Endereçamento IP

Cada máquina na Internet possui um ou mais endereços de rede que são únicos, ou seja, não pode haver dois endereços iguais. Este endereço é chamado de **número Internet**, **Endereço IP** ou ainda **número IP**.

Atualmente existem dois tipos de endereços IP: o IPv4, que foi inicialmente introduzido em 1º de janeiro de 1983, consistindo de um número de 32 bits, sendo comumente representado por quatro números decimais separados por pontos, como 143.54.8.11. Este endereço pode ser estruturado de maneiras diferentes, usando uma parte para designar uma rede e as demais para designar os computadores naquela rede. O Ipv6 foi introduzido em 1999, e consiste de uma série de 128 bits representados em hexadecimal, como por exemplo:

3ffe:6a88:85a3:08d3:1319:8a2e:0370:7344.

Quem gerencia a numeração IP no mundo?

Tanto o espaço de endereçamento do IPv4 como do IPv6 são delegados por um organismo central da Internet, chamado IANA (*Internet Assigned Numbers Authority* - http://www.iana.org), que é subsidiado pelo governo. Para apoio na distribuição de números, o IANA conta com quatro regiões mundiais:

• LACNIC (*Latin-American and Caribbean IP Address Registry*) – América Latina e algumas ilhas do Caribe;

• ARIN (*American Registry for Internet Numbers* – http://www.arin.net), responsável pela América do Norte, Caribe e África abaixo do Sahara;

• RIPE (*Reséau IP Européens* – http://www.ripe.net), responsável pela Europa, parte da África e países do oriente médio;

• APNIC (*Asia-Pacific Network Information Center* – http://www.apnic.net), responsável pela ásia e pacífico.

Para se ter uma idéia da distribuição atual mundial de endereços Ipv4, pode-se consultar o endereço http://www.iana.org/assignments/ipv4-address-space, do IANA. Nesse local pode-se verificar os números delegados para cada região. Por exemplo, o LACNIC possui os endereços 200/8 (novembro de 2002)) e 201/8 (abril de 2003). Desde outubro de 1998 existe também uma entidade chamada ICANN (*Internet Corporation for Assigned Names and Numbers* – http://www.icann.org), que é um órgão privado responsável por entrega de nomes de domínio e números IP. Ele supostamente deveria estar gradativamente tomando as funções do IANA. A empresa que necessita um número IP deve procurar seu provedor, que, por sua vez, deve procurar o representante da sua região (no nosso caso o LACNIC) ou um provedor de *backbone*.

Correspondência número IP - nome:

Além de números IP, cada máquina na Internet está associada com um nome que a distingue das outras. Esse nome é composto de caracteres separados por ponto, como www.fiat.com.br, formando o Fully Qualified Domain Name (FQDN) de cada máquina. Neste caso, **"www"** é o nome da máquina e **"fiat.com.br"** é o domínio ao qual esta máquina pertence. Os caracteres após o último ponto ("**com"** no exemplo anterior), indicam o tipo da organização. Existem vários tipos que diferenciam as entidades entre si, entre eles pode-se citar:

com - instituição comercial ou empresa (ex: apple.com - Apple Computers);
edu - instituição educacional (ex: berkeley.edu - Universidade de Berkeley). No Brasil, é comum as universidades não possuírem sufixo ".edu";
gov - órgão do governo (ex: nasa.gov - NASA);
mil - organização militar (ex: nic.ddn.mil - departamento de defesa dos EUA);
net - gateways e hosts administrativos de uma rede (ex: uu.net);
org - organizações privadas que não se enquadram nas outras categorias (ex: eff.org)

Problemas relacionados com o crescimento da Internet:

- **Eventual exaustão do endereçamento IPv4**: Essa exaustão teve uma folga com a definição de números de intranet e utilização de NAT (*Network Address Translator-RFC 1631*), bem como a utilização de *proxy* nas empresas.

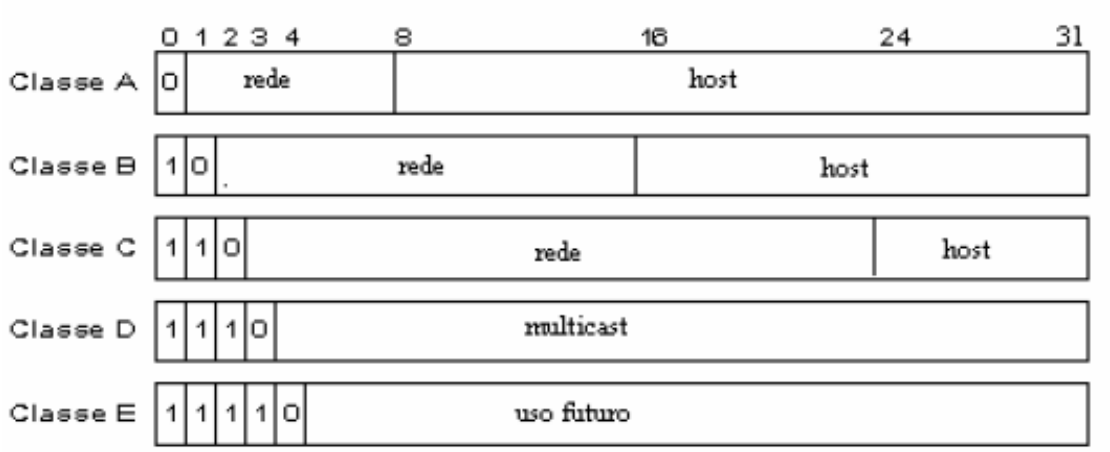
- Problemática de rotear tráfego em um número crescente de redes (tabelas de roteamento)

- **IPv4**: endereços de 32 bits, que consiste num total de 2^{32}, ou 4.294.967.296 endereços disponíveis. Parece bastante, mas ele é mal distribuído na visão *classful* de endereços. A **exaustão** dos endereços IPV4 está prevista para 2014.

- **Tabelas de roteamento**: Continuando o crescimento de forma desorganizada, haveria um excesso de entradas nas tabelas de roteamento.

Endereçamento Classful

Cada computador ligado à Internet deve possuir um endereço IP único, a fim de que os roteadores saibam como encaminhar um pacote a esse local, sem confusão de rotas. Entretanto, a numeração não pode ser aleatória, pois acarretaria um excesso de entradas nas tabelas de roteamento. Para contemplar esse problema, no princípio da Internet definiu-se a utilização do endereçamento *classful*, agrupando hosts em classes de redes conforme pode ser visto na tabela a seguir:



	Número de redes	Hosts por rede	Valor do 1º octeto
Classe A	126	16.277.214	1-126
Classe B	16.384	65.534	128-191
Classe C	2.097.152	254	192-223

Observe que o endereço é auto-contido, ou seja, não precisa máscara. Por exemplo, se os primeiros dois bits de um endereço IP são 1-0, então se trata de um endereço classe B, e o ponto de divisão entre rede (empresa responsável pelo número) e *host* (cada máquina dentro da empresa) é entre o 15º e o 16º bit. Esse conceito simplificado de roteamento foi usado no princípio da Internet, pois os protocolos de roteamento originais não suportavam máscara.

Assim, uma grande empresa recebia um endereço classe A (como por exemplo a Apple.com (17.x.x.x) e Xerox.com (13.x.x.x)), significando para um roteador que um pacote contendo o número IP iniciando com "17" deveria ser roteado para chegar na "rede" da Apple. Internamente à empresa, TODOS os computadores (*hosts*) deveriam ser configurados iniciando com o número "17" (e.g. 17.1.32.7, ou 17.150.21.3), o que permitia um total de aproximadamente 16 milhões de máquinas (2^{24}). Isso pode ser constatado na tabela acima, onde existem 24 bits para "hosts" no endereçamento classe A. Obviamente isso acarreta um desperdício de endereços, pois nenhuma empresa possui 16 milhões de máquinas. Supondo que a Apple possuísse 100.000 computadores, ainda assim haveria um desperdício de 15.900.000 endereços IP válidos.

Uma empresa de médio porte recebia uma classe B (como por exemplo a UFRGS (143.54.x.x), USP (143.107.x.x) e IBM (129.42.x.x)). Dessa forma, como pode ser visto na tabela acima, haveria 16 bits para determinar a "rede" da empresa (utilizada pelo roteador) e 16 bits para configurar máquinas dentro da empresa. Uma empresa do porte da USP possui aproximadamente 20.000 máquinas, e acarreta um desperdício de mais de 40.000 endereços.

Uma empresa de pequeno porte recebia uma classe C, significando que teria até 256 endereços para configurar as máquinas internas à empresa.

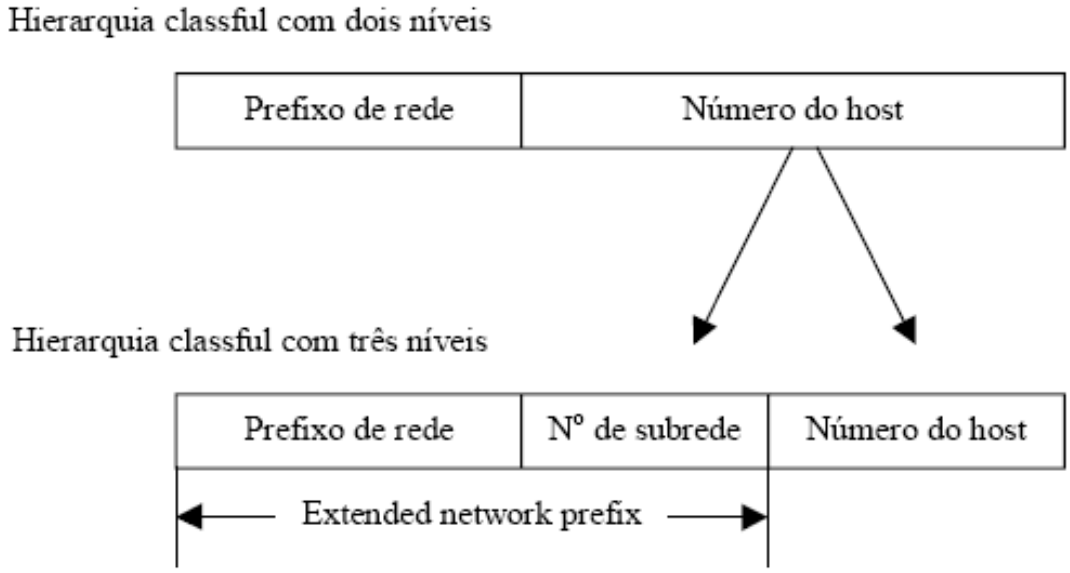
Inserir exercícios de conversão de binário x decimal e vice-versa

Conceito de SUBREDES

Como foi visto anteriormente, a utilização do endereçamento *classful* provoca um desperdício de endereços, além de uma má distribuição dos números IP. Para melhorar esse sistema, foi definido na RFC 950 (1985) um processo padrão para dividir uma classe A, B ou C em pedaços menores, utilizando subredes. As melhorias do novo sistema são:

a) Diminui tabelas de roteamento na Internet;
b) Administradores podem ter autonomia na criação de subredes internas à empresa (antes necessitavam requisitar outro número de rede).

A figura a seguir mostra a idéia básica de subredes.



As sub-redes melhoram a eficiência do endereçamento de rede. A adição de sub-redes não altera a forma como o mundo externo percebe a rede, mas dentro da organização, há uma estrutura adicional. De um ponto de vista do endereçamento, as sub-redes são a extensão de um número de rede. Os administradores de rede determinam o tamanho das sub-redes com base nas necessidades de expansão de suas organizações. Os dispositivos de rede usam as máscaras de sub-redes para identificar que parte do endereço é da rede e que parte representa o endereçamento de host.

Uma máscara de subrede é do tipo **255.255.255.0.** Como se pode notar, o valor máximo para cada um dos campos é 255 (todos os bits 1) e o mínimo é 0 (todos os bits 0). Uma máscara de subrede obrigatoriamente deve ter valores máximos seguidos de valores mínimos. Assim sendo, **0.255.0.255** não é uma máscara de subrede válida.

A máscara de subrede serve para extrair a identificação da rede do endereço IP, através de uma operação "AND" binária bit a bit. Por exemplo, vamos considerar o endereço de um host 128.7.254.12 – a máscara de subrede padrão da classe B é 255.255.0.0. Assim, teríamos a seguinte operação:

10000000.00000111.11111100.00001100 (128.7.254.12)

"AND"

11111111.11111111.00000000.00000000 (255.255.0.0)

10000000.00000111.00000000.00000000 (128.7.0.0)

O "extended network prefix" apresentado na figura anterior é identificado pela máscara de subrede, e forma a nova notação de endereçamento utilizada atualmente – o "/x" – o qual representa o número de bits "1" da máscara de subrede (ou bits de rede). Por exemplo, uma classe A tradicional é um /8; uma classe B é um /16 e uma classe C é um /24. Assim, por exemplo, uma máscara "/24" é equivalente a "11111111.11111111.11111111.00000000" ou, em decimal, "255.255.255.0". Por exemplo, um endereço de rede 143.54.8.11 com máscara 255.255.255.0 pode ser expresso como 153.54.8.11/24.

- Endereço base, broadcast e default gateway

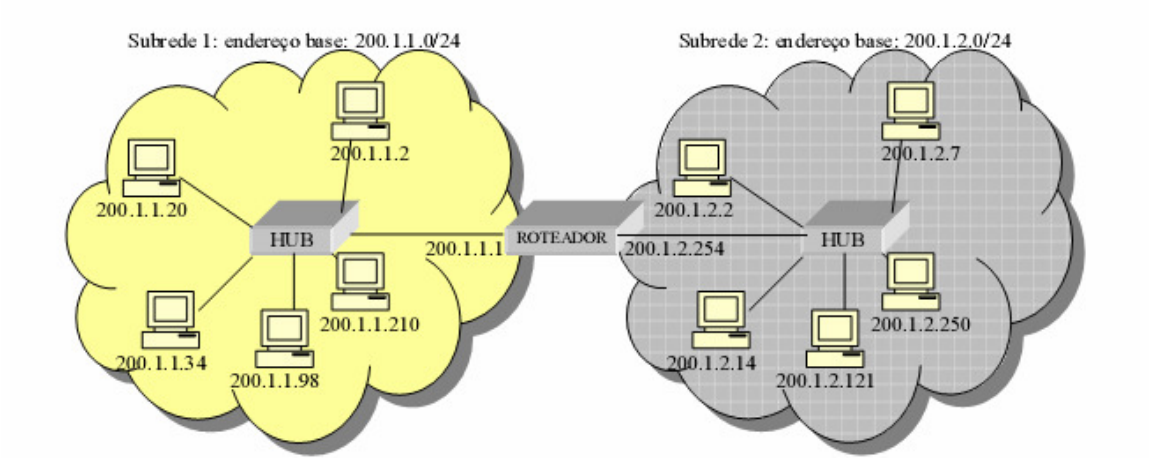
Para configurar uma máquina numa subrede, é necessário entender algumas definições, como subrede, endereço base, endereço de broadcast e default gateway.

