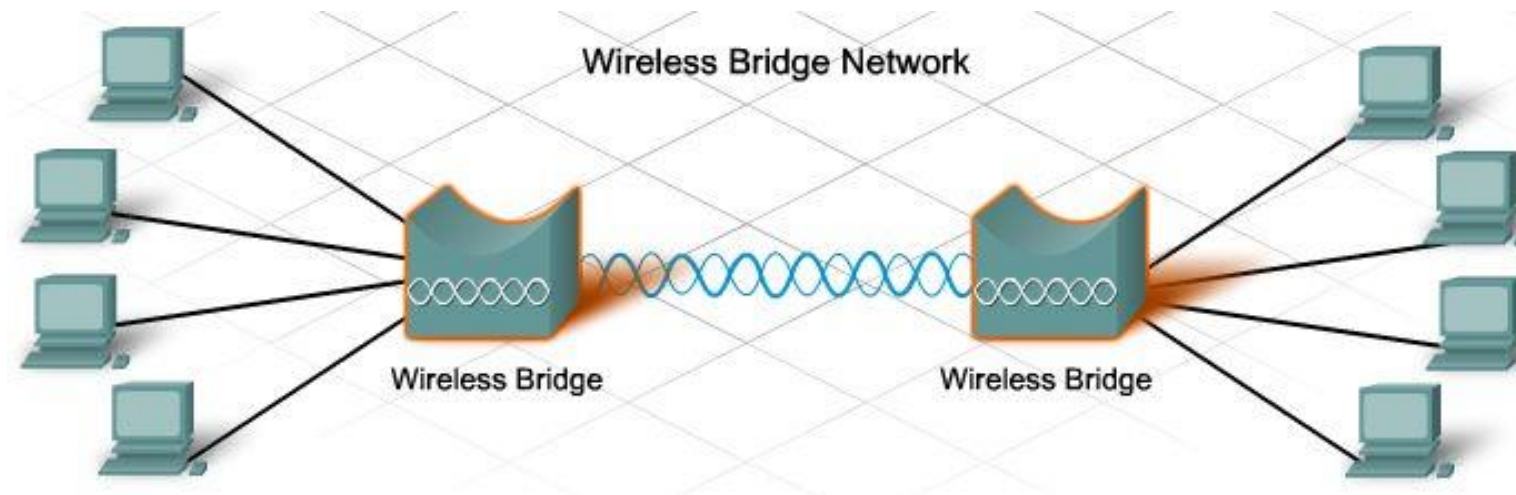
- Nas WLAN os clientes são ligados à rede através de um ponto de acesso (Access Point – AP) em vez de um switch
 - ✓ Em vez de um AP pode-se usar um router wireless

- Na figura pode ver-se um router wireless e 3 cliente wireless ligados a ele

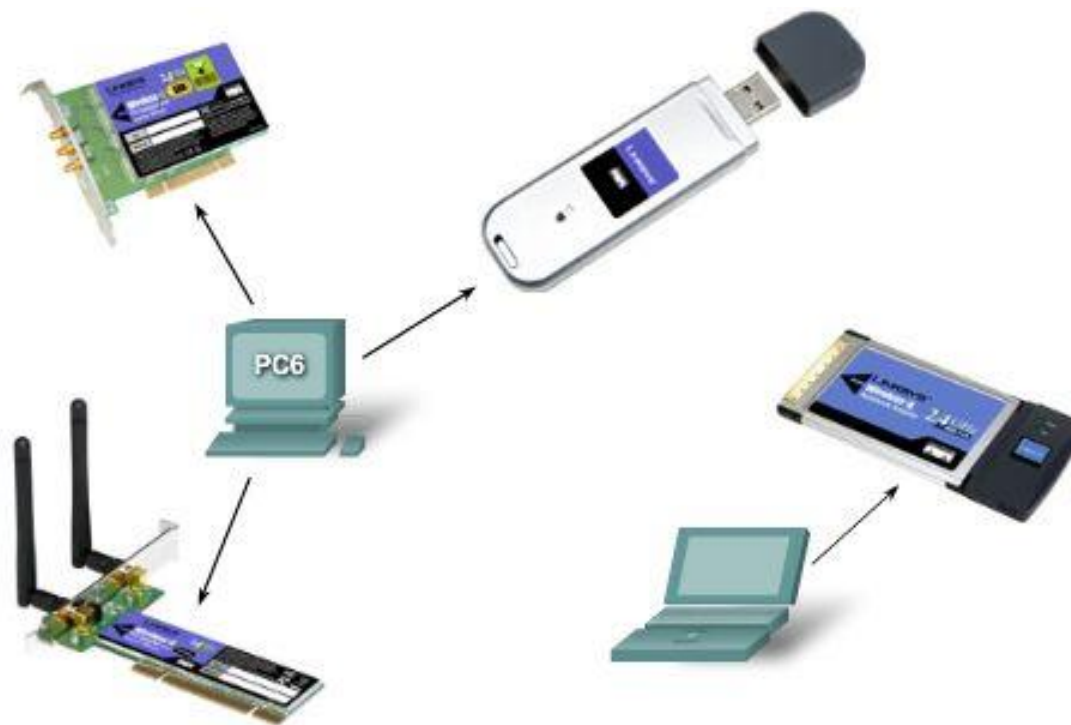




- Uma bridge wireless é usada para ligar duas redes através de uma ligação wireless
 - ✓ Grande alcance
 - ✓ Ligação ponto a ponto entre as redes
- Na figura podem ver-se duas bridges wireless ligadas uma à outra através de uma ligação sem fios



