
MÓDULO DE:

# PROJETO DE REDES

AUTORIA:

## FILIPE DE CASTRO FERREIRA

Módulo de: Projeto de Redes
Autoria: Filipe de Castro Ferreira

Primeira edição: 2008

CITAÇÃO DE MARCAS NOTÓRIAS

Várias marcas registradas são citadas no conteúdo deste módulo. Mais do que simplesmente listar esses nomes e informar quem possui seus direitos de exploração ou ainda imprimir logotipos, o autor declara estar utilizando tais nomes apenas para fins editoriais acadêmicos.
Declara ainda, que sua utilização tem como objetivo, exclusivamente a aplicação didática, beneficiando e divulgando a marca do detentor, sem a intenção de infringir as regras básicas de autenticidade de sua utilização e direitos autorais.
E por fim, declara estar utilizando parte de alguns circuitos eletrônicos, os quais foram analisados em pesquisas de laboratório e de literaturas já editadas, que se encontram expostas ao comércio livre editorial.

# Apresentação

A etapa de projetar uma rede de computadores é, sem dúvida, uma das etapas mais importantes na informatização de um sistema.

Como será a topologia; qual a carga de dados que trafegará pela rede; como será o modelo de segurança; estas são algumas perguntas que o projetista de rede deve responder para garantir um Projeto de Redes eficiente e de qualidade.

Um Projeto de Rede mal elaborado trará sérios problemas à organização.

Uma dica para o aluno que se interessar em se aprofundar neste assunto é buscar cursos oficiais de cabeamento estruturado (os da Furukawa são os mais conhecidos) e de redes (recomendados da Cisco).

# Objetivo

Proporcionar ao aluno uma visão arquitetural em um Projeto de Redes de Computadores, inserindo conceitos básicos e avançados das tecnologias e técnicas mais utilizadas na construção de uma Rede de Computadores.

O conteúdo deste módulo será focado na construção do Projeto de Rede de computadores. O objetivo principal deste módulo é dar subsídio ao aluno, ao se deparar com a necessidade de Projetar (ou participar da equipe de Projeto) uma rede de computadores, fazê-lo de forma segura e precisa.

# Ementa

Revisão dos conceitos básicos de redes de computadores; Definição, Classificação e Princípio de Transmissão; Meios de Transmissão e Topologias; Modelo OSI; Dispositivos de Conectividade; Subsistemas do Cabeamento Estruturado; Sala de Entrada de Telecomunicações e Sala de Equipamentos; Sala de Equipamentos; Sala Cofre; Rede Primária e Armário de Telecomunicação; Rede Secundária; Área de Trabalho e Administração; Administração - Plantas e Desenhos; Contornando problemas de ruído – Aterramento; Redes sem Fio - compreender o conceito de redes sem fio; tipos de redes sem fio, características do padrão IEEE e suas especificações; Compreender quais são os elementos de hardware de uma rede sem fio WLAN; Compreender o conceito de Visada e antenas adequadas para cada situação; Explorar as tecnologias Bluetooth e WiMax; Vulnerabilidade das Redes sem fio; Aplicação de redundância e contingência; O que é uma VLAN?; Entender o uso de um Firewall; Entendendo os Proxies; Entender as Redes Privadas Virtuais – VPN; Limitações de uma VPN; Compreender uma DMZ.

# Sobre o Autor

Pós-Graduado em Engenharia de Sistemas, Pós-Graduado em Gerência de Projetos e Bacharel em Sistemas de Informação.

Consultor Microsoft e Gerente de Projetos. Certificado Microsoft (MCTS) em SharePoint 2007, Project Server 2007 (EPM 2007) e MS Project 2007.

Experiência como projetista e administrador de redes Windows e Linux.

Tutor na ESAB (Escola Superior Aberta do Brasil) em Cursos de Pós-Graduação.

Experiência como Gerente de Fábrica de Software, Analista em Projetos de desenvolvimento de Sistemas e conteúdos para EAD.

# SUMÁRIO

# UNIDADE 1

*Objetivo: Apresentar pré-requisitos do módulo, objetivos e metas.*

**Primeiras Palavras**

Seja bem-vindo ao módulo Projeto de Redes!

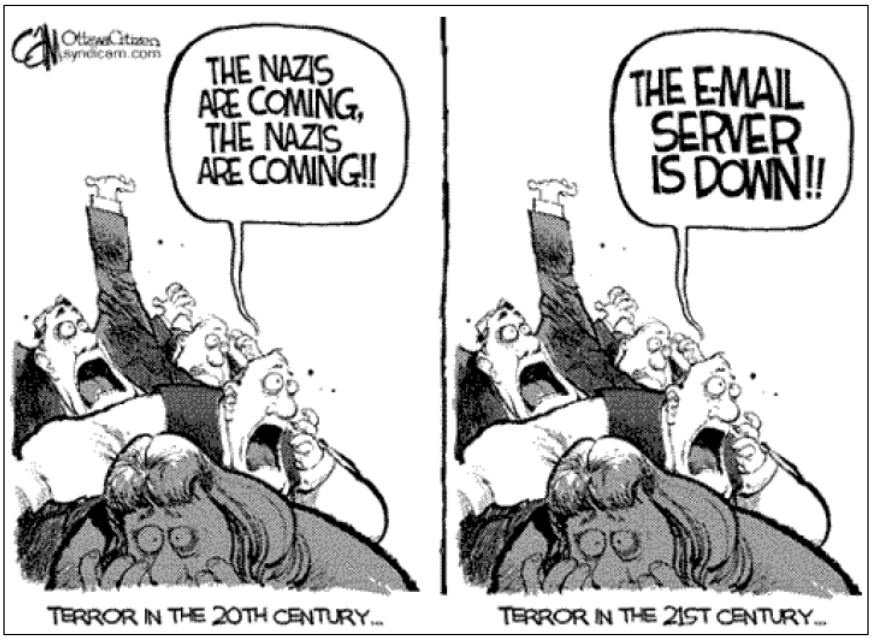
Este módulo foi criado como parte integrante do curso lato sensu Rede de Computadores da ESAB. Entretanto, pode ser estudado separadamente como conhecimento complementar no estudo de Rede de Computadores.