Subrede: conjunto de endereços que contém o mesmo endereço base. Na figura a seguir, existem duas subredes, uma com o endereço base 200.1.1.0 e outra com o endereço base 200.1.2.0;

Endereço base: é o endereço que representa a subrede, e é obtido efetuando-se um "AND" entre o número IP e a máscara da subrede. Por exemplo, qualquer IP da subrede 1 gera o mesmo endereço base: "200.1.1.2 AND 255.255.255.0=200.1.1.0"; "200.1.1.210 AND 255.255.255.0=200.1.1.0", e assim por diante. Esse endereço é reservado e não pode ser utilizado para configurar máquinas;

Endereço de broadcast: é o último endereço da subrede, ou seja, quando todos os bits do endereço IP são iguais a "1". Por exemplo, o endereço broadcast da subrede 1 é 200.1.1.255. Esse endereço é reservado e não pode ser utilizado para configurar máquinas;

Default gateway: é configurado em cada máquina e serve para informar qual o endereço IP do roteador.

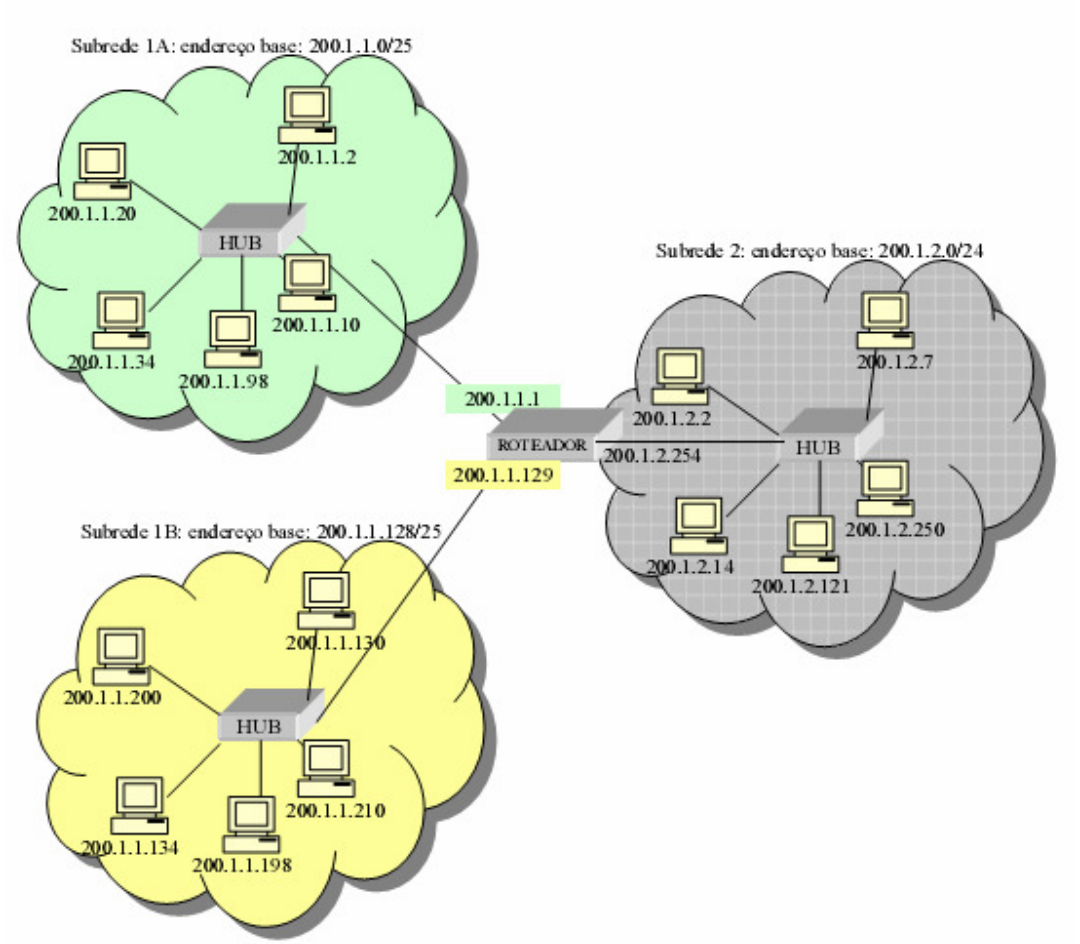


Percebe-se, através das explicações anteriores, que o tamanho da subrede (número máximo de máquinas que podem ser configurados na subrede) é dado pelo número de zeros da máscara de rede. Quanto maior o número de zeros, maior o número de máquinas. Assim, uma rede "/24" possui 8 bits "0", e gera um tamanho de 254 endereços (2 elevado a oito -2) pois o endereço base e o endereço de broadcast são reservados.

Criar uma subrede significa adicionar bits "1" à máscara padrão. Supondo que fosse necessário subdividir a subrede 1 da figura anterior em duas outras subredes (subrede 1A e subrede 1B), como mostra a figura a seguir, seria necessário alterar a máscara para um "/25" (11111111.11111111.11111111.10000000). Observe que são 7 "zeros", e o tamanho da subrede passa a ser de um máximo de 128 endereços. Conseqüentemente, a configuração ficaria:

Subrede 1A: endereço base: 200.1.1.0; endereço de broadcast: 200.1.1.127, máscara: "/25", ou 255.255.255.128.

Subrede 1B: endereço base: 200.1.1.128; endereço de broadcast: 200.1.1.255, máscara: "/25", ou 255.255.255.128.



* obs.: a máscara de subrede, além de extrair o número da rede de um endereço IP, nos diz número máximo de hosts que pode haver nessa rede.

Range de IPs livres para Intranet (RFC 1918)

Para facilitar a configuração de números IP internamente à empresa, definiu-se uma numeração destinada especificamente para uso em Intranets. Esse conjunto de números IP, visto a seguir, é conhecido como IP falso, ou IP de intranet, ou ainda IP interno;

. 10.0.0.0 ate 10.255.255.255 para Classe A

. 172.16.0.0 ate 172.31.255.255 para Classe B

. 192.168.0.0 ate 192.168.255.255 para Classe C

* A classe A 127 é destinada para o endereço de loopback (127.0.0.1)

Assim, internamente à empresa, pode-se utilizar um endereço tipo "10.x.x.x", porém, para se efetuar a conexão na Internet "verdadeira", deve-se utilizar um conjunto de números IP válido, delegado para a empresa pelo provedor que, por sua vez, conseguiu esses números da entidade responsável no País ou região (LACNIC, por exemplo).

A conversão entre o número IP "falso" e o número IP "verdadeiro" é feita normalmente através de um software de NAT (Network Address Translator – RFC 2663) instalado no roteador de borda da empresa.

- Exercícios de Subredes:

1. Verifique se os seguintes endereços IP pertencem à mesma rede:
    a. 200.136.16.32/27 e 200.136.16.31/27
    b. 192.168.0.10/25 e 192.168.0.107/25
    c. 192.168.0.129/28 e 192.168.0.144/28
    d. 200.112.16.4/26 e 200.112.16.65/26
    e. 10.1.170.240/9 e 10.100.7.254/9
    f. 90.78.200.145/12 e 90.65.150.82/12
    g. 10.150.8.0/16 e 10.150.240.8/16
    h. 10.17.25.188/15 e 10.17.228.3/15

2. Uma organização recebeu o número de rede 156.1.1.0/24, e precisa definir 6 subredes. A maior subrede deve suportar 25 hosts. Defina o seguinte:
    a. o tamanho do extended network prefix
    b. máscara de subrede
    c. número de cada subrede
    d. endereço broadcast de cada subrede
    e. endereços de host para cada subrede
    f. endereço do roteador/default gateway para cada subrede, sabendo-se que o padrão da empresa é utilizar o primeiro endereço de cada rede para tal função.

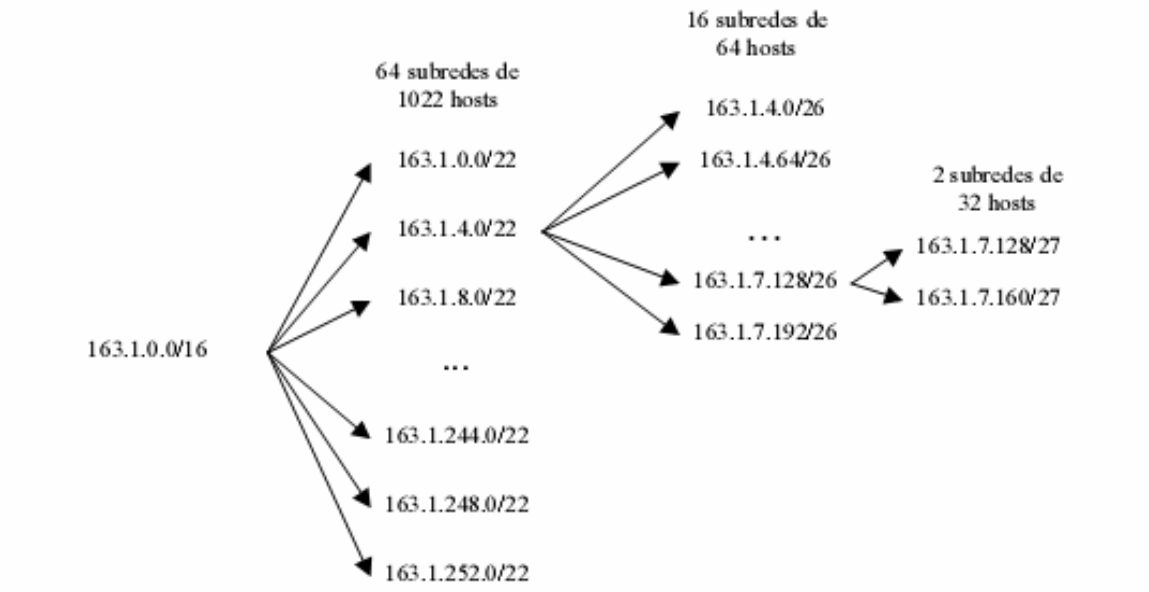
3. Uma organização recebeu o número de rede 156.1.0.0/16, e precisa definir 8 subredes. Defina o seguinte:
    a. o tamanho do extended network prefix
    b. máscara de subrede
    c. número de cada subrede
    d. endereço broadcast de cada subrede
    e. endereços de host para cada subrede
    f. endereço do roteador/default gateway para cada subrede, sabendo-se que o padrão da empresa é utilizar o primeiro endereço de cada rede para tal função.

VLSM (Variable Length Subnet Masks)

Podendo-se dividir a rede em subredes de tamanho variável permite-se uma melhor utilização do espaço de endereços destinados à empresa. Antes a empresa tinha que ficar com um número fixo de subredes de tamanho fixo. Com VLSM, é possível ter redes com grande número de hosts e também com pequeno número de hosts.

Exemplo: Suponha que uma empresa razoavelmente grande tenha um classe B cheio (163.1.0.0/16), permitindo até 65.534 hosts. Entretanto, essa empresa precisa de algumas subredes com aproximadamente 1.000 máquinas, e outras em setores com aproximadamente 30 máquinas. Se dividir igualmente o espaço de endereçamento (um /22), terá somente 64 subredes de 1022 hosts, o que provocará um desperdício em setores pequenos (aproximadamente 1.000 endereços desperdiçados). Qual a solução? VLSM.

A figura a seguir mostra uma alternativa.



- Exercícios

1. Uma empresa recebeu o espaço de endereços IP 200.200.200.0/24 e resolveu dividí-lo da seguinte forma: 2 subredes com 50 hosts e 8 subredes com 8 hosts. Defina o endereço das subredes e também as suas máscaras.

2. Uma empresa recebeu o espaço de endereços IP 198.155.226.0/24 e resolveu dividí-lo da seguinte forma: 2 subredes com 58 hosts e 8 subredes com 12 hosts. Defina o endereço das subredes e também as suas máscaras.

CIDR (Classless Inter-Domain Routing)

O protocolo **IP** tem sido largamente utilizado por mais de uma década. Apesar de estar funcionando muito bem, dois problemas surgiram: a exaustão dos endereços **IP** e a explosão das tabelas de roteamento.

Uma das alternativas a este problema que está sendo experimentada é **CIDR**. A idéia básica por trás de **CIDR** consiste em alocar o restante das redes classe C em blocos de tamanho variável. Por exemplo, se uma organização precisa de 2000 endereços, é destinada a ela 2048 endereços (oito redes classe C contíguas) e não uma rede classe B inteira (65536 endereços).

Há dois componentes básicos neste esquema:

1. Alocação distribuída de endereços Internet.
2. Agregação da informação de alocação.

Alocação de espaço de endereçamento distribuído

A idéia básica do plano é alocar um ou mais blocos de rede classe C para cada provedor de serviço da rede. Para toda organização que se conecte à Internet via provedor, são alocados subconjuntos de endereços deste provedor. Esta subalocação hierárquica de endereços implica que clientes com um subconjunto de endereços de um provedor terão, obrigatoriamente, sua informação roteada pela infra-estrutura do provedor.

Duas observações devem ser feitas para esta alocação hierárquica:

1. Espera-se que seja mais fácil para pequenos provedores obterem endereços junto à autoridade central do que clientes individuais (cujo número cresce monotonicamente)
2. Este médoto é escalável e delegável, características desejáveis por causa da alta taxa de crescimento da Internet.