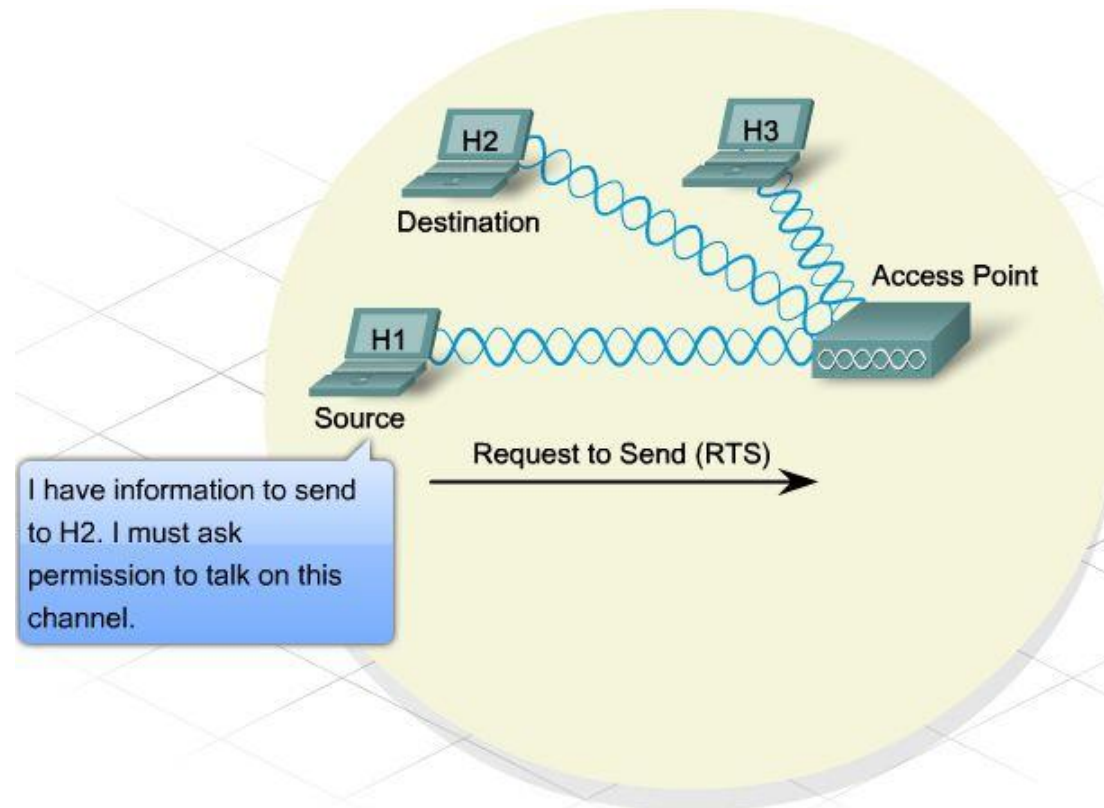
- Os clientes wireless possuem um NIC wireless
- Os cliente podem ser estacionários ou móveis
- Exemplos: Portáteis, Impressoras, projetores, PDAs, etc