***Pré-requisitos***

Ter estudado ou conhecer Conceitos de Redes de Computadores (Conectividade, Tipo de Mídias, Meios de Acesso, etc), Serviços de Redes (Tipos de Servidores, DNS, DHCP, Protocolos, entre outros), Topologias (Anel, Estrela, etc) e Tipos Cabeamentos (Coaxial Par trançado, Fibra Óptico e demais).

***Sobre o Módulo***

Este módulo de estudos é uma compilação dos pontos mais importantes a serem analisados em um Projeto de Redes, portanto não esgotará o conhecimento sobre esta disciplina. O aluno deve pesquisar em livros, internet, contratar consultoria ou qualquer outro meio que possa apoiá-lo, caso se depare com uma situação em que não se sinta confortável para responder.



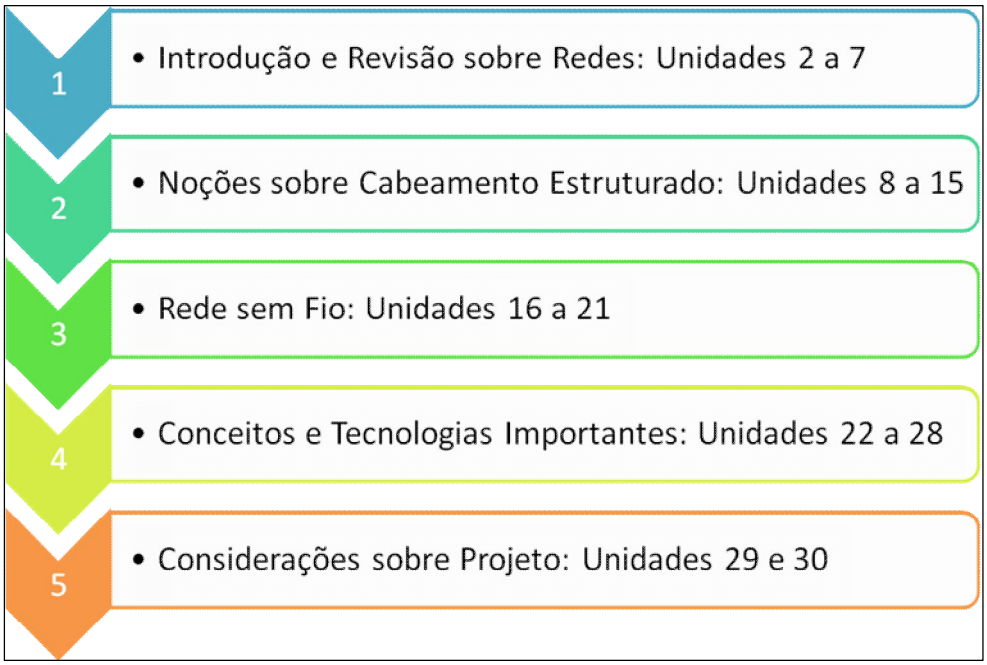

Ao final deste módulo, o aluno terá condições de Projetar Redes de Computadores que atendam as necessidades específicas, identificando seus riscos, custos, desempenho, confiabilidade e segurança.

Serão abordados aspectos e tecnologias que possibilitará projetar redes de computadores de diferentes tamanhos e características.

### *Organização e Diretrizes de Estudo*

Este módulo apresentará uma quantidade significativa de conhecimentos, entretanto não se aprofundará em nenhuma dos assuntos. Portanto, a sequência lógica de ensino deve estar clara para que o aluno se sinta confortável e apto a pesquisar, caso deseje se aprofundar em determinado item.

O módulo foi agrupado em 5 grupos de conhecimentos:



# UNIDADE 2

*Objetivo: Introduzir o módulo de Projeto de Redes, apresentar diretrizes para construção de um Projeto.*