Pela política **CIDR**, o mundo foi dividido em quatro zonas, a saber:

Endereços 194.0.0.0 a 195.255.255.255 - **Europa**
Endereços 198.0.0.0 a 199.255.255.255 - **América do Norte**
Endereços 200.0.0.0 a 201.255.255.255 - **América do Sol**
Endereços 202.0.0.0 a 203.255.255.255 - **Ásia e Pacífico**

Para este exemplo considere que:

- a **Universidade de Cambridge** precisa de 2048 endereços e foram alocados para ela os endereços de **194.24.0.0** a **194.24.7.255**
- a **Universidade de Oxford** precisa de 4096 endereços, sendo alocados os endereços de **194.24.16.0** a **194.24.31.255**
- a **Universidade de Edinburgh** precisa de 1096 endereços e foram alocados os endereços de **194.24.8.0** a **194.24.11.255**

Se forem estes os únicos *sites* existentes na Europa, os roteadores europeus ficariam com a seguinte tabela dos endereços acima:

Endereço	Máscara
11000010 00011000 00000000 00000000	11111111 11111111 11111000 00000000
11000010 00011000 00010000 00000000	11111111 11111111 11110000 00000000
11000010 00011000 00001000 00000000	11111111 11111111 11111100 00000000

Suponha que um pacote está sendo enviado para o endereço 194.24.17.4 (que em binário é 11000010 00011000 00010001 00000100) Inicialmente, este valor sofre uma operação de **AND** booleano com a máscara da primeira entrada (resultado 11000010 00011000 00010000 00000000), que não é igual ao primeiro endereço.

Desta forma, o endereço sofre novamente uma operação de AND booleano com a máscara da próxima entrada (resultado 11000010 00011000 00010000 00000000), que é o mesmo valor do endereço da segunda entrada da tabela. Logo, este pacote é enviado para o roteador da Universidade de Oxford (segunda entrada).

Agregação

O exemplo de funcionamento anterior mostra as vantagens da agregação em **CIDR**: não se precisa de uma entrada para cada endereço em uma organização, mas apenas do endereço e máscara da organização. Mas há duas situações em que se perde eficiência de agregação:

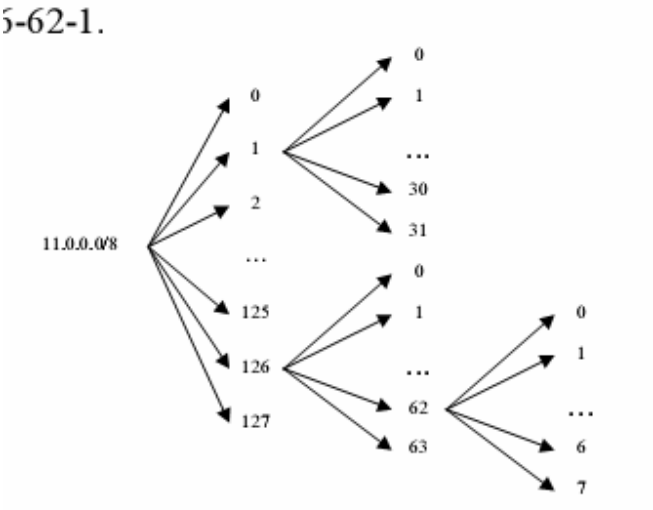
1. Quando a organização conecta-se à Internet através de dois ou mais provedores, suas rotas serão anunciadas por cada um do seus provedores, o que limita as vantagens obtidas pelo agregação em **CIDR**.
2. Organizações que trocam de provedor de acesso e não renumeram seus endereços. Neste caso, cria-se um "buraco" na agregação de endereços do provedor de servicos original.

Finalmente, a mesma idéia é aplicada para todos endereços, e não somente endereços classe C, de forma que redes classes A, B e C não são mais utilizadas. Daí o nome desta política: Classless Inter-Domain Routing.

Exercícios:

1 - Para a figura a seguir, definir a) todas as subredes envolvidas, com máscaras de subrede e extended network prefix para cada uma b) endereçamento de hosts, e endereço broadcast para as subredes 1-1, 13 e 14-14-1.

2 - Para a figura a seguir, definir a) todas as subredes envolvidas, com máscaras de subrede e extended network prefix para cada uma b) endereçamento de hosts, e endereço broadcast para as subredes 1-1, 125 e 126-62-1.



3 – Agregue os seguintes blocos de endereços IP /27 utilizando a maior agregação possível:

a) 192.168.50.128/27

   192.168.50.160/27

   192.168.50.196/27

   192.168.50.224/27

b) 200.13.31.64/27

   200.13.31.96/27

   200.13.31.128/27

   200.13.31.160/27

Endereçamento FIXO e DINÂMICO

Endereçamento IP fixo é quando o número IP é configurado de forma explícita na máquina do usuário, conforme exemplos anteriores. Já endereçamento dinâmico requer a utilização de um servidor (geralmente, DHCP) para fornecimento de números IP quando a máquina é inicializada.

Com IP dinâmico, na inicialização, a máquina envia uma mensagem broadcast (nível 2) solicitando um número IP. O servidor de DHCP deve procurar por algum IP livre, reservar o mesmo para a máquina que solicitou e enviar uma mensagem de retorno informando o IP que a máquina pode utilizar.

Curso: Tecnologia em Sistemas de Informação

Disciplina: Redes de Computadores

Lista de exercícios 3

Exercício 1: Subnetting e CIDR

Parte 1 - Subnetting

Suponha que você possui o seguinte bloco de endereços de rede: 132.45.0.0/16. Com estes endereços, você precisa cirar 8 subredes de tamanho igual;

1. Quantos dígitos binários adicionais são necessários para criar estas subredes?

2. Especifique a máscara que permite a criação destas subredes.

3. Expresse o número de rede de cada uma destas redes em formato binário e em formato decimal com ponto.

#0

#1

#2

#3

#4

#5

#6

#7

4. Liste a faixa de endereços de host que podem ser utilizadas na subrede #3 e informe também o endereço de broadcast

Parte 2 - CIDR

1. liste os números de rede /24 que podem ser definidos para o bloco CIDR 200.56.168.0/21

2. Agregue os seguintes conjuntos de blocos de endereços IP /24 usando a maior agregação possível:

a)
212.56.132.0/24
212.56.133.0/24
212.56.134.0/24
212.56.135.0/24

b)
202.1.96.0/24
202.1.97.0/24
202.1.98.0/24
...
202.1.126.0/24
202.1.127.0/24
202.1.128.0/24
202.1.129.0/24
...
202.1.158.0/24
202.1.159.0/24

Exercício 2: VLSM

Uma empresa recebeu o seguinte espaço de endereços: 200.100.152.0/22. Esta empresa precisa distribuir estes endereços pelas suas subredes. Sua rede corporativa é constituída dos seguintes sites:

a) Um site central com 200 hosts

b) Quatro sites remotos grandes; dois com 50 e dois com 40 hosts

c) Quatro sites remotos pequenos, dois com 25 e dois com 20 hosts

Todos os sites devem se ligar ao nó central através de enlaces ópticos independentes. Baseando-se nestas informações faça o seguinte:

1. Um diagrama mostrando a interconexão de todos os roteadores desta rede.

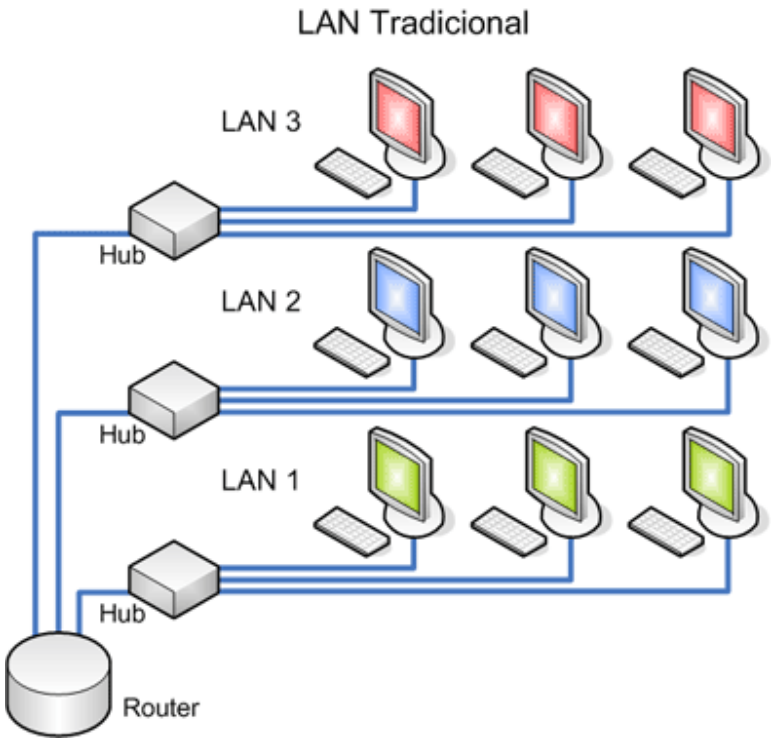
2. Calcule o ID de rede e a máscara de subrede para cada subrede desta empresa.

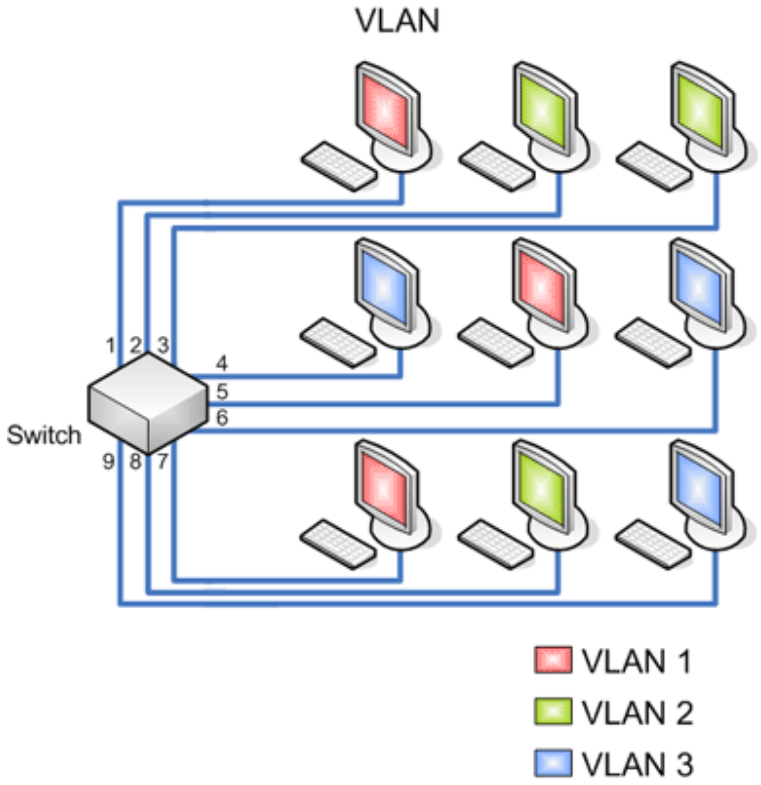
3. Atribuia um endereço IP válido a cada interface dos roteadores da rede.

VLAN's (Tanenbaum, 4.7.6)

Uma VLAN é um agrupamento lógico de dispositivos ou usuários que podem ser agrupados por função, departamento ou aplicativo, independentemente da localização de seus segmentos físicos. A configuração da VLAN é feita no switch através de software. A implementação de VLAN's é feita através do protocolo IEEE 802.1Q, o qual também estabelece um padrão para inserção de informações sobre à qual VLAN o quadro pertence no cabeçalho Ethernet.

Uma LAN típica é configurada de acordo com a infra-estrutura física que ela está conectando - os usuários são agrupados de acordo com a sua localização. O roteador que está interconectando cada hub/switch compartilhado geralmente fornece segmentação e pode desempenhar o papel de um firewall de broadcast. Os segmentos criados por switches não. A segmentação de LAN tradicional não agrupa os usuários de acordo com o grupo de trabalho ou com a necessidade de largura de banda. Dessa forma, eles compartilham o mesmo segmento e competem pela mesma largura de banda, embora os requisitos de largura de banda possam variar bastante conforme o grupo de trabalho ou departamento.





Cada vez mais, as LANs estão sendo divididas em grupos de trabalho conectados através de backbones compartilhados para formar topologias de VLAN. As VLANs segmentam logicamente a infra-estrutura física da LAN em diferentes sub-redes (ou domínios de broadcast para a Ethernet). Os quadros de broadcast são comutados entre portas dentro de uma mesma VLAN. A figura anterior mostra a diferença entre a segmentação de LAN e VLAN. Algumas das principais diferenças são:

- As VLANs operam nas camadas 2 e 3 do modelo de referência OSI.
- A comunicação entre as VLANs é fornecida pelo roteamento da camada 3.
- As VLANs proporcionam um método para controlar os broadcasts da rede.
- O administrador da rede atribui usuários a uma VLAN.
- As VLANs podem aumentar a segurança da rede definindo que nós da rede podem se comunicar entre si.

Usando tecnologia VLAN, você pode agrupar as portas do switch e seus usuários conectados em grupos de trabalho logicamente definidos, como os seguintes:

- Colegas de trabalho no mesmo departamento
- Uma equipe polivalente
- Vários grupos de usuários compartilhando o mesmo aplicativo de rede ou software

Você pode agrupar portas e usuários de grupos de trabalho em um único switch ou em switches conectados. Agrupando as portas e os usuários através de vários switches, as VLANs podem abranger infra-estruturas de um único prédio, de prédios interconectados ou mesmo de redes de longa distância (WANs).

Um conceito fundamental para a utilização de VLANs é a introdução de quadros rotulados (tagged frames, em inglês). Os quadros são as unidades de informação compartilhadas no nível de enlace, isto é, o que efetivamente a sua placa de rede irá colocar no barramento. O quadro irá sofrer uma alteração como descrita na Figura 1, onde a identificação da VLAN é adicionada ao quadro Ethernet. Isto torna o quadro incompatível com os padrões antigos, requerendo equipamentos e sistemas operacionais com capacidade de lidar com VLANs. é através destes rótulos (tags, em inglês) que é possível identificar a que VLANs um determinado quadro pertence. As VLANs são padronizadas através do protocolo IEEE 802.1Q [1], que prevê quadros especiais para ethernet, token ring e FDDI.