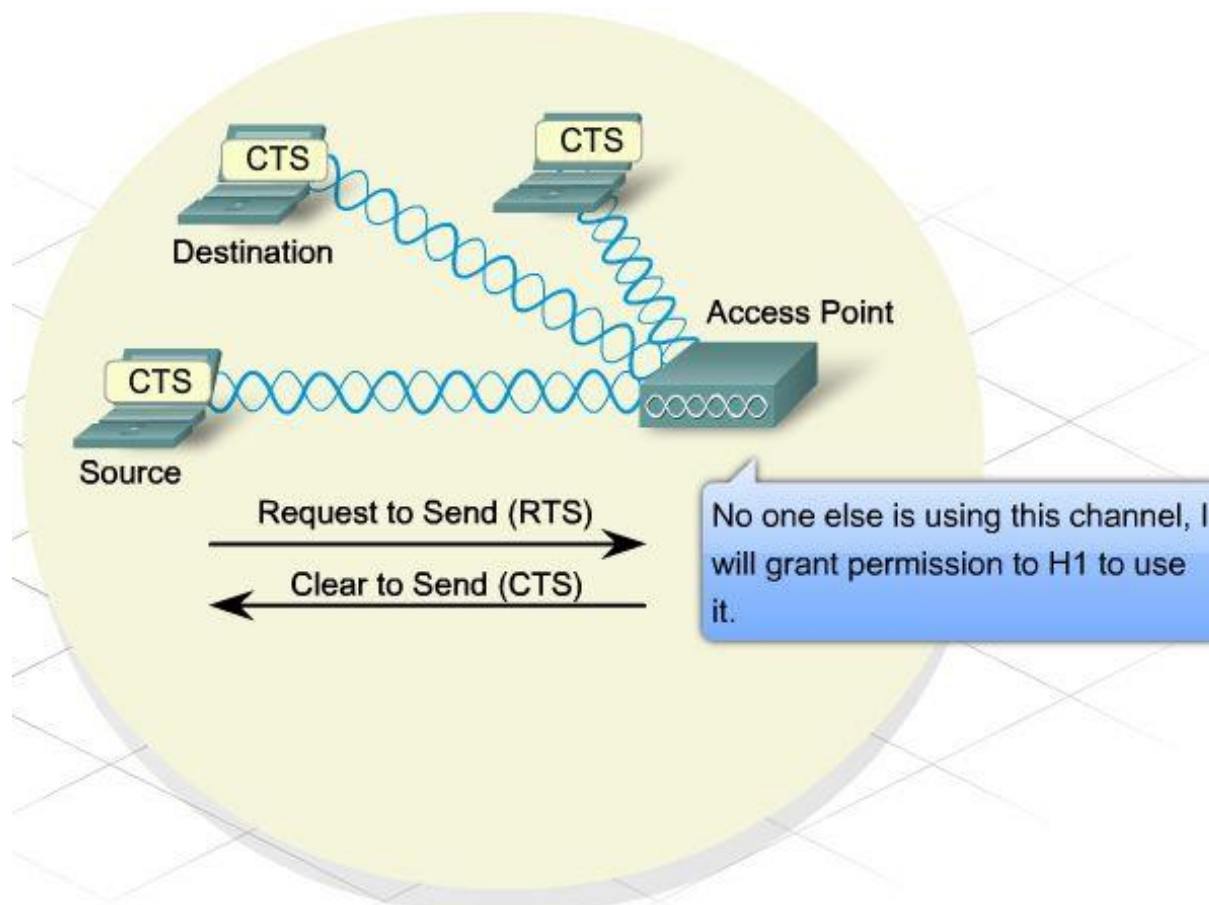
- Controla o acesso entre a rede wireless (sem fios) e a rede wired (com fios)
 - ✓ Controla quem pode comunicar e quando
 - ✓ Assegura que todos os clientes têm igual acesso ao meio
- Funciona como um conversor
 - ✓ Aceita quadros ethernet da rede wired e converte-os para quadros 802.11 antes de os transmitir na WLAN e vice versa
- A área de alcance de um AP é limitada, é conhecida como célula ou Basic Service Set (BSS)

- A ligação de equipamentos a uma rede wireless especifica é conseguido através da utilização de um Service Set Identifier SSID
 - ✓ É uma string alfanumérica
 - ✓ Enviado no cabeçalho de todos os quadros transmitidos na WLAN
 - ✓ Todos os equipamentos numa mesma rede wireless devem ser configurados com o mesmo SSID

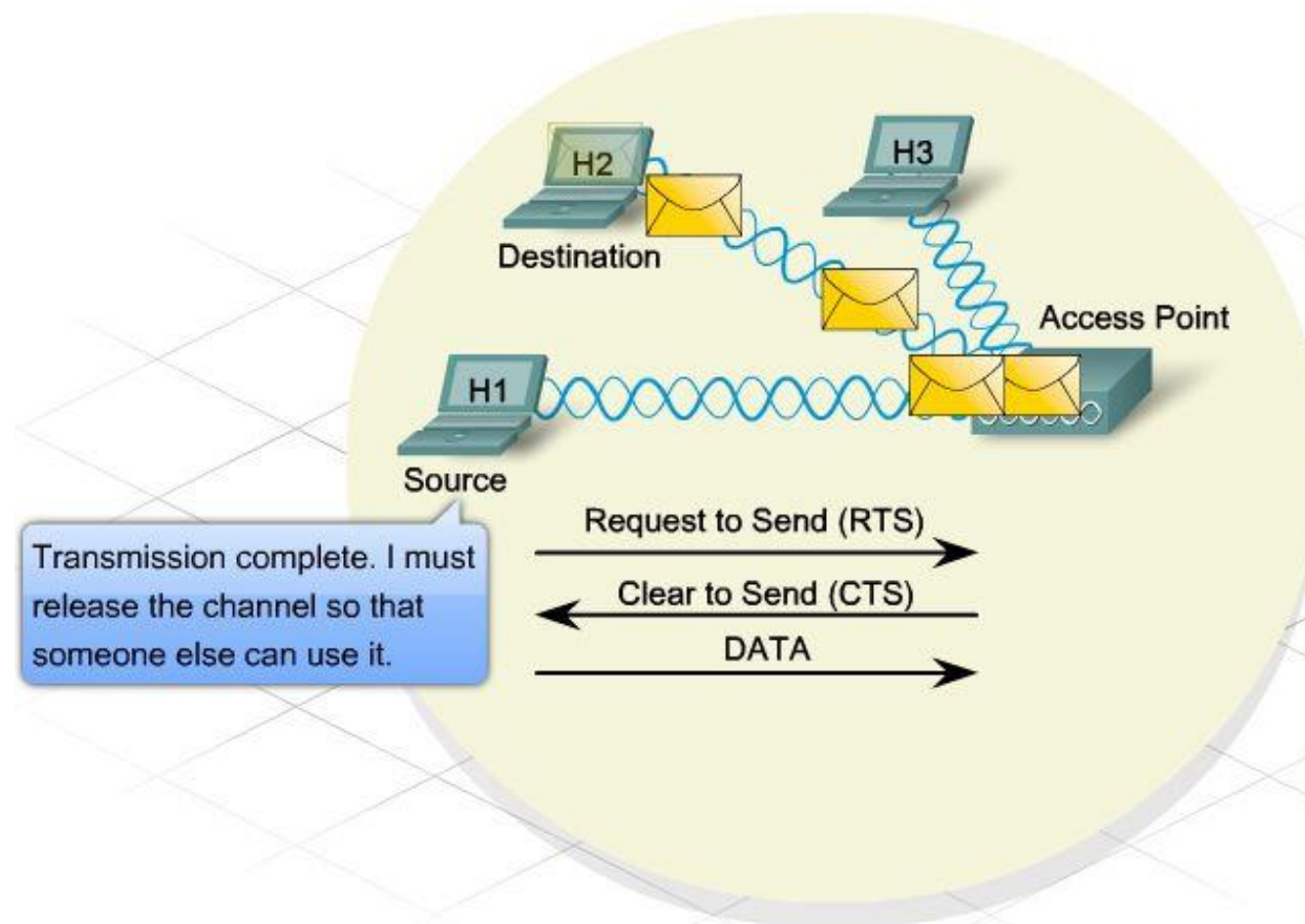
- Cliente pede permissão para emitir (RTS)