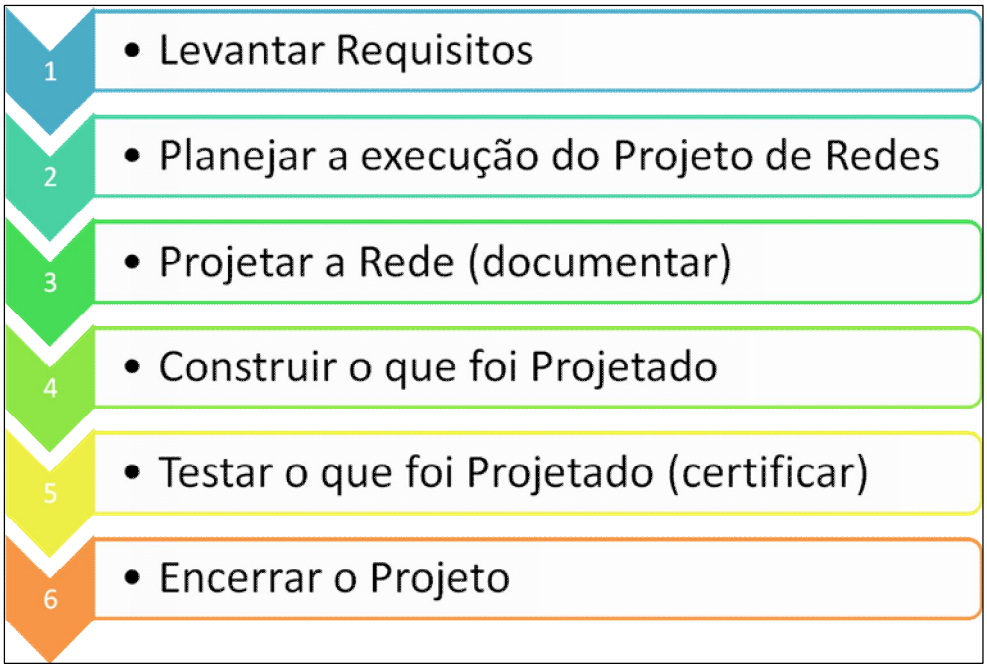
**Introdução ao módulo**

As redes de computadores atuais caracterizam-se tanto pela sua especificidade quanto pelas suas diversidades tecnológicas disponíveis. Os sistemas de comunicação exigem cada vez maior confiabilidade e poder de capacidade dos meios de transmissão, uma vez que o grau de complexidade desses sistemas torna-se maiores.

A implantação de uma topologia de rede não é algo tão simples, principalmente as que devem dar suporte a um conjunto de aplicações. Cada arquitetura possui características e particularidades que atendem certas necessidades e outras não.

O principal objetivo de uma rede de computadores é compartilhar recursos e possibilitar a comunicação confiável entre os diversos sistemas, melhorando o fluxo e o acesso a essas informações.

Para construir um Projeto de Redes, o profissional deve seguir, basicamente, os seguintes passos:




1. ***Levantar Requisitos:***

   - O que será construído? Qual objetivo? Atenderá quais sistemas?

2. ***Planejar a execução do Projeto de Redes***

   - Qual o escopo? Quanto tempo? Qual é orçamento do Projeto? Quantas pessoas você precisará para construir esta rede? Como estas pessoas serão gerenciadas e comunicadas? O que precisará ser comprado/adquirido? Como você poderá garantir a qualidade da rede? Quais são os riscos identificados que impactarão em seu projeto e como mitigá-los?

3. ***Projetar a Rede (arquitetar/documentar)***

   - Desenho lógico, desenho físico, documentação dos equipamentos, etc.

4. ***Construir o que foi Planejado***

   - Fase em que deverá executar a construção física da rede.

5. ***Testar o que Projetado (certificar)***

   - O que foi construído atendeu aos Requisitos? (passo 1). A rede foi certificada por uma empresa certificadora?

6. ***Encerrar o Projeto***

   - Os contratos foram encerrados corretamente? O cliente está satisfeito com o que foi construído? Alguma coisa ficou para trás?

Este módulo de estudos focará no “Passo 3” (Projetar a Rede) e trará dicas dos demais passos. Veja que o Projetista de Redes, assim como qualquer projetista, não deve se focar apenas em questões técnicas do conteúdo – boa comunicação e relacionamento interpessoal são imprescindíveis para equalizar a necessidade do cliente e o que será entregue.

**Dica**

Há diversos cursos especializados em como Planejar e Gerenciar Projetos. Faça uma pesquisa pela Internet por “Especialização em Gerenciamento de Projetos”.

**Fórum**

**FÓRUM I**

Em sua opinião, na fase de Levantamento de Requisitos, o que acha mais importante na hora de documentar o que o cliente deseja?

# UNIDADE 3

*Objetivo: Rever - Definir, Classificar e Conhecer o Princípio de Transmissão.*

**Definição de Rede de Computadores**

Um conjunto de dispositivos capazes de se comunicar através de mensagens (microcomputadores, terminais, impressoras, computadores de grande porte, etc), capazes de trocar informações e compartilhar recursos, interligados por um sistema de comunicação.

***Benefícios das Redes***

- Acessar dados armazenados em alguma outra área.
- Permitir que um grupo de computadores compartilhem dispositivos caros que seriam utilizados por somente uma pessoa.
- Dar aos usuários um meio de comunicarem-se eletronicamente, utilizando os computadores pessoais já existentes.