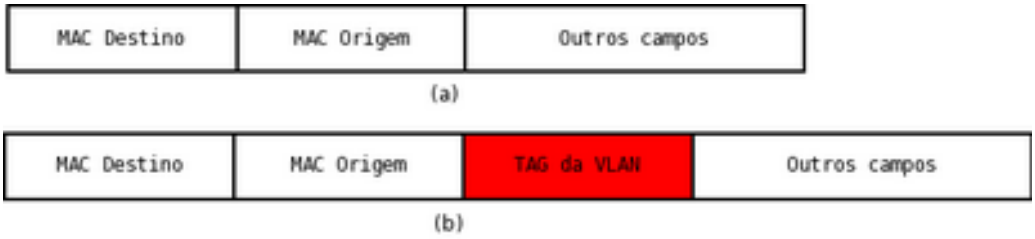


Figura1: Um quadro tradicional, em uma visão simplificada (a) e um quadro com o rótulo da VLAN (b)

Os quadros enviados pelas estações em geral não possuem nenhum tipo de suporte a VLANs e são rotulados ao passarem por switches com uma configuração de VLAN ativa. Isto irá requerer um reprocessamento do quadro, com a inclusão do tag, recálculo do FCS (Frame Check Sequence – um CRC de 32 bits situado ao final do quadro Ethernet, usado para verificação da integridade do quadro) e do campo de preenchimento (Padding – Bytes adicionados para que o tamanho mínimo do quadro ethernet seja obedecido). O procedimento inverso terá que ser feito ao se entregar um quadro para uma estação destino que não é capaz de entender o protocolo 802.1Q. Na Figura 2 pode-se ver esta operações de inclusão e remoção de rótulos, representados em vermelho.

Figura2: Inclusão e remoção de rótulos nos quadros ethernet.

O processo de inclusão do tag irá depender do tipo de equipamento que se possui, sendo que nem todos possuem os mesmos métodos. De acordo com a complexidade do equipamento e da camada do modelo OSI na qual ele opera, métodos diferentes podem ser usados. Entre os métodos mais comuns, tem-se:

- *Baseado em portas (camada 1).* Neste caso, a configuração é feita associando-se portas do seu equipamento de rede (switch ou roteador) com números de VLANs, denominados VLAN IDs. Assim todo tráfego que chegar por estas portas será rotulado de acordo com o VLAN ID configurado. Todo tráfego com o mesmo número de VLAN ID passará então a fazer parte da mesma sub-rede lógica, não importando de onde estejam vindo. Esta configuração é muito comum em switches, onde as estações que não usam quadros com rótulos são conectadas. O switch irá adicionar o rótulo ao receber um quadro da estação e remover ao devolver. Este método irá requerer uma reconfiguração do switch caso a estação seja levada para outro lugar.

- *Baseado em MACs (camada 2).* Basicamente é feita uma tabela onde se associa endereços MACs a endereços de VLAN. O MAC (Media Access Control) é o endereço de enlace da placa de rede, também chamado de endereço de hardware, que pode ser obtido através do comando ifconfig. Obviamente, este método pode ser bastante enfadonho quando o número de endereços for grande e requer bastante configuração manual.

- *Baseado em subnets (camada 3).* Requer um equipamento que opere também na camada 3, de forma que uma tabela de endereços de VLAN ID versus endereços de sub-redes possa ser especificada (equipamentos mais caros).

Tipos menos usuais mas bastante interessantes e previstos na norma 802.1Q são VLANs definidas por protocolos de aplicação (por exemplo, o tráfego de email poderia ser feito em uma VLAN enquanto o de FTP em outra), endereços de multicasting e tipos de protocolos presente no quadro Ethernet (IP e IPX poderiam estar em VLANs diferentes, já que isto pode ser previsto diretamente através do quadro Ethernet, via consulta ao campo Protocol Type.

Outro conceito presente no jargão de VLANs é o de tronco (trunk). Um tronco é uma conexão física entre dois equipamentos que possuem implementação de VLANs. Neste caso, podem ser trocados quadros de diversas VLANs através deles. Por exemplo, suponha um switch e um roteador interligados, ambos com suporte a VLANs. Os quadros trocados entres eles precisam levar consigo a informação de VLAN de forma que o roteador possa executar o roteamento adequadamente. Geralmente cada VLAN é definida no roteador e associada com um endereço de sub-rede, facilitando o trabalho de construção de rotas e geração de regras de firewall. é interessante que as conexões do tipo tronco possuam um banda passante (thoughput) maior do que as outras portas, já que o tráfego por ela será provavelmente maior.

O protocolo também define o conceito de Links de Acesso (Access Links) como o segmento que multiplexa um ou mais dispositivos que não possuem VLANs numa porta de um equipamento com VLANs habilitadas. Desta forma, através deste equipamento (geralmente uma bridge ou switch) é possível agregar a informação de VLAN aos quadros. Na Figura 3 são ilustradas estas situações. Suponha que no switch com VLAN as duas primeiras portas estejam associadas às VLANs A e B, respectivamente, e que no roteador exista uma interface de rede virtual associadas às subnets A e B. Através das portas do switch com VLAN, todo o tráfego proveniente das subnets é rotulado e o domínio de broadcast se torna limitado, não sendo repassado entre as sub-redes. Este tráfego rotulado chega até o roteador através de um link tronco, capaz de levar diferentes tipos de VLANs. Finalmente, no roteador, as ações de roteamento e firewall são tomadas.

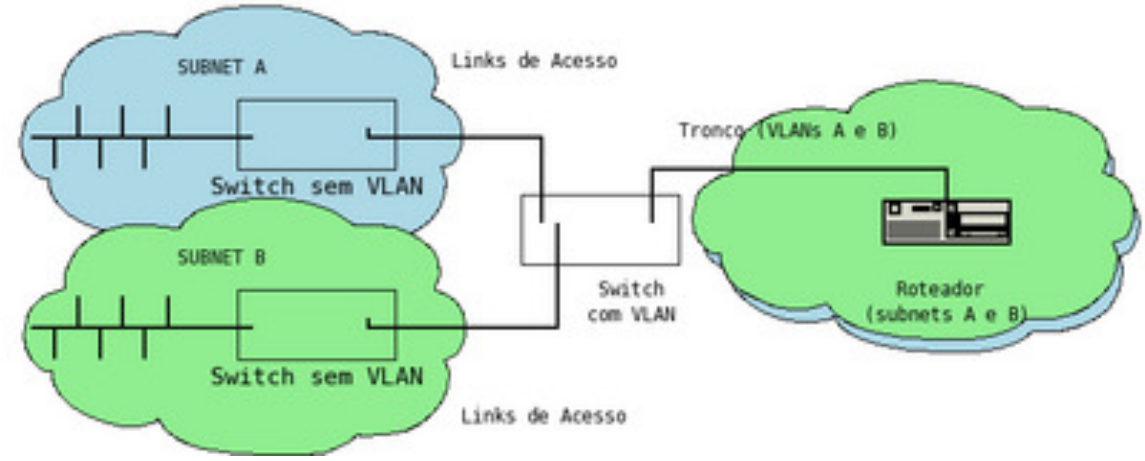


Figura 3: Links de acesso são empregados para que o tráfego possa ser rotulado.

Para que equipamentos de VLAN's diferentes se comuniquem é necessário que estejam em subredes IP diferentes – daí a necessidade de um equipamento de camada 3 para efetuar a tarefa de roteamento entre estas subredes.

Tecnologia WAN – Frame Relay e ATM (Tanenbaum, 1.5.2)

Frame Relay

Histórico:

Como introdução às redes WAN (redes que conectam redes) destacamos o conceito de redes orientadas à conexão, onde o primeiro exemplar são as redes X.25 – primeira rede pública de dados – a partir da qual se desenvolveram as redes Frame Relay. O X.25 foi desenvolvido na década de 70, na época em que o serviço de telefonia era um monopólio em todos os lugares. Para usar a X.25, primeiro um computador estabelecia uma conexão com o computador remoto, isto é, fazia uma chamada telefônica. Essa conexão recebia um número que seria usado em pacotes de transferência de dados (porque várias conexões poderiam estar abertas ao mesmo tempo). Os pacotes de dados eram muito simples, consistindo em um cabeçalho de 3 bytes e até 128 bytes de dados. O cabeçalho tinha um número de conexão de 12 bits, um número de seqüência de pacote, um número de confirmação e alguns bits variados. Os sofisticados algoritimos de detecção e correção de erros a transformou numa rede extremamente confiável, mas com um overhead (processamento) considerável, o que não permitia taxas maiores de transmissão de dados. As redes X.25 operaram por cerca de uma década com relativo sucesso.

Na década de 80, as redes X.25 foram substituídas em grande parte por um novo tipo de rede chamado Frame Relay. Além de ser considerada uma evolução das redes X.25, sua essência é o fato de ser uma rede orientada a conexões sem controle de erros e nenhum controle de fluxo. Por se tratar de uma rede orientada a conexões, os pacotes também são entregues em seqüência (em ordem), quando são entregues. As propriedades de entrega em ordem, nenhum controle de erros e nenhum controle de fluxo tornam o Frame Relay semelhante à uma LAN de área extensa. Sua aplicação mais importante é a interconexão de LAN's instaladas em vários escritórios de uma empresa, por exemplo.

Quadro Frame Relay:

FLAG	CABEÇALHO	INFORMAÇÃO DE USUÁRIO	FCS	FLAG

O cabeçalho é composto dos seguintes campos:

Byte 1			Byte 2				
DLCI	C/R	EA	DLCI	FECN	BECN	DE	EA
8 7 6 5 4 3	2	1	8 7 6 5	4	3	2	1

- Flag: Indicam o início e o fim de cada frame. O valor 01111110 é utilizado. Para garantir que esse valor não se repita na área de dados, é utilizada a técnica de "bit stuffing"

- Cabeçalho:
  - DLCI (Data Link Connection Identifier), com 10 bits, dividido em duas partes, representa o endereço designado para o destinatário de um PVC (Permanent Virtual

Circuit) dentro de um canal de usuário, e tem significado local apenas para a porta de origem. O switch Frame Relay mapeia os DLCIs entre um par de roteadores para criar um circuito virtual permanente.

- C/R (Command / Response): Com 1 bit, é usado pela aplicação usuária e não pela rede Frame Relay.
- FECN (Foward Explicit Congestion Notification), com 1 bit, é usado pela rede para informar um equipamento receptor de informações que procedimentos de prevenção de congestionamento devem ser iniciados.
- BECN (Backward Explicit Congestion Notification), com 1 bit, é usado pela rede para informar um equipamento transmissor de informações que procedimentos de prevenção de congestionamento devem ser iniciados.
- DE (Discard Eligibility Indicator), com 1 bit, indica se o frame pode ser preferencialmente descartado em caso de congestionamento na rede.
- EA (Extension Bit), com 2 bits, é usado para indicar que o cabeçalho tem mais de 2 bytes, em caso especiais;

- Informações de usuário: Dados de usuário (ou ***payload***). Pode ser de comprimento variável, provocando atraso variável na rede.

- FCS (Frame Check Sequence): CRC de 16 bits.

A seguir estão outros termos que são usados para discutir o Frame Relay:

- Taxa de acesso -- A velocidade de clock (ou velocidade da porta) da conexão (loop local) com a nuvem Frame Relay. É a velocidade na qual os dados viajam para fora ou para dentro da rede.
- Committed Information Rate (CIR) -- A CIR é a taxa garantida, em bits por segundo, que o provedor de serviços se compromete em fornecer.
- Committed Burst -- O número máximo de bits que o switch/rede – em condições normais - concorda em transferir durante um intervalo de tempo. (É descrito como Bc e é um dos parâmetros utilizados para se calcular a CIR).
- Excess Burst -- O número máximo de bits não garantidos que o switch Frame Relay tenta transferir além da CIR. O Excess Burst depende das ofertas de serviços disponíveis do fornecedor, mas é geralmente limitado à velocidade da porta do loop de acesso local.
- Forward Explicit Congestion Notification (FECN) e Backward Explicit Congestion Notification (BECN)-- Se um dispositivo A está enviando dados para o dispositivo B através de uma infraestrutura Frame Relay e um dos switches Frame Relay encontra congestionamento (buffers cheios, portas sobrecarregadas, recursos esgotados) ele marcará o bit BECN nos pacotes que estão sendo enviados de volta para o dispositivo de envio e o bit FECN nos pacotes encaminhados ao dispositivo receptor. Isto tem o efeito de dizer ao roteador transmissor para “segurar” a transmissão e aplicar “controle de fluxo”, avisando às camadas superiores para diminuir o tamanho da janela de transmissão. Um pacote com o bit FECN ativado diz ao dispositivo receptor que o caminho está congestionado para que os protocolos das camadas superiores fiquem

cientes do “delay” esperado nas transmissões. Se o roteador receber BECNs durante o intervalo de tempo atual, ele diminuirá a taxa de transmissão em 25%.

- Indicador Discard Eligibility (DE) -- Um bit definido que indica que o quadro pode ser descartado no lugar de outros quadros, se houver congestionamento. Quando o roteador detectar um congestionamento na rede, o switch Frame Relay abandonará primeiro os pacotes com o bit DE definido. O bit DE é definido quando o limite de tráfego é ultrapassado (isto é, o tráfego recebido depois que a CIR é atingida).

Diferença PVC e SVC:

Um PVC (Permanent Virtual Circuit) efetua uma conexão dedicada e permanente entre dois pontos, devendo ser configurada após o estabelecimento do contrato de tráfego entre o usuário e a operadora. Um PVC é análogo a uma linha privativa sempre ligada, tipo ADSL ou Cable Modem. No caso do SVC (Switched Virtual Circuit), a chamada é criada no momento da conexão, e terminada no final. Pode-se fazer uma analogia com o sistema telefônico atual, onde é estabelecida uma conexão no início da chamada, sendo terminada ao final, e os recursos voltam para a rede. É fácil inferir que o controle de um circuito SVC é bem maior que um PVC, que necessita ser criado apenas uma vez no estabelecimento do contrato, entretanto, os recursos ficam alocados àquele usuário (que paga por isso, claro).