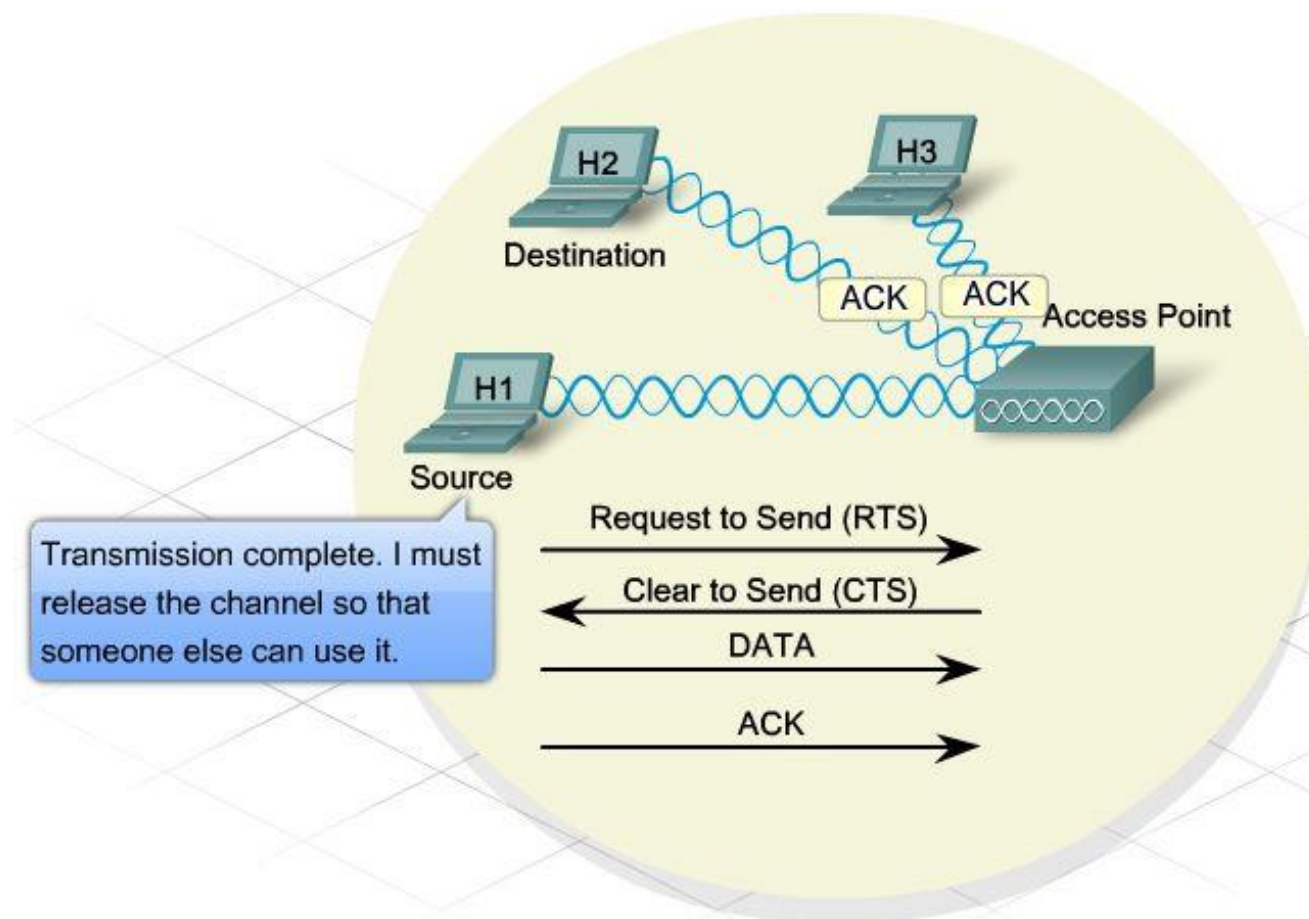
- O AP dá a permissão para emitir (CTS) e informa os outros clientes