***Classificação das Redes***

As Redes de Computadores podem ser classificadas, basicamente, quanto à:

- **Velocidade de transmissão**
  - Baixa (ex: modem), média (ex: ADSL) e alta velocidade (ex: fibra óptica)
- **Extensão geográfica**
  - Locais (LAN), campus (CAN), Metropolitanas (MAN) e Longa Distância (WAN)

- **Confiabilidade**
    - Confiáveis (Funcional, mesmo sob falhas) e não confiáveis
- **Modo de transmissão**
    - Determinísticas e não determinísticas

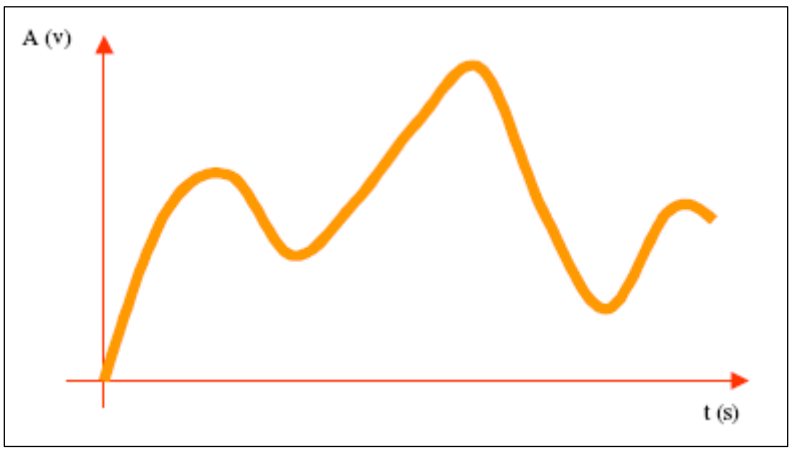
***Princípios de Transmissão***

Referem-se como os sinais são transmitidos através dos Meios de Comunicação (Cabos, Ar, etc)

Sinais são ondas (elétricas, eletromagnéticas ou luminosas) que se propagam através de algum meio físico, seja ele o ar ou um par de fios telefônicos. Sinais podem, assim, ser representados como uma função do tempo.

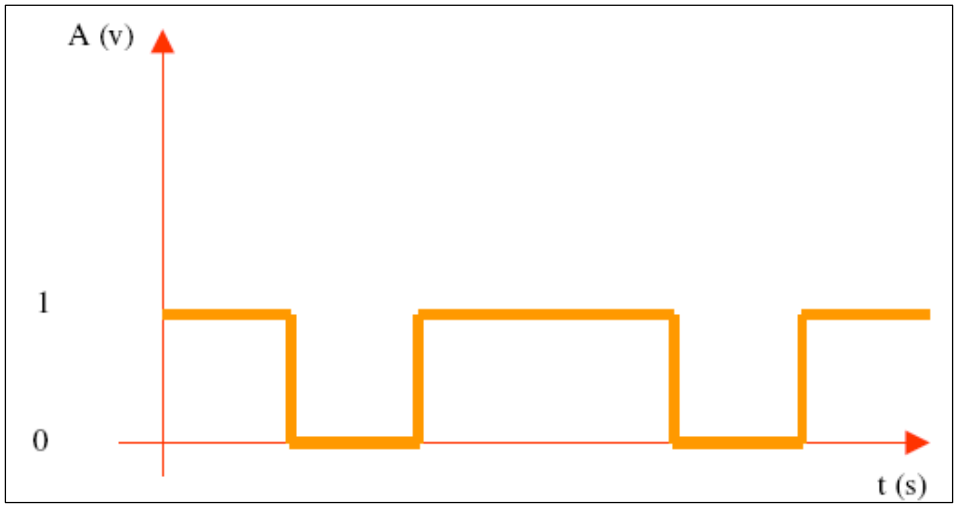
***Sinal Analógico***

Ocorre variação contínua do sinal ao longo do tempo. Ex: Voz e fontes sonoras.



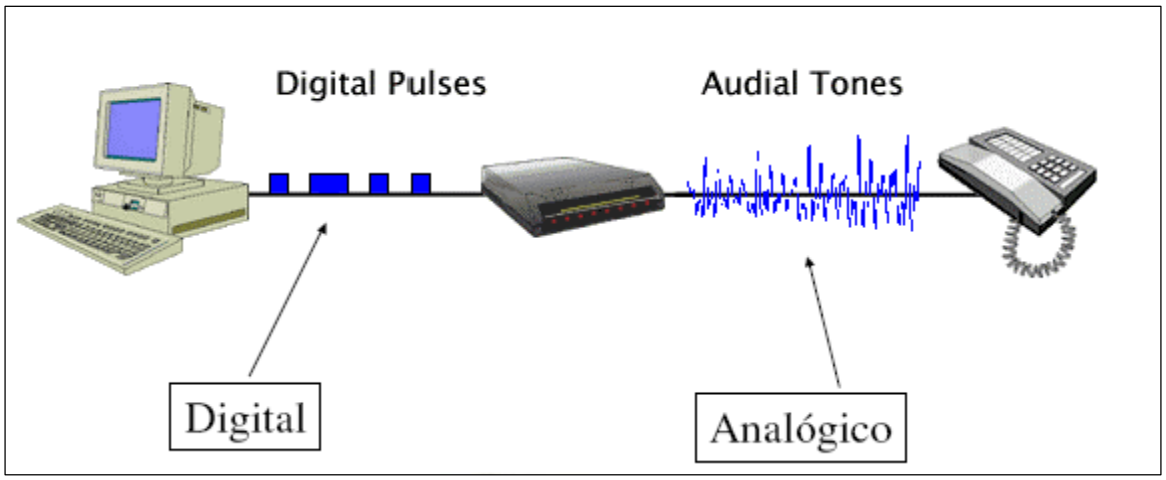
### *Sinal Digital*

Ocorre variação discreta do sinal ao longo do tempo, possui pulsos nos quais a amplitude é fixa. O sinal é construído através de uma sequência de intervalos de tamanho fixo iguais. Ex: Transmissão de informações do disco rígido para a CPU.