Elegibilidade para Descarte:

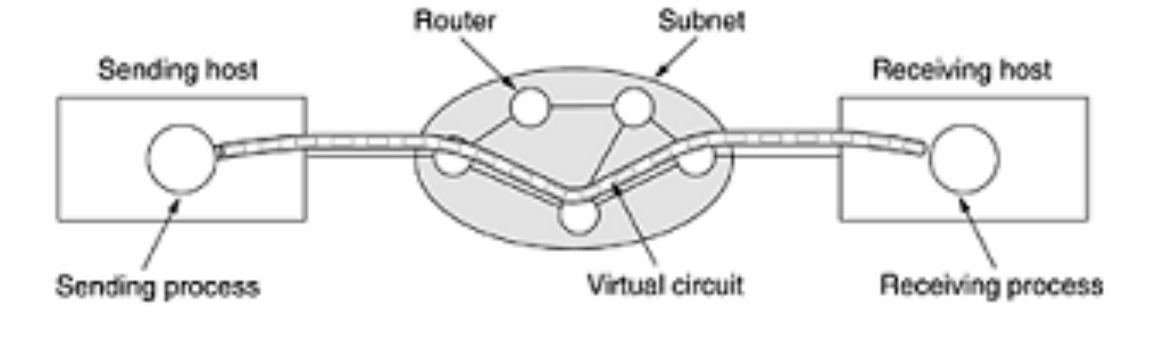
Como parte do padrão básico do Frame Relay existe no cabeçalho do protocolo o bit DE que, se ativado, indica aos equipamentos da rede que o frame pode ser descartado em caso de congestionamento. Para definir o procedimento de ativação do bit DE, o padrão Frame Relay definiu o CIR (Committed Information Rate), que representa a capacidade média de informação de um circuito virtual. Para cada VC a ser ativado na rede, o usuário deve especificar o CIR de acordo com a necessidade de sua aplicação. Normalmente o CIR é especificado como sendo uma porcentagem da capacidade máxima da porta física onde é conectado o equipamento de aplicação do usuário, ou seja, para uma porta de 2 Mbits/s, por exemplo, pode-se adotar um CIR de 1Mbit/s (50%) a ser configurado para o VC. Desta forma, tanto os equipamentos de usuário como os equipamentos de rede passam a ativar o bit DE toda vez que um quadro a ser enviado ultrapasse o CIR configurado para o respectivo VC. Isto implica que, em caso de congestionamento, os quadros que possuem o bit DE ativado são preferencialmente descartados para tentar normalizar o carregamento da rede. Quando o descarte de quadros com o bit DE ativado não é suficiente para acabar com o congestionamento da rede, qualquer tipo de quadro é descartado, independente do estado do bit DE.

ATM (Assincronous Transfer Mode)

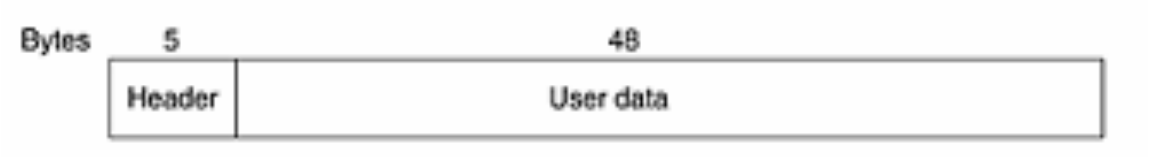
Outra rede orientada a conexões, e muito mais importante, é o ATM (Asynchronous Transfer Mode). O termo “Asyncronous” é explicado pelo fato de, no sistema de telefonia, a maioria das transmissões ser síncrona (vinculada a um relógio que mantém o sincronismo) em contraste com o método assíncrono do ATM. O ATM prometia resolver todos os problemas de redes e telecomunicações do mundo, mesclando voz, dados, televisão a cabo e etc. em um

único sistema integrado que poderia fazer tudo para todos. É amplamente utilizado dentro do sistema de telefonia, com freqüência para mover pacotes IP. Por ser utilizado principalmente pelas operadoras para transporte interno, muitas vezes os usuários não percebem sua existência mas, sem dúvida, ele está vivo e muito bem.

O envio de dados exige primeiro o envio de um pacote para configurar a conexão. À medida que o pacote de configuração passa pela subrede, todos os roteadores do caminho inserem uma entrada em suas tabelas internas registrando a existência da conexão e reservando os recursos necessários para ela. Com freqüência, as conexões são chamadas circuitos virtuais, em uma analogia com os circuitos físicos utilizados no sistema de telefonia. A maioria das redes ATM também admite circuitos vituais permanentes, que são conexões permanentes entre dois hosts distantes. Eles são semelhantes a linhas dedicadas no universo a telefonia. Cada conexão (temporária ou permanente) tem um identificados de conexão exclusivo. Um circuito virtual é ilustrado a seguir:



Uma vez estabelecida uma conexão, um ou outro lado pode iniciar a transmissão de dados. A idéia básica por trás do ATM é transmitir todas as informações em pequenos pacotes de tamanho fixo chamado células. As células têm 53 bytes, dos quais 5 formam o cabeçalho e 48 a carga útil, como mostra a figura a seguir:



Uma parte do cabeçalho é o identificador da conexão e assim os hosts transmissor e receptor e todos os roteadores intermediários podem saber quais células pertencem a cada conexão. Essa informação permite que cada roteador saiba como rotear cada célula de entrada. O roteamento de células é feito em hardware, em alta velocidade. De fato, o principal argumento para se ter células de tamanho fixo é a facilidade para construir roteadores de hardware capazes de tratar células curtas de comprimento fixo. Pacotes IP de comprimento variável têm de ser roteados por software, um processo mais lento. Outra vantagem do ATM é a possibilidade de configurar o hardware para copiar uma célula de entrada em várias linhas de saída, uma propriedade necessária para manipular um programa de televisão que esteja sendo transmitido por difusão a muitos receptores. Por fim, células pequenas não bloqueiam nenhuma linha por muito tempo, o que torna mais fácil grantir a qualidade de serviço.

Todas as células seguem a mesma rota até o destino. A entrega de células não é garantida, mas a sua ordem sim. No caso de células perdidas, cabe aos protocolos mais altos recuperar células perdidas. Observe que, embora essa garantia não seja perfeita, é melhor que a garantia oferecida pela Internet. Lá, os pacotes não só podem se perder, mas também podem ser entregues fora de ordem.

As redes ATM são organizadas como WANs tradicionais, com linhas e switches. As velocidades mais comuns para o ATM são 155 Mbps e 622 Mbps, embora também sejam admitidas velocidades mais altas. Devido à possibilidade de integrar os diversos serviços existentes (voz, dados e vídeo) conjugados com altas taxas de transmissão e com a compatibilidade com as diversas redes existentes atualmente, o ATM foi a tecnologia escolhida para suportar a diversidade de serviços definida pela Rede Digital de Serviços Integrados de Faixa Larga (B-ISDN).

Tecnologia WAN – xDSL (Tanenbaum, 2.5.3)

DSL (Digital Subscriber Line)

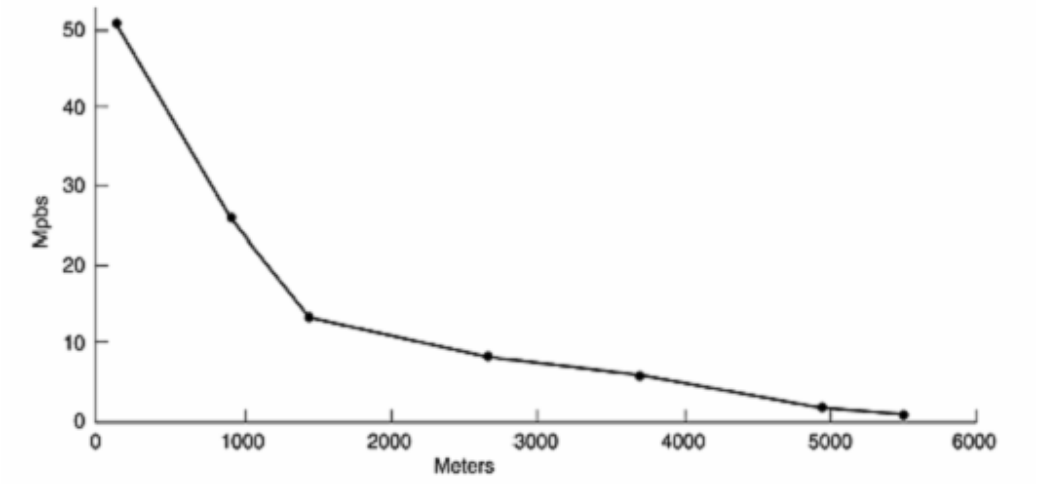
Antes mesmo de falar sobre a tecnologia ADSL precisamos entender o padrão DSL. Todas as abreviaturas (IDSL, CDSL, DSL Lite, HDSL, SDSL, ADSL, RADSL, UDSL e VDSL) deste padrão foram criadas pela Bellcore Corp. e estão associadas aos modems que cada uma utiliza. Portanto, é imprescindível que isto fique claro:

"A tecnologia não está associada ao meio físico, e sim aos modems que serão utilizados pela mesma".

São utilizados modems digitais, mais conhecidos como **MODEM BANDA BASE** ou **DATA SET** e não realizam a modulação/demodulação propriamente dita do sinal digital. Estes equipamentos codificam o sinal digital de forma a adequá-lo à transmissão em uma linha física. Esta codificação é uma mudança na representação do sinal digital, transformando o próprio sinal digital oriundo do micro em um outro sinal mais adequado às condições da linha. Estes modems só podem ser utilizados em distâncias curtas (poucos quilômetros) e em linhas de boa qualidade (também chamadas de *linhas tipo **B***). Isto se deve ao fato de que a faixa de freqüência disponível nos meios de transmissão geralmente é limitada, fazendo com que o sinal sofra bastante distorção ao se propagar pelo meio.

O mais interessante é que o meio físico utilizado é composto pelos mesmos velhos cabos de fio de cobre que utilizamos para estabelecer a nossa velha conexão discada . Só que desta vez podemos atingir uma taxa de transferência de até 52,8 Mbps (downstream do VDSL) ao invés da velha taxa de 56Kbps (modem convencional). Desta forma as companhias telefônicas podem usar os fios de cobre já instalados, evitando maiores gastos com instalações de meio físico. Para que possamos utilizar esta tecnologia precisamos de dois modems xDSL unidos pelo meio físico distando no máximo, aproximadamente, 5,4Km (para IDSL, CDSL, DSL Lite e ADSL). Apesar das tecnologias xDSL utilizarem o mesmo meio físico de sua linha telefônica, você pode usá-los simultaneamente sem nenhuma interferência. Ou seja, enquanto você navega pela Internet o seu telefone continua funcionando normalmente, livre para receber e efetuar chamadas por exemplo.

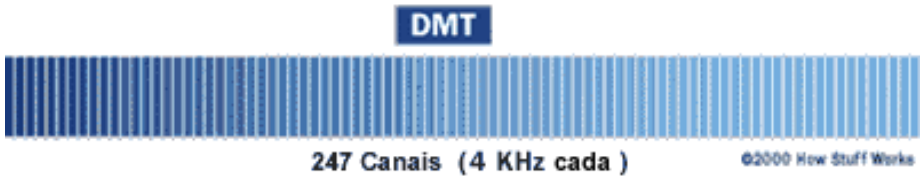
A seguir, um gráfico de Largura de Banda x Distância sobre cabos CAT3 para a família xDSL:



O ADSL utiliza duas taxas de transferência distintas: a grosso modo, uma para upload e outra para download. Os valores dessas taxas variam de acordo com a distancia entre um modem e outro - quanto mais próximos os modems, maiores taxas podem ser atingidas. Colocando isto em valores reais, temos que, a uma distância de aproximadamente 5,4Km podemos atingir taxas de até 1,544Mbps downstream, enquanto à aproximadamente 2,7Km podemos atingir taxas de até 8,448Mbps downstream. É fácil perceber porque é interessante manter as taxas de downstream e upstream com valores distintos: na grande esmagadora maioria das vezes que acessamos a Internet recebemos mais dados do que enviamos. Como o ADSL tem o seu uso geral para acesso a Internet (para outras aplicações são utilizadas outras tecnologias xDSL – consulte a tabela fornecida) foi definido um valor menor para upstream, e um maior para downstream. Desta forma, busca-se uma forma mais eficiente de utilizar os escassos recursos disponíveis, adequando-se a sua aplicação. Seguindo a tecnologia DSL, o ADSL também suporta voz e dados simultaneamente, dividindo a linha telefônica em duas partes. A primeira parte é delimitada a ondas de até 4Khz, que ocupam cerca de 1% (um por cento) da capacidade do meio físico que, para a nossa surpresa, é o suficiente para se transmitir voz. As ondas de 26Khz até 2Mhz são utilizadas para transmitir dados, que utilizam cerca de 99% (noventa e nove por cento) da capacidade do meio físico. O padrão oficial (atual) para a ADSL, ANSI (em inglês), é um sistema chamado **multitom discreto**, ou DMT. De acordo com os fabricantes de equipamentos, a maioria dos equipamentos ADSL instalados hoje usa o DMT.

O sistema DMT:

O sistema DMT também divide os sinais em canais separados, mas não usa dois canais amplos para enviar ou receber os dados da Internet. Em vez disso, o DMT divide os dados em 247 canais separados, cada um com 4 kHz de largura.