- O cliente envia os dados para o AP que os retransmite para o destino



- Após o envio dos dados pelo cliente este sinaliza que vai deixar de emitir (ACK)

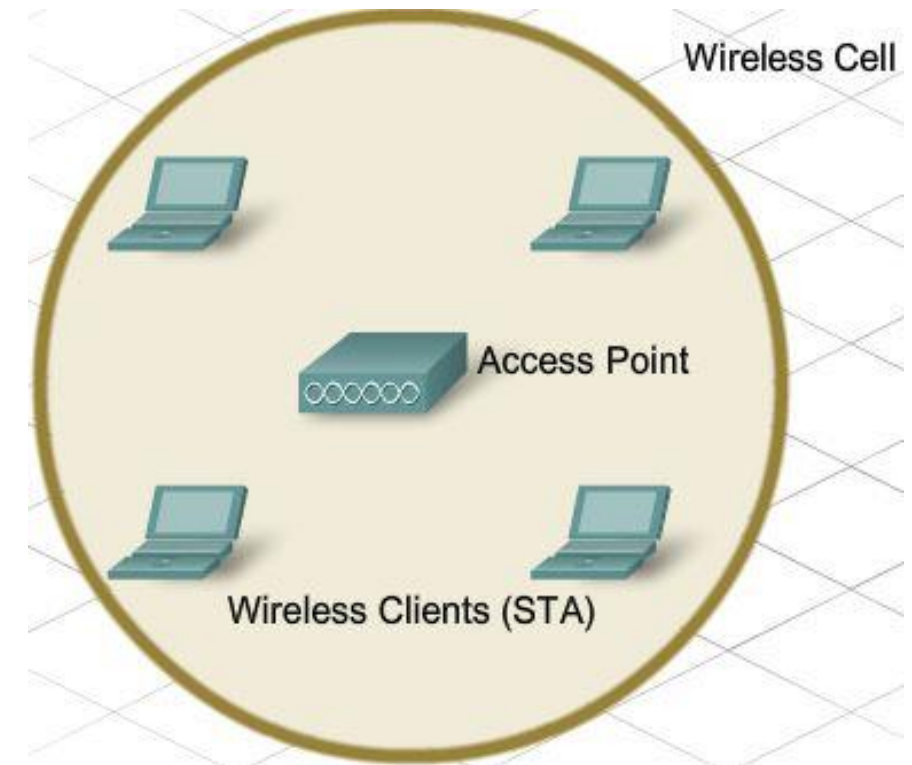


- Existem duas formas básicas de instalações wireless
 - ✓ Ad-hoc
 - ✓ Modo de infraestrutura

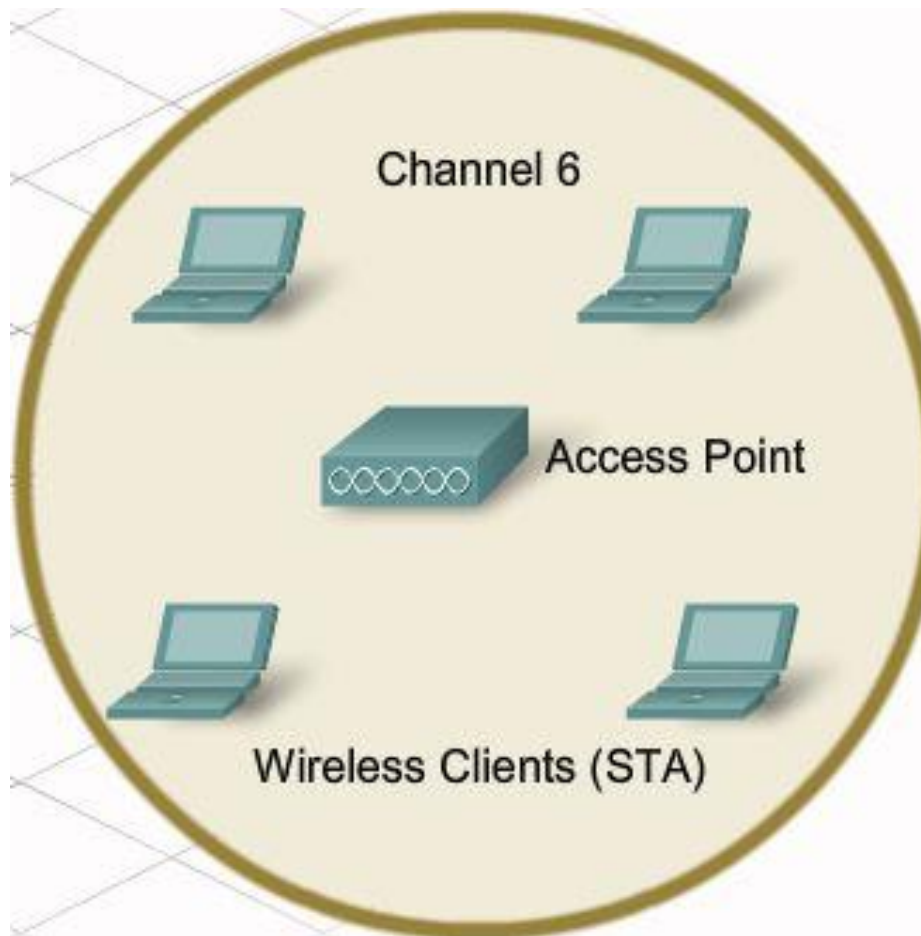
- É a forma mais simples de uma rede wireless ser criada
- Os clientes wireless são ligados numa rede peer-to-peer
 - ✓ Todos os clientes na rede são iguais
- Não inclui um AP
- A área coberta é designada por Basic Service Area (BSA)
- As redes Ad-hoc também são designadas por Independent Basic Service Set (IBSS)
- Usado em redes pequenas
- Ex.: troca de ficheiros entre clientes sem a necessidade de um AP