### *Modem*

O modem é um excelente exemplo de uso dos sinais analógico e digital, uma vez que o modem é responsável por modular e desmodular o sinal (e vice-versa).



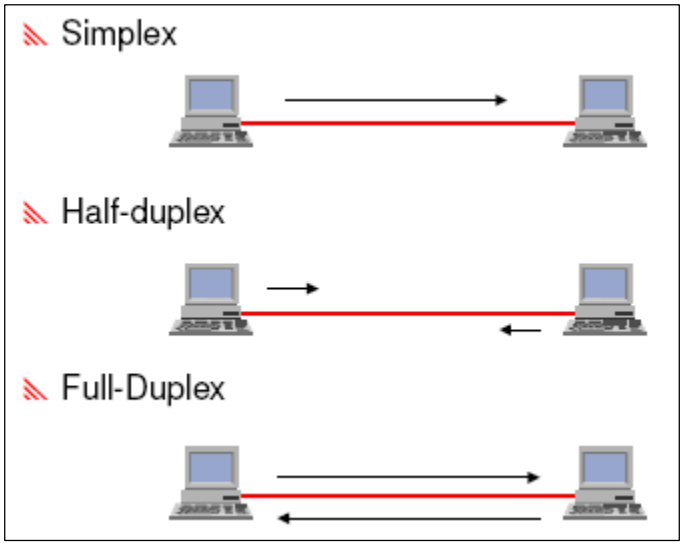
***Linhas de Transmissão***

As Linhas de Transmissão podem ser classificadas em:

Simplex – Os sinais são transmitidos em um único sentido. Ex: Rádio, Televisão, etc

Half-dulplex – Os sinais são transmitidos em ambos sentidos, entretanto apenas um dispositivo transmite por vez. Ex: Walk talk.

Full-duplex – Os sinais são transmitidos em ambos sentidos e simultaneamente. Ex: Telefone.



# UNIDADE 4

*Objetivo: Continuar a Revisão - Meios de Transmissão e Topologias.*

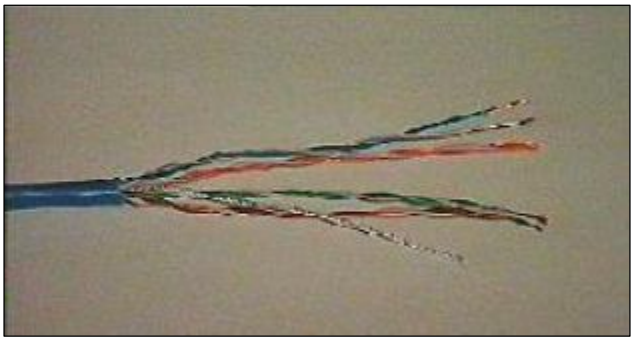
**Meios de Transmissão**

O Meio de Transmissão define como a comunicação é realizada entre computadores. É a codificação de dados na forma de energia. Ex: corrente elétrica, ondas de rádio, luz, etc.

Os principais Meios de Transmissão utilizados no mercado em Rede de Computadores:

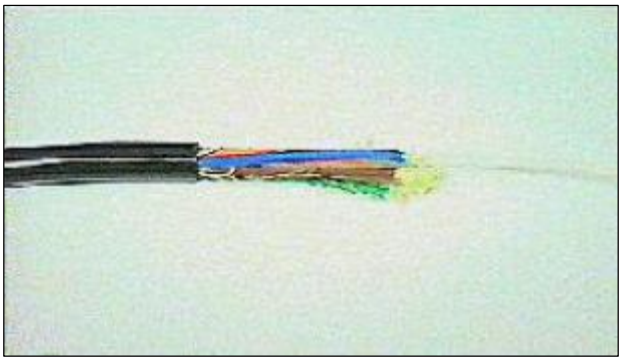
- ***Par Trançado***

É o cabo mais utilizado na implementação de redes locais, por sua flexibilidade e baixo custo.



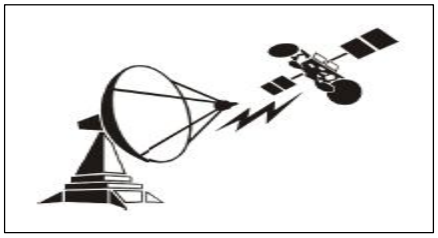
- ***Fibra Ótica***

São utilizadas em redes de longas distâncias, ou em locais em que haja necessidade de uma maior banda de transmissão. São imunes a interferência eletromagnética e ruídos, pois o sinal é transmitido através de feixe de Luz. Ex: Backbone, ligação entre Servidores, etc.



- ***Ar***

É utilizado nos Projetos de Rede sem Fio, quando a utilização de cabos se torna inviável.



Para se definir o Meio de Transmissão que será utilizado no Projeto, as seguintes características devem ser observadas:

- Taxa de transmissão
- Tecnologia de transmissão
- Extensão Geográfica das redes
- Aspectos econômicos
- Confiabilidade

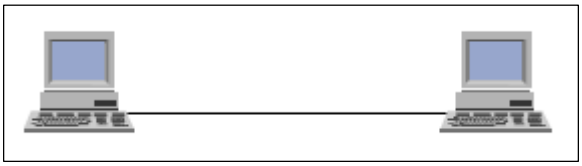
***Topologia***

É o layout físico de interconexão dos equipamentos de uma rede.