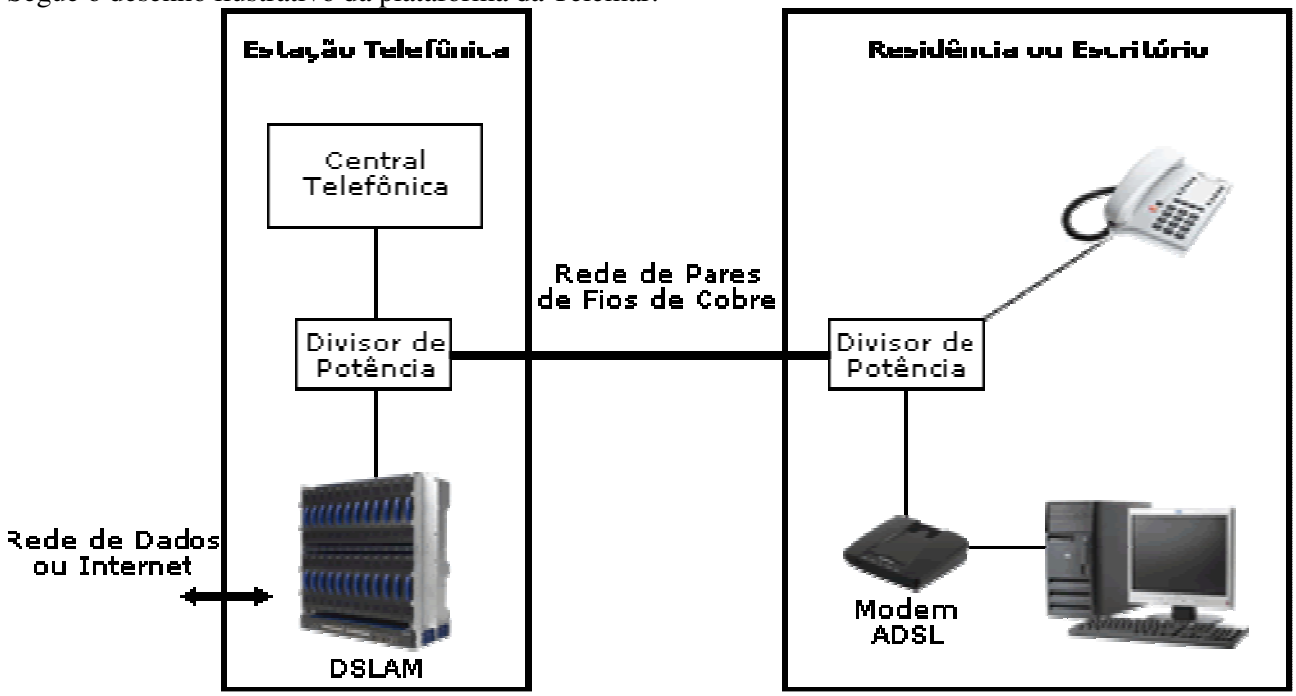


Uma maneira de pensar sobre isso é imaginar que a companhia telefônica divide sua linha de cobre em 247 linhas diferentes, cada uma com 4 kHz, e então conecta todas a um modem. Você obtém o equivalente a 247 modems conectados a seu computador de uma vez. Cada canal é monitorado e, se a qualidade não for boa, o sinal será desviado para outro canal. Esse sistema constantemente desvia os sinais entre os diferentes canais, buscando os melhores canais para transmissão e recepção. Além disso, alguns dos canais inferiores (aqueles que começam em cerca de 8 kHz) são usados como canais bidirecionais para as informações enviadas e recebidas da Internet. Monitorar e classificar as informações nos canais bidirecionais e manter a qualidade de todos os 247 canais torna o DMT mais complexo de implementar, mas dá maior flexibilidade em linhas de diferentes qualidades.

VELOX

Para exemplificar o funcionamento do ADSL escolhemos o serviço Velox prestado pela Telemar Telecomunicações. Quando você solicita o serviço ADSL, não há nenhuma substituição de cabos telefônicos da sua residência, nem da rua onde você mora. Apenas é deixado um modem ADSL em suas mãos que utiliza a linha telefônica para conectar-se a outro modem ADSL, que está na outra extremidade com a sua prestadora do serviço. No cliente, os sinais de voz e dados são multiplexados na linha telefônica, e seguem seu rumo no mesmo meio físico. Na prestadora do serviço ADSL existe um equipamento chamado Splitter que separa a voz dos dados, de acordo com a freqüência do sinal. Os sinais de voz são encaminhados para a rede telefônica a fim de serem tarifados, e também para utilizar o serviço de telefonia. Os sinais de dados são encaminhados para um outro equipamento chamado DSLAM (Digital Subscriber Line Access Multiplexer), que , de um lado, concentra o tráfego de dados das várias linhas com modems DSL, e do outro acessa o serviço de Internet. A conexão através de circuitos ATM é a mais utilizada em redes ADSL. Existem equipamentos DSLAM que assumiram o papel de nó de acesso incorporando sistemas de comutação ATM. As informações vindas da Internet seguem o sentido oposto, em direção ao cliente, passando pelo DSLAM e chegando ao Splitter. A partir daí os dados passam a compartilhar novamente o meio físico com a voz (vinda da rede telefônica) até chegar novamente ao cliente do serviço.

Segue o desenho ilustrativo da plataforma da Telemar:



Componentes de uma rede ADSL:

- Modem/Transceptor ADSL - Na residência ou escritório do usuário é instalado um Transceptor ADSL para conexão com um PC. O transceptor é geralmente conectado a uma placa de rede no micro. Este micro pode ser um servidor de acesso à Internet para uma pequena rede local. A maioria dos clientes residenciais chama seu transceptor como um "modem DSL". Os engenheiros na companhia telefônica ou no provedor de internet (ISP) o chamam de **ATU-R**. Independentemente do nome pelo qual é chamado, ele é o ponto em que os dados do computador ou rede do usuário se conectam com a linha DSL.

Modem/Transceptor DSL

- Divisores de potência - Divisores de potência e filtros colocados na residência do usuário e na Estação telefônica permitem a separação do sinal de voz da chamada telefônica do tráfego de dados via ADSL.
- DSLAM - Na estação telefônica cada par telefônico é conectado a um mutiplexador de acesso DSL (DSLAM). A função do DSLAM é concentrar o tráfego de dados das várias linhas com modems DSL e conectá-lo com a rede de dados. A conexão através de circuitos ATM é a mais utilizada em redes ADSL. Existem equipamentos DSLAM que assumiram o papel de nó de acesso incorporando sistemas de comutação ATM. O DSLAM proporciona uma das principais diferenças entre o serviço ao usuário por meio de ADSL e por modems a cabo. Como os usuários de modem a cabo geralmente compartilham uma malha de rede que corre através de um bairro, em muitas situações a adição de usuários significa uma redução do desempenho. O ADSL fornece uma conexão dedicada a partir de cada usuário até o DSLAM, o que significa que os usuários não verão uma diminuição de desempenho à medida que novos usuários forem acrescentados

É importante registrar que a Telemar mudou recentemente a utilização do protocolo ATM pelo Ethernet na sua Rede Multiserviço.

DSLAM (Digital Subscriber Line Access Multiplexer)

Tabela de tecnologias xDSL:

	Pares de fio	Telefone e dados	Transmissão	Taxa de dados	
ADSL Asymetric DSL	1	Sim	Assimétrica	1,5-8 Mbit/s 64-640 kbit/s	Mais popular. Utiliza-do para acesso à Internet.
ADSL 2 Asymetric DSL 2	1	Sim	Assimétrica	1,5-12 Mbit/s 64 k-1,1 Mbit/s	Evolução do ADSL. Também é utilizado para acesso à Internet.
ADSL 2+ Asymetric DSL 2+	1	Sim	Assimétrica	1,5-24 Mbit/s 64 k-1,1 Mbit/s	Evolução do ADSL 2. Também é utilizado para acesso à Internet.
RADSL Rate-adaptive DSL	1	Sim	Assimétrica	1-7 Mbit/s 128k-1 Mbit/s	Variação do ADSL que permite o ajuste da taxa de transmissão de acordo com a necessidade do cliente
HDSL High-bit-rate DSL	2	Não	Simétrica	2 Mbit/s	Uma das primeiras tecnologias DSLs a ser usada amplamen-te. Provê linhas dedicadas de 2Mbit/s.
SDSL Symetric DSL	1	Não	Simétrica	768 kbit/s	Implementação do HDSL utilizando 1 par de fios
G.shdsl	1	Não	Simétrica	até 2,3 Mbit/s	Novo padrão que melhora o desempe-nho do SDSL
MSDSL Multirate SDSL	1	Sim	Simétrica	n x 64 kbit/s até 2 mbit/s	Variação do SDSL que permite o provi-mento de serviços TDM com múltiplas taxas de dados.
IDSL ISDN DSL	1	Não	Simétrica	até 144 kbit/s	Empregado em acessos ISDN
Reach DSL	1	Sim	Simétrica	até 1 Mbit/s	Projetado para supor-tar as condições mais adversas da rede externa.

Redes Wireless

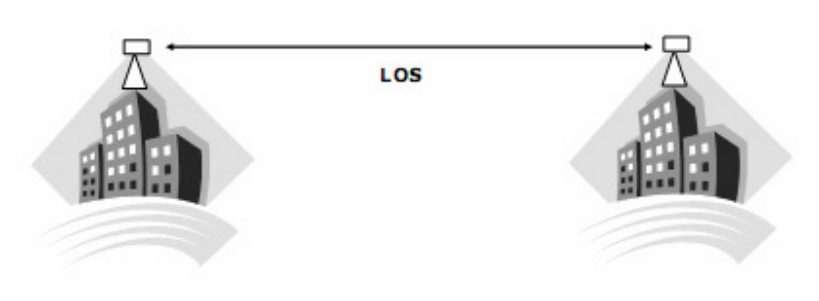
Conceito de Rádio Frequência

Um sinal ou onda de rádio freqüência é um onda eletromagnética que pode se propagar por meio do ar, água, muros, paredes, objetos físicos etc. Sinais RF são gerados por corrente alternada (AC) de alta freqüência que são transmitidos por meio de um elemento condutor (em geral cobre) e são irradiados ou propagados no ar por meio de uma antena. Neste caso, uma antena desempenha o papel de um elemento responsável por converter ou transformar o sinal transmitido em um cabo em um sinal aéreo (sem fio – wireless) e vice versa.

Um sinal RF é propagado no ar na forma de ondas de rádio que se propagam simultaneamente da antena para diversas direções. O comportamento dos sinais RF propagados por uma antena corresponde ao formato de ondas concêntricas que fluem a partir de um ponto central. Um exemplo bastante clássico que é utilizado para o entendimento do comportamento dos sinais RF propagados por uma antena é a situação resultante de uma pedra sendo jogada em um lago. Entender o comportamento dos sinais RF propagados por uma antena ajuda a entender como as redes locais wireless atualmente funcionam e foram projetadas.

Linha de Visada/Visão (Line of Sight – LOS)

Corresponde a linha reta imaginária entre o transmissor e o receptor de sinal RF



Potência Irradiada

A potência irradiada ou propagada por uma antena é a quantidade de energia do sinal emitido e é medida em dB (decibel). É regulamentada no Brasil, pela ANATEL para diversas aplicações, servindo para determinar se um enlace Wireless é viável ou não.

Os sinais RF propagados por uma antena são normalmente afetados por fenômenos que causam interferências (tempestades solares, outras fontes de tranmissão na mesma freqüência, etc.) e por características ambientais (paredes, água, etc.).

Antenas

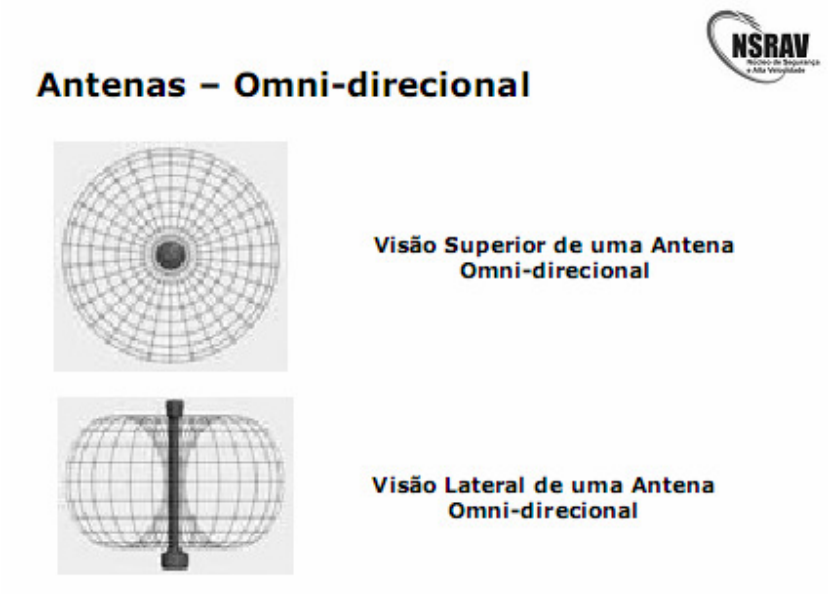
uma antena consiste em um dispositivo que converte sinais RF de alta freqüência transmitidos via cabo em ondas propagadas via meio aéreo. Três categorias genéricas de antenas RF são definidas:

• Omni-direcional (Omni-directional)

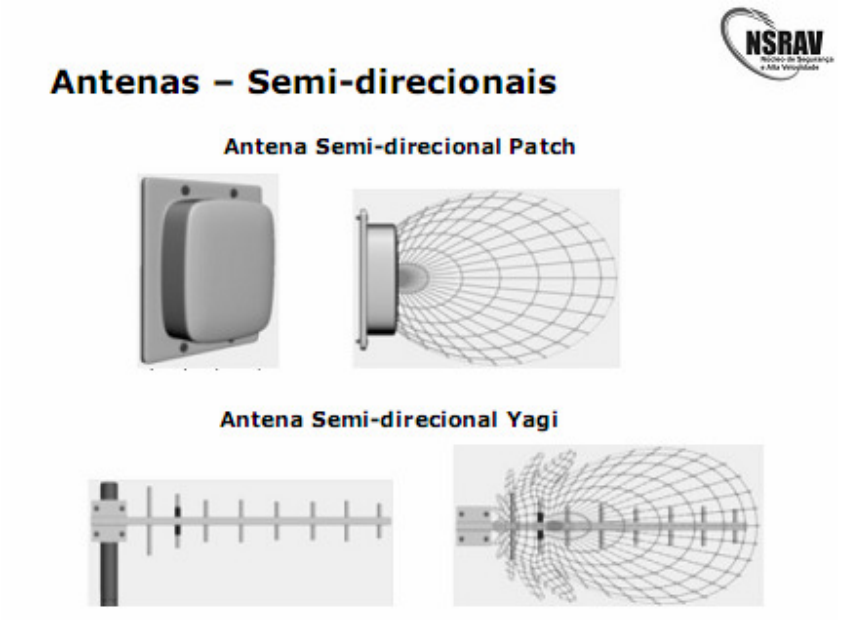
• Semi-direcional (Semi-directional)