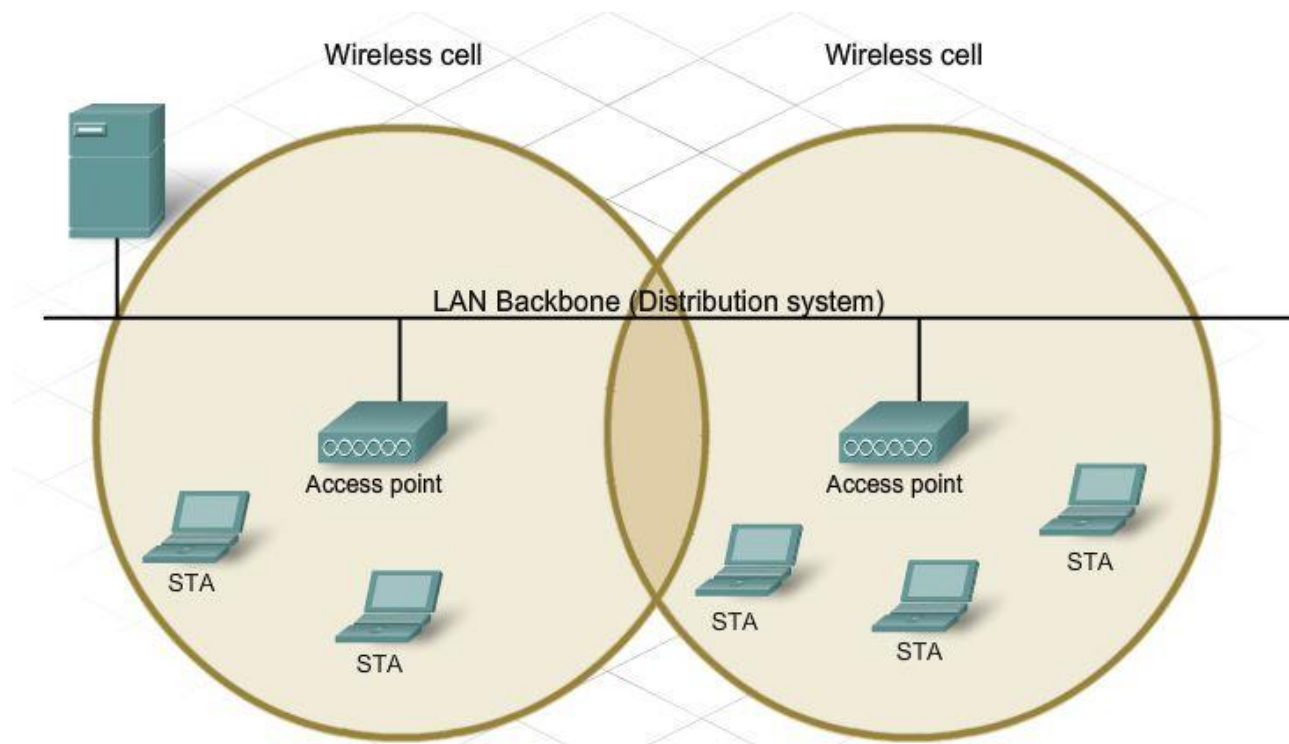
- As redes wireless, não pequenas, precisam de um equipamento que controle a comunicação na célula wireless
- O modo mais usado tanto em ambientes empresariais como domésticos
- Os clientes não comunicam diretamente uns com os outros
 - ✓ Para comunicar cada equipamento precisa de obter permissão do AP
- Estas redes também são designadas por Independent Basic Service Set (IBSS)
- A área de cobertura é conhecida como célula ou Basic Service Area (BSA)