Os principais tipos utilizados nos Projetos de Rede são:

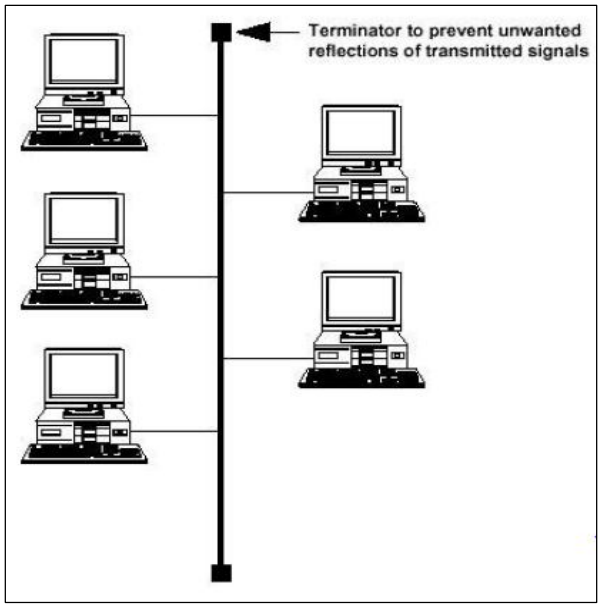
- ***Ponto a Ponto***

Um meio físico para cada par de computadores. Foi o Modelo adotado pelas primeiras redes e ainda é utilizado em tecnologias como Infra Vermelho e BlueTooth.



- ***Barramento***

É o compartilhamento do mesmo meio físico (barramento) pelos dispositivos da rede.



***Vantagens***

- Utilização de menor quantidade de cabos
- Gerenciamento mais simples dos cabos

***Desvantagens***

- Complexidade mediana do projeto
- Extremamente necessário um planejamento prévio
- Difícil manutenção e conservação
- A falha de um cabo derruba toda a rede

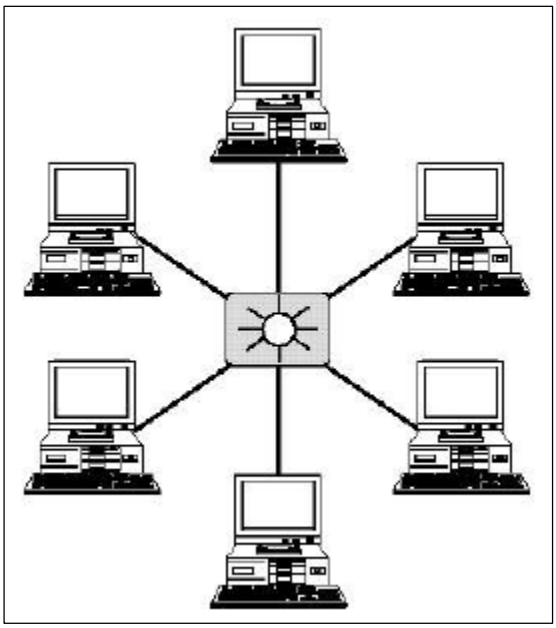
# UNIDADE 5

*Objetivo:Continuar  a Revisão - Topologias.*

**Estrela**

Caracteriza-se pela utilização de um Dispositivo Centralizador (Hub ou Switch), responsável por interligar todos os dispositivos da rede.

É a topologia mais utilizada e recomendada na construção de novas Redes de Computadores.



***Vantagens***

- Projeto e roteamento de cabo excepcionalmente fácil
- Necessidade mínima de planejamento prévio
- A mais simples em termos de manutenção e conservação

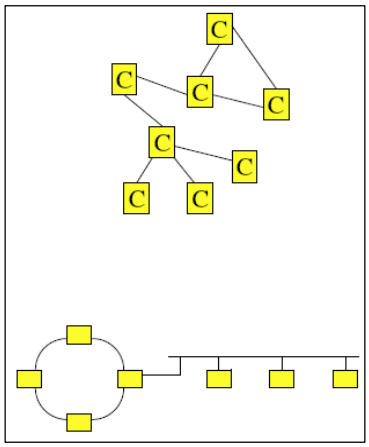
- O eixo central fornece um ponto de isolamento central para qualquer nó
- Pode acomodar outras topologias lógicas
- A topologia de rede mais confiável

***Desvantagens***

- Maior quantidade de cabos
- Ponto central de falha: se o centro for destruído, toda a rede falha.

***Híbrida***

Caracteriza-se por aproveitar vantagens de diversas topologias diferentes. Melhor compatibilidade com soluções específicas.