• Altamente-direcional (Highly-directional)

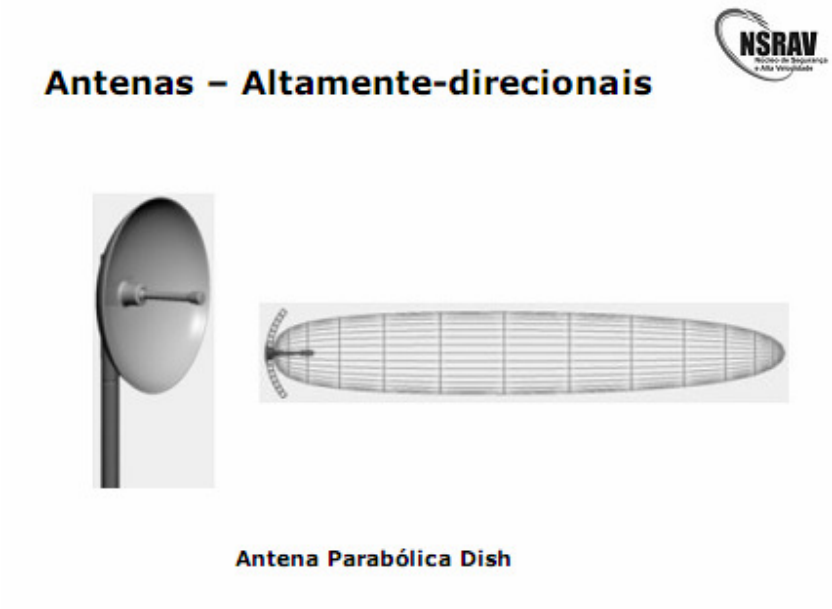
Uma antena **omni-direcional** irradia sua energia igualmente em todas as direções ao longo de seu eixo (360 graus horizontal formando uma esfera em visão tri-dimensional). Omni-direcional é o tipo de antena mais comumente utilizada em redes locais wireless, também chamada de antena bipolar. Quando utilizada em redes locais wireless, as antenas omni-direcionais possuem um tamanho pequeno devido a sua alta freqüência de transmissão em torno de 2.4 GHz. Quando a freqüência do sinal aumenta, seu comprimento de onda e as antenas diminuem. Antenas omni-direcionais são normalmente utilizadas na maioria das aplicações internas em prédios e escritórios, fornecendo uma ampla área de cobertura e inclusive possibilitando a formação de áreas com sobreposição de sinais emitidos por múltiplos pontos de acesso espalhados. Se uma antena omni-direcional for colocada no centro do andar de um prédio, o sinal será irradiado ao longo da área física deste andar com algumas partes do sinal sendo enviadas para os andares acima e abaixo da localização do ponto de acesso.



Uma antena semi-direcional irradia a sua energia diretamente em uma direção particular. Antenas direcionais possuem um ganho muito maior do que as antenas omni-direcionais, como por exemplo, com um valor de 12 dB ou até mais. Um exemplo clássico de uso de uma antena semi-direcional seria para a interligação entre dois prédios de escritório separados por uma distância não muito grande (uma rua ou alguns metros).



Uma antena **altamente direcional** também irradia a sua energia diretamente em uma direção particular, mas de forma mais concentrada que uma antena semi-direcional, permitindo comunicações do tipo ponto a ponto. A melhor utilização das antenas altamente direcionais é para cobrir grandes distâncias em uma área estreita (37 milhas ou até mais), podendo formar inclusive enlaces ponto a ponto entre prédios de escritório mais distantes. Antenas altamente direcionais possuem o maior ganho dentre as outras anteriormente abordadas, entretanto, apresentam uma largura de banda bem estreita tornando seu uso adequado apenas para comunicações de longa distância.



Histórico

Traçando um histórico geral das redes wireless, nota-se que seu desenvolvimento inicial esteve atrelado ao uso da tecnologia para fins militares, e com o tempo, gradualmente, a tecnologia envolvida com as redes wireless passou por sucessivas fases que focaram principalmente na redução de custos de hardware e em melhorias da qualidade tecnológica, fases estas que culminaram por estimular e tornar tal tecnologia apta e adequada para uso em ambientes civis, como por exemplo, universidades, empresas, escritórios, hospitais, uso doméstico etc.

Histórico detalhado das redes wireless depois dos trabalhos de desenvolvimento da Internet:

- Intervalo - Desenvolvimento da Internet
- 1989 - O Federal Communications Commission (FCC), órgão americano responsável pela regulamentação do uso do espectro de freqüências, autorizou o uso de três faixas de freqüência;
- 1990 - IEEE instala comitê para definição de um padrão para conectividade wireless;
- 1997 - Após sete anos de pesquisa e desenvolvimento, o comitê de padronização IEEE aprova o padrão IEEE 802.11
- 1998 - Ericsson, IBM, Intel, Nokia e Toshiba anunciam o desenvolvimento do bluetooth para troca de dados wireless
- 1999 - Padrões IEEE 802.11b e 802.11a aprovados. Nesse mesmo ano foi criada a Wireless Ethernet Compatibility Alliance (WECA), com o objetivo de garantir a interoperabilidade entre dispositivos de diferentes fabricantes

- 2000 - Redes 802.11 tornam-se populares com maior demanda, houve o surgimento dos primeiros hot spots (áreas públicas onde é possível acessar a Internet por meio das redes wireless IEEE 802.11)
- 2001 - Cafeterias Starbucks implementam hot spots. Os pesquisadores Scott Fluhrer, Itsik Mantin e Adi Shamir demonstraram que o protocolo de segurança Wired Equivalent Privacy (WEP) é inseguro. O WEP é quebrado. Aumenta-se a procura por maior segurança em redes wireless 802.11
- 2002 - A WECA passou a se chamar Wi-Fi Alliance (WFA) e lançou o protocolo Wi-Fi Protected Access (WPA) em substituição ao protocolo WEP
- 2003 - O comitê de padronização IEEE aprova o padrão IEEE 802.11g
- 2004 - A especificação 802.11i aumentou consideravelmente a segurança, definindo melhores procedimentos para autenticação, autorização e criptografia
- 2005 - Especificação 802.11e foi aprovada, agregando qualidade de serviço (QoS) às redes IEEE 802.11
- 2006 - Surge o padrão 802.11n, que usa múltiplas antenas para transmissão e recepção, Multiple-Input Multiple-Output (MIMO).

Entretanto, como em toda tecnologia que se usa, quer seja em um ambiente corporativo de TI ou em ambientes domésticos conhecidos como SOHO (Small Office Home Office), as redes wireless apresentam vulnerabilidades que podem ser amplamente exploradas por atacantes que desejam concretizar uma ameaça específica. As primeiras noções de explorações maliciosas e ataques em redes wireless surgiram em 2001 com Peter Shipley, e daí em diante este tópico passou a ser discutido nas principais conferências sobre segurança da informação que publicaram novas técnicas e abordaram ferramentas muitas vezes avançadas de ataques.

Dados em redes wireless são transmitidos utilizando-se freqüências de rádio. Por este motivo, as redes wireless devem ser regulamentadas pelas mesmas normas que atualmente são aplicadas para rádio AM/FM e televisão. Em termos de padrões, os mais aceitos são mantidos e atualizados pelo **IEEE (Institute of Electrical and Electronic Engineers)**. Considerando a predominância de acesso, como as redes wireless predominam em ambientes de rede local ou simplesmente LANs, tal tecnologia de rede necessita de um ponto de entrada para a rede cabeada principalmente nos pontos de distribuição ou no backbone. Contribuem para este cenário e contexto as limitações de velocidades de transmissão das redes wireless. Redes wireless ainda não alcançaram velocidades de transmissão e níveis de confiabilidade suficientes para substituir redes cabeadas. Adicionalmente, com referência ao método de acesso, as redes wireless devem ser consideradas como tecnologias de camada de enlace da mesma forma como o Ethernet.

Benefícios e Vantagens:

Mobilidade:

- Usuários tem plena liberdade de acesso a rede em qualquer região remota desde que esteja ao alcance do sinal e sensibilidade do ponto de acesso.
- Não necessita de cabos ou pontos de rede

Flexibilidade e facilidade:

- Conectividade pode estar presente mesmo em locais de difícil acesso onde cabos não podem ser instalados ou locais onde o custo é inviável (por ex. áreas rurais)
- Áreas físicas podem ser rearranjadas sem que os usuários percam o acesso aos recursos de rede (desde que se mantenham dentro da área de cobertura)
- Usuários domésticos tem acesso total à rede sem precisar instalar cabos e independetemente do local onde estejam
- Em um ambiente acadêmico, salas de aula, auditórios, lanchonetes, restaurantes e etc. podem ter também redes wireless

Custo:

- O Custo de instalação das redes wireless é, em geral, menor do que o custo de instalação das redes cabeadas tradicionais
- O Custo dos equipamentos de uma rede wireless ainda é um pouco maior do que o custo dos equipamentos utilizados em uma rede cabeada tradicional

Escalabilidade:

- Novos dispositivos, equipamentos e usuários podem ser adicionados ou retirados de uma rede wireless sem afetar aqueles já existentes

Tendências:

- Acesso amplo aos recursos de rede e conectividade em qualquer lugar (alto nível de impregnação);
- Adoção crescente das redes wireless em provedores de acesso (atendimento à consumidores)
- Desenvolvimento da especificação 802.16, comumente chamada de WiMAX. A especificação 802.16 WiMAX visa tornar mais fácil e menos custoso desenvolver redes wireless de longo alcance. Com isso, clientes poderão utilizar seus provedores de acesso por meio da tecnologia wireless, e provedores de acesso continuarão à oferecer seus serviços com um custo efetivo e viável aos clientes, mesmo para aqueles situados em regiões mais longínquas e de difícil acesso. Uma rede local wireless de longo alcance poderia até atender a um município específico ou à vários municípios fornecendo acesso a serviços emergenciais, como por exemplo, polícia, bombeiros, serviços de resgate, hospitais, utilidades públicas etc;
- Padronização crescente.

O padrão 802.11

O padrão 802.11 é um padrão IEEE criado para comunicação Wireless. Também é conhecido como Wi-Fi e utiliza freqüências da banda ISM de 2,4 ou 5,8 GHz

Bandas ISM:

As LANs podem utilizar as bandas industrial, científica ou médica (ISM), as quais são isentas de licença. As larguras de banda estão localizadas em 900 MHz, 2,4 GHz e 5,8 GHz e variam de 26 MHz até 150 MHz. A banda de 900 MHz ainda é utilizada por alguns telefones sem fio, algumas câmeras e algumas LANs wireless antigas. As LANs wireless abandonaram a banda de 900 MHz pelas freqüências de bandas mais mais altas (2,4 e 5,8 GHz) devido ao fato de que elas possuem larguras de banda maiores e então permitem maior vazão. Encontrar peças de reposição para WLANs de 900 MHz é praticamente impossível.

A banda de 2,4 GHz é de longe a mais populada entre as três bandas ISM. Muitos dispositivos portáteis como telefones sem fio e babás eletrônicas também utilizam a banda de 2,4 GHz, assim como fornos de microondas (os fornos de microondas emitem alguma interferência perto do canal 9 ou em 2,540 GHz). Apesar da faixa ISM estar entre 2,4 e 2,5 GHz, o FCC especificou somente a potência de emissão para a faixa de 2,4 GHz até 2,4835 GHz, pois esta é a faixa que as WLANs utilizam. O FCC (Federal Communications Commission - EUA) define uma potência máxima de emissão igual 1 W (30 dB) e uma EIRP (Effective Isotropic Radiated Power) de 4 W (36 dB).

O IEEE dedica bastante tempo na melhoria das funcionalidades e robustez de redes wireless, resultando na família de padrões 802.11. Estes padrões são baseados no padrão 802.3 de tecnologias Ethernet. Isso permite que uma rede wireless seja facilmente integrável com redes Ethernet convencionais. O conjunto de padrões 802 é composto pelos padrões 802.1 (gerenciamento), 802.2 (controle) e 802.3 (Ethernet). Os padrões 802.11a, 802.11b e 802.11g são os principais. No entanto são resultantes de diversas modificações feitas ao longo do tempo.

A lista completa começa com o padrão 802.11 seguido do 802.11a passando por cada letra do alfabeto até a letra y.

Padrões IEEE 802.11 principais:

- 802.11 – 2 Mbps em 900 MHz, 2,4 GHz
- 802.11b – 11 Mbps em 2,4 GHz (Troughput real de 5,5 Mbps)
- 802.11a – 54 Mbps em 5,8 GHz (velocidade total somente a uma distância limitada)
- 802.11g – 54 Mbps em 2,4 GHz (interoperável com 802.11b com perda de desempenho)

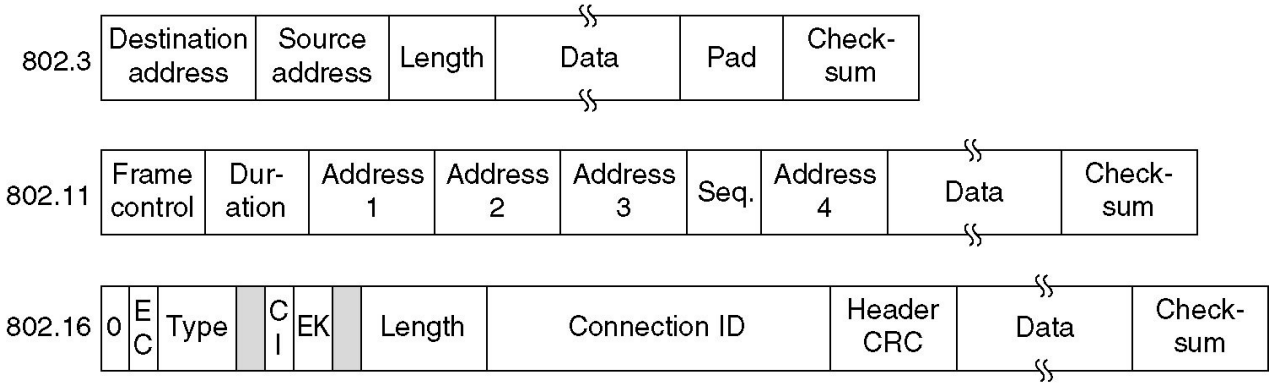
O protocolo CSMA/CA:

A camada MAC 802.11 é descrita pelo padrão ISO/IEC 8802-11:1999 que define os mecanismos básicos de acesso ao meio aéreo (wireless) por meio do algoritmo **CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)**. Portanto, o padrão 802.11 utiliza um controle de acesso ao meio um pouco diferente do controle de detecção de colisão (collision detection) implementado no Ethernet – CSMA/CD. O padrão 802.11 utiliza um controle de acesso ao meio por prevenção de colisão (CSMA / collision avoidance).