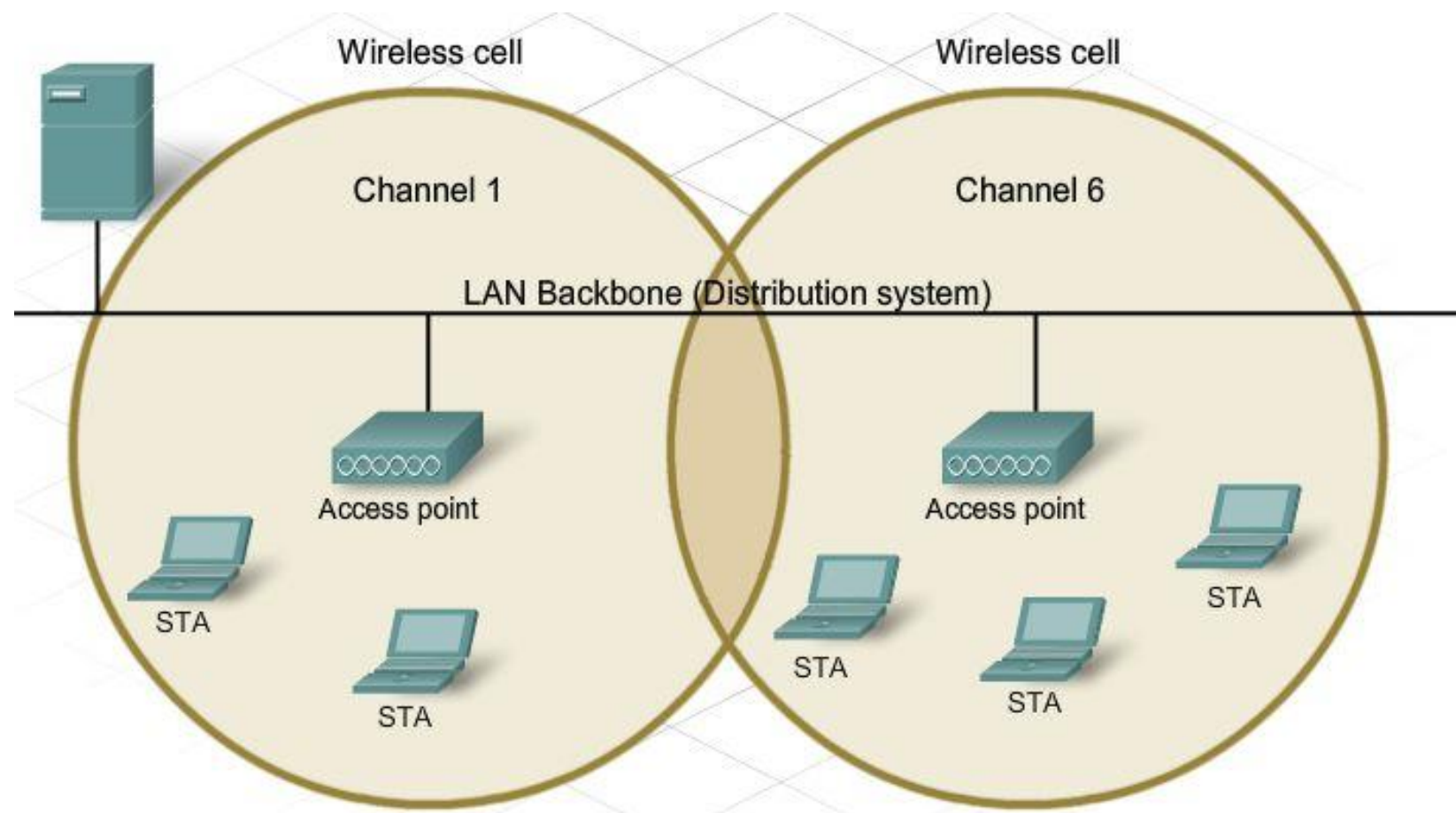


- Em cada célula é usado um canal

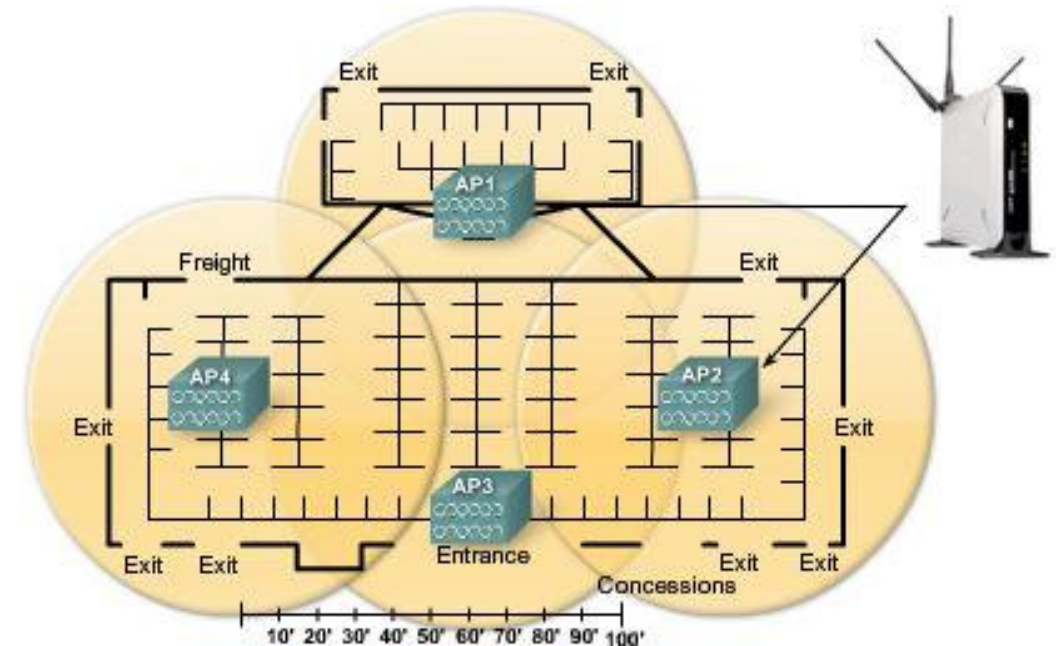


- Para expandir a área de cobertura de um BSS são ligados vários através de um Distribution System (DS)
 - ✓ Resulta num Extended Service Set (ESS)