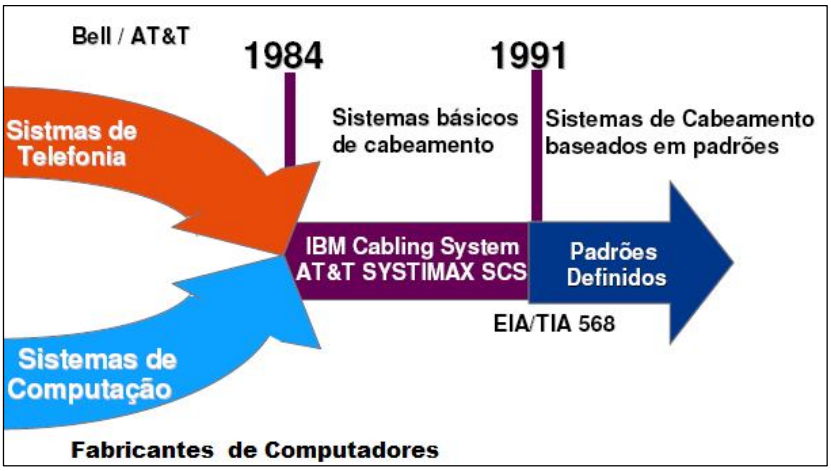
# UNIDADE 6

*Objetivo: Continuar a Revisão - Modelo OSI*

**Padrões Internacionais**

São acordos documentados contendo especificações técnicas para definir como um produto específico será projetado ou desenvolvido para evitar problemas como:

- Integração
- Aparecimento de Arquiteturas proprietárias
- Falta Padronização - Estrutura Única
- Ausência de Organismos de Padronização



## Estudo Complementar

Veja em Estudo Complementar um resumo das Normas de Cabeamento Estruturado

***Principais Organizações Internacionais de Padronização***

- **American National Standards Institute (ANSI)**
  - Representantes do governo e indústria
  - Define padrões para a indústria de eletrônicos e outros campos

- **Electronic Industries Alliance (EIA)**
  - Organização comercial composta de representantes de indústrias de eletrônicos dos Estados Unidos


- **Institute of Electrical and Electronic Engineers (IEEE)**
  - Sociedade internacional de profissionais de engenharia
  - Promove o desenvolvimento e a educação nos campos da Engenharia e Computação

- **International Organization for Standardization (ISO)**
    - Reunião de diversas organizações de padronização
    - Objetivo: Estabelecer padrões internacionais para facilitar a troca de informações

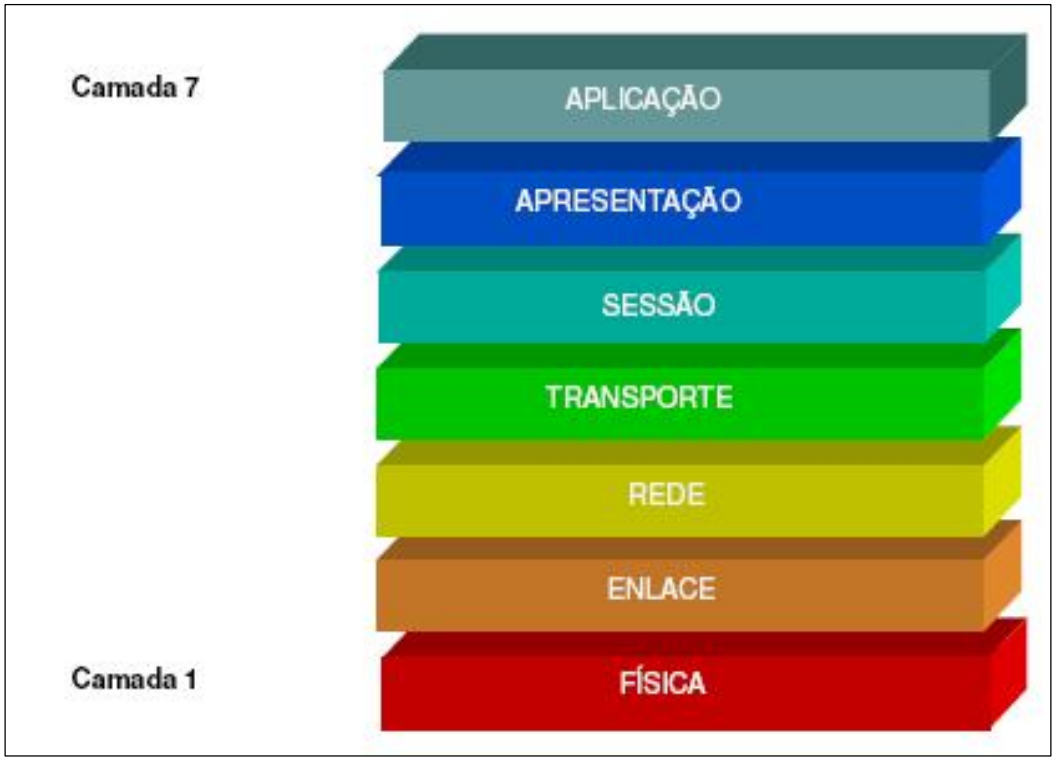

- **IETF (Internet Engeneering Task Force)**

- **International Telecommunication Union (ITU)**
    - Inicialmente chamada de Consultative Committee on International Telegraph and Telephony (CCITT)
    - Agência das Nações Unidas para regulação internacional das telecomunicações