De uma forma geral, o protocolo CSMA funciona da seguinte forma: uma estação que deseja transmitir deve verificar o meio de acesso, e caso o meio de acesso esteja ocupado (alguma outra estação está transmitindo pacotes) a estação transmitirá mais tarde. Caso o meio de acesso esteja livre, então a estação cliente pode transmitir seus pacotes. Quando duas estações decidem transmitir dados ao mesmo tempo, ocorrem colisões que são tratadas pelo Ethernet CSMA/CD em uma rede cabeada. Com o CSMA/CA equipamentos de rede wireless não operam em modo full-duplex, portanto as estações não conseguem detectar colisões de sinal enquanto transmitem dados. No esquema do CSMA/CA, uma estação que deseja transmitir dados verifica o meio de acesso e, caso o meio de acesso esteja ocupado, a estação transmitirá mais tarde. Caso o meio de acesso esteja livre, a estação espera por um período aleatório de tempo (DIFS – Distributed Inter Frame Space), então se o meio de acesso continuar livre a estação cliente pode transmitir seus pacotes. O receptor deve verificar o CRC do pacote recebido e retornar com um pacote de reconhecimento (ACK). A estação transmissora ao receber o pacote de reconhecimento ACK admite que não ocorreu colisão de dados. Se a estação transmissora não receber o pacote de reconhecimento ACK, então retransmite os dados até receber o pacote de reconhecimento ACK ou até atingir um número limitado de retransmissões.

No CSMA/CA, o transmissor também pode implementar um mecanismo que libera o meio de acesso (clear to send, request to send) de qualquer atividade, fazendo com que nenhuma outra estação envie mensagens quando a estação anterior deseja transmitir dados. Entretanto, na prática um usuário consegue transmitir dados na rede wireless mesmo quando o meio de acesso está reservado para uma outra estação.

Formato dos quadros 802:



A figura acima ilustra o formato genérico de um quadro 802.11 entre os quadros 802.3 e 802.16:

- **Campo FC (Frame Control – 2 bytes):** define as opções que devem ser usadas nos outros campos do quadro 802.11, o tipo de quadro (gerenciamento, dados ou controle) e as informações necessárias para o processamento do quadro
- **Campo DUR (Duartion/ID – 2 bytes):** campo relacionado com o acesso ao meio de transmissão, contendo um valor de tempo que se espera que o meio esteja ocupado. Um valor igual a 0x0000 indica que o meio de acesso não está ocupado;
- **Campo ADDRESS 1 (6 bytes):** endereço de destino
- **Campo ADDRESS 2 (6 bytes):** endereço de origem
- **Campo ADDRESS 3 (6 bytes):** corresponde ao BSSID da rede wireless *****
- **Campo SEQ (Sequence Control – 2 bytes):** utilizado para conter informações sobre os processos de fragmentação e remontagem de pacotes
- **Campo ADDRESS 4 (6 bytes):** campo opcional, utilizado somente em uma rede permanente WDS ****** para indicar o endereço do transmissor. Quando o campo ADDRESS 4 não é utilizado, está parte do cabeçalho deve conter a porção de dados
- **Campo DATA (tamanho variável):** contém a porção de dados a ser transmitida
- **Campo FCS (Frame Check Sequence – 4 bytes):** campo que contém um código de integridade CRC32 calculado sobre o quadro 802.11, possibilitando ao receptor verificar problemas de integridade quando um quadro 802.11 é acidentalmente corrompido durante a transmissão

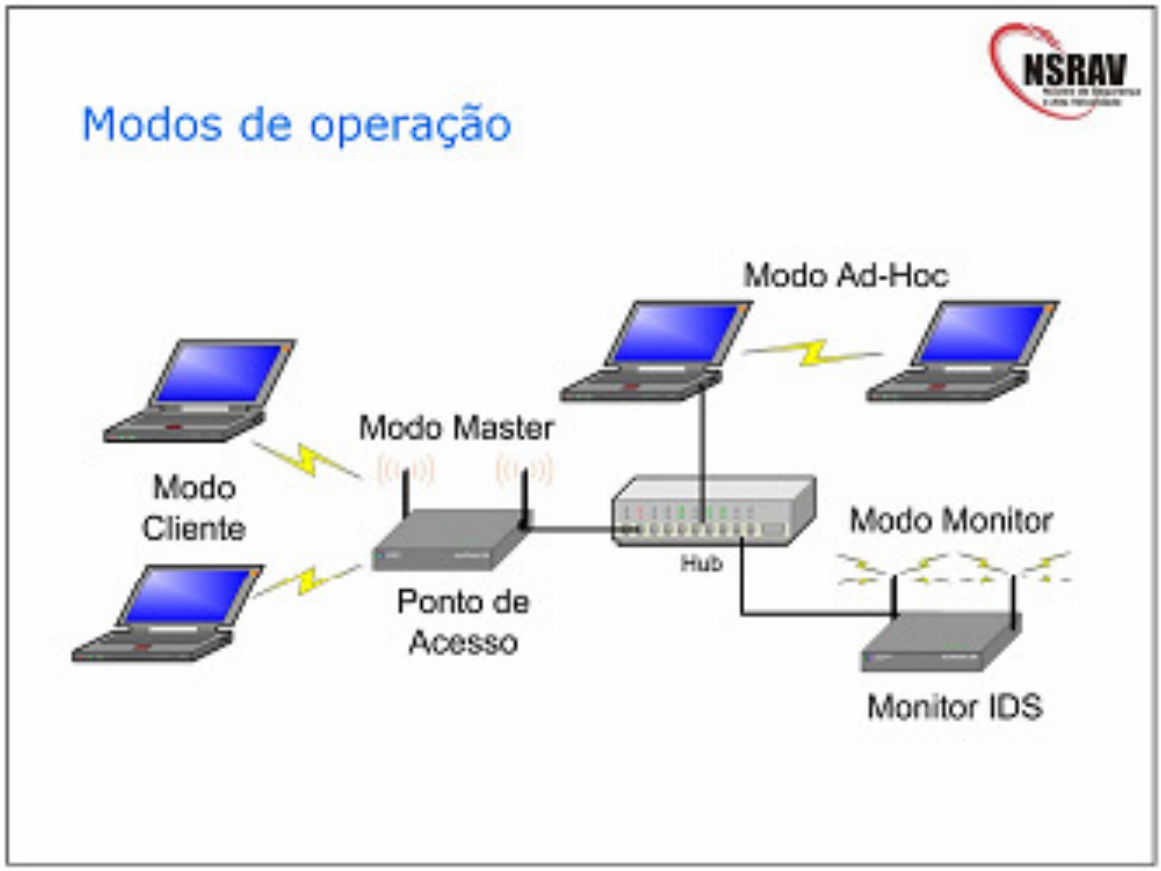
***** BSSID corresponde ao endereço MAC de 48 bits do ponto de acesso wireless.

****** WDS são dois ou mais dispositivos wireless retransmitindo o tráfego entre estações wireless formando uma comunicação ponto a ponto.

Infraestrutura

Alguns acrônimos necessários ao entendimento da infrarestrutura de acesso a redes Wireless:

- **dB** – Decibéis é uma escala logarítmica utilizada para descrever níveis de potência de forma relativa.
- **SSID** – Service Set Identifier, ou nome de rede. É um nome atribuído a um agrupamento lógico de pontos de acesso que oferecem serviços um agrupamento lógico de pontos de acesso que oferecem serviços similares
- **BSSID** – Basic Service Set Identifier. E um endereço MAC único para identificar um ponto de acesso e seus clientes conectados. O BSSID é tipicamente o mesmo endereço MAC utilizado pelo ponto de acesso.
- **BSS** – Basic Service Set. É utilizado para descrever um único ponto de acesso que está conectado a uma rede com fio.
- **ESS** – Extended Service Set. Descreve um grupo de pontos de acesso conectados por meio de rede cabeada sendo que todos os pontos de acesso compartilham o mesmo SSID.



A figura anterior apresenta um exemplo real da aplicação de cada um dos modos de operação, a saber:

- Modo Cliente: Dentre os quatro modos de operação existentes, o modo cliente é o mais utilizado pelas interfaces de rede, uma vez que a maior parte dos equipamentos de rádio são destinados a operar como cliente. O modo de operação cliente (managed mode) permite que um equipamento de rede wireless se torne uma estação da rede BSS.
- Modo Master: Uma interface de rede em modo master (master mode) atua como um ponto de acesso, transmitindo e recebendo requisições de autenticação e associação, de acordo com a configuração da interface. É comum encontrar placas que oferecem suporte ao modo master e modo cliente, dependendo somente das funcionalidades do driver da placa para a configuração de cada um dos modos.
- Modo Ad-Hoc: possibilita o estabelecimento de uma rede P2P (Peer-to-Peer) entre um ou mais clientes que estejam utilizando o mesmo modo de operação. Ao configurar este modo, a interface de rede se torna um ponto (peer) da rede e está apto a ser um cliente e ao mesmo tempo um roteador de mensagens para clientes que estejam mais distantes do gateway da rede. Normalmente, todas as interfaces que suportam o modo cliente, também suportam o modo Ad-Hoc.
- Modo Monitor: permite que todo o tráfego observado na camada física seja submetido diretamente para o sistema operacional. Ou seja, ao invés de converter para o formato ethernet, a comunicação é capturada e apresentada no formato IEEE 802.11. Dessa forma, é possível capturar os frames de gerenciamento, frames de controle e o cabeçalho do pacote 802.11 sem requerer autenticação ou associação com um ponto de acesso. Estes frames, por não utilizarem qualquer tipo de cifragem, permitem a identificação de informações valiosas para implementar ataques sobre a rede wireless, inclusive sobre a criptografia WEP. Além disso, utilizando uma técnica conhecida como “channel hopping”,é possível obter informações de todos os canais e analisá-las em um programa de sniffer. Por fim, nem todas as placas suportam este modo de operação e a configuração pode variar de acordo com o chipset utilizado pela interface. Não existem muitas interfaces e drivers com suporte a este modo de operação para o sistema operacional Windows.

Um ponto de acesso é considerado um portal, pois permite a conectividade de clientes de uma rede 802.11 (wireless) com redes 802.3 (Ethernet). Pontos de acesso estão diponíveis com diversas opções de hardware e software.

Segurança

Existem diversas ameaças inerentes às redes wireless. De acordo com uma pesquisa do grupo Gartner realizada em 2004, foi apontado que até o final de 2006, 70% dos ataques sobre as redes wireless ocorreram devidos a problemas de configuração. O resultado desta pesquisa permite concluir que a primeira grande ameaça para redes wireless é o desconhecimento. Existem diversas forma de desconhecimento, as quais estão relacionadas tanto com o usuário final quanto a concepções errôneas por parte das organizações. A relação existente entre a segurança do equipamento com a própria privacidade ainda não está totalmente disseminada para o usuário final, que compra os equipamentos "plug&play", os conecta em sua rede sem qualquer tipo de configuração de segurança.

Já as organizações nem sempre estão muito preocupadas com a segurança de seu ambiente, ignorando o risco que uma rede mal configurada ou um ponto de acesso não autorizado traz para o ambiente de rede, refletindo na organização de forma geral. Outra ameaça bastante comum é a utilização de equipamentos com a potência de sinal mal ajustada. Neste caso, o problema incide no tamanho do raio de propagação de RF, que pode permitir que instalações vizinhas, prédios e casas, tenham acesso ao sinal emitido. No entanto, a principal ameaça trata-se da possibilidade de realizar ataques de Negação de Serviço (DoS) efetivos e eficazes, sendo que não é possível adotar medidas pró-ativas, somente reativas.

Obter uma melhor compreensão dos elementos de segurança da LAN wireless e implementar algumas das práticas recomendadas pode ajudar bastante para que você possa alcançar os benefícios da rede wireless.

Elementos de segurança wireless

Quatro ações básicas que podem ajudar a proteger uma rede wireless:

- **Desabilitar o broadcast do SSID da rede no AP:** Sem o SSID sendo publicado regularmente no espaço pelo AP, as estações wireless adjacentes não vão perceber a existência do AP. Somente as estações configuradas para o SSID da rede wireless vão enxergar o AP.
- **Proteger dados enquanto estão sendo transmitidos através de criptografia:** Simplificando, a criptografia é um código secreto: ele traduz seus dados em informações incompreensíveis que apenas o destinatário entende. A criptografia exige que tanto o remetente quanto o destinatário tenham uma chave para decodificar os dados transmitidos. A criptografia mais segura usa chaves ou algoritmos bastante complicados que mudam regularmente para proteger os dados. Três soluções também estão disponíveis para criptografia: Wired Equivant Privacy (WEP), Wi-Fi Protected Access (WPA) e Wi-Fi Protected Access 2 (WPA2)
- **Ativar filtros de MAC address:** Através da descrição dos MAC addresses que podem se conectar ao AP podemos garantir que somente equipamentos autorizados farão uso da rede wireless.
- **Evitar conexões não-oficiais através da eliminação de pontos de acesso falsos:** Um funcionário bem intencionado que utilize uma rede wireless em casa pode comprar um ponto de acesso barato e conectá-lo a uma entrada de rede sem pedir permissão. Eles são conhecidos como pontos de acesso falsos e a maioria é instalada por funcionários, e não por invasores mal intencionados. Verificar os pontos de acesso falsos não é difícil. Algumas ferramentas podem ajudar e a verificação pode ser feita com um laptop wireless e software ou usando dispositivo de gerenciamento que colete dados a partir dos seus pontos de acesso.