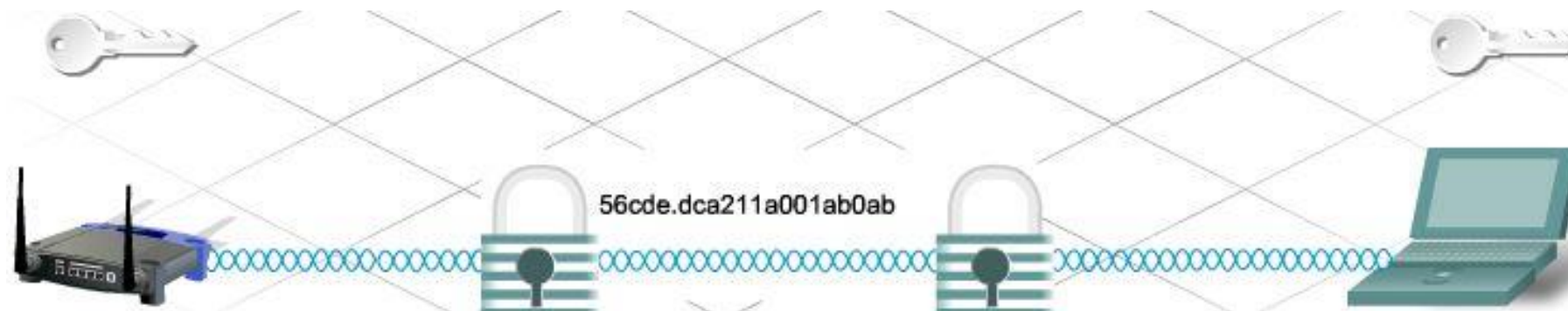
- Saber o número de utilizadores
- Área a abranger
- Taxas de transmissão esperadas
- Conhecer as especificações dos AP
- Para possibilidade de roaming é necessário:
 - ✓ Utilizar canais que não se sobreponham
 - ✓ Sobreposição das células de 10 a 15%
 - ✓ SSID comum



- Ameaças à segurança:
 - ✓ War driving
 - ✓ Crackers
 - ✓ AP malicioso (Rogue) – AP instalado pelos funcionários sem autorização

- Autenticação é uma forma de controlar o acesso a uma WLAN
- A autenticação permite limitar o acesso à rede aos equipamentos que forneçam um determinado conjunto de credenciais
- Existem 3 tipos de autenticação
- Autenticação Aberta
 - ✓ PSK (Pre-Shared Keys)
 - ❖ Chaves partilhadas
 - ✓ EAP (Extensible Authentication Protocol)
 - ❖ Chaves geridas centralmente

- Embora a autenticação possa impedir um atacante de ligar-se à rede não o impedirá de ver os dados que estão a ser transmitidos
- Para evitar que os dados transmitidos possam ser compreendidos é necessário usar encriptação
- Ao longo do tempo foram propostos diversos mecanismos/algoritmos de encriptação simétricos – utilização da mesma chave para encriptar e descriptar
 - ✓ WEP
 - ✓ TKIP
 - ✓ AES



- Inicialmente WEP (Wired Equivalent Protocol) foi desenvolvido para tentar fornecer a mesma segurança nas WLAN que existe nas redes com fios
 - ✓ No entanto o protocolo era vulnerável (facilmente quebrável)
- Para evitar as limitações mais graves do WEP, e enquanto não foi desenvolvido o protocolo 802.11i (WPA2) foi criado um novo protocolo, TKIP, que usa o algoritmo de encriptação usado no WEP mas evita algumas das suas vulnerabilidades
 - ✓ Suporta mudança periódicas de chaves WEP
 - ✓ Inclui uma verificação de integridade do pacote na parte encriptada
- Finalmente foi desenvolvido o protocolo 802.11i (WPA2) que usa o algoritmo de encriptação AES (Advanced Encryption Standard) muito mais forte

- A utilização dos mecanismos de encriptação TKIP e AES são denominados, geralmente pelos nomes WPA (Wifi Protected Access) e WPA2, respetivamente
- Num ambiente doméstico estes algoritmos são geralmente usados num contexto de chave partilhada (PSK ou PSK2)
 - ✓ WPA–PSK implica normalmente a utilização de TKIP
 - ✓ WPA2–PSK implica normalmente a utilização de AES
- Para evitar os problemas logísticos da gestão das chaves partilhadas as empresas geralmente usam EAP para tratar do processo de gestão das chaves
 - ✓ De acordo com o protocolo 802.1x
 - ✓ Embora quer WEP quer TKIP possam ser usados, atualmente é mais comum usar AES com EAP naquilo a que se chama WPA2 empresarial

- Medidas básicas
 - ✓ Alterar os valores definidos por omissão
 - ❖ SSID, username e password
 - ✓ Desativar a difusão do SSID
 - ✓ Configurar limitação por endereços MAC
- Medidas avançadas
 - ✓ Configurar autenticação
 - ✓ Configurar encriptação
 - ✓ Configurar filtragem por tipo de tráfego