- **ABNT (Associação Brasileira de Normas Técnicas)**

### *O Modelo OSI (Open System Interconnection)*

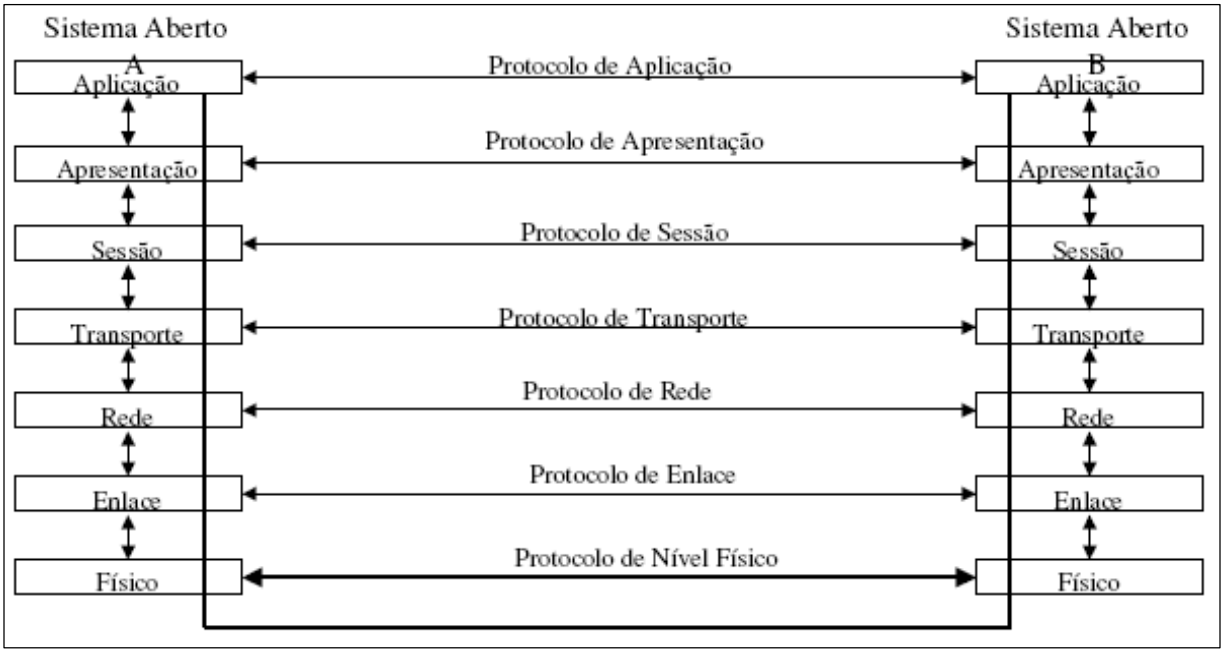
Modelo para compreensão e desenvolvimento da comunicação entre computadores, desenvolvido em 1980 pela ISO e divide a arquitetura de uma rede em 7 camadas.




- ***Principais Características do Modelo OSI***
  - o É um Modelo de Referência (conceitual) para interconexão de sistemas abertos.
  - o É uma Arquitetura Hierárquica - cada camada presta serviço a camada imediatamente superior.
  - o Padrão aberto e público – não há proprietário.
  - o Redes Locais e de Longa Distância – engloba a padronização de todos os tipos e tecnologias.

- ***Benefícios***

  - Conectividade – Permite a comunicação entre equipamentos de diferentes fabricantes.
  - Modularidade – Cada camada segmenta a função exercida por cada componente de serviço.
  - Facilidade de Implementação e utilização – Por ser um padrão aberto e público.
  - Confiabilidade – Por ser um padrão aberto e público, não está restrito a falhas de projeto de um determinado fabricante.
  - Demonstração do fluxo de tráfego entre as camadas do Modelo OSI entre dois sistemas:



# UNIDADE 7

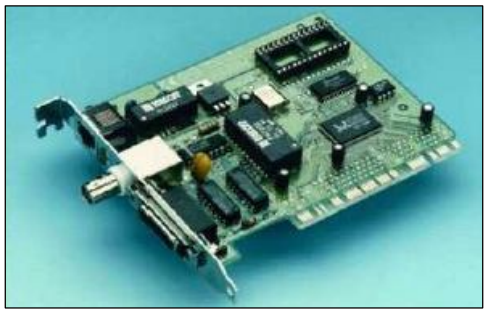
*Objetivo: Continuar a Revisão - Dispositivos de Conectividade.*

**Principais Dispositivos de Rede**

Vários dispositivos são usados em uma rede, cada um deles possuindo funções específicas. Como exemplos de equipamentos dedicados, podemos citar: as placas de rede, os hubs, switches, bridges, routers, etc, que possuem a finalidade de interpretar os sinais digitais processados na rede e encaminhá-los ao seu destino, obedecendo a um determinado padrão e protocolo.

***Placa de Rede***

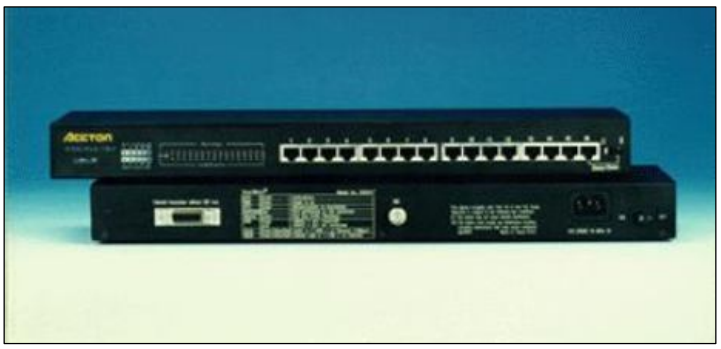
É a responsável em conectar os equipamentos fisicamente na rede.



Repetidores/HUB

***HUB***

Também conhecido como Repetidor Multiporta. Promove um ponto de conexão física entre os dispositivos de uma rede (concentrador).



HUB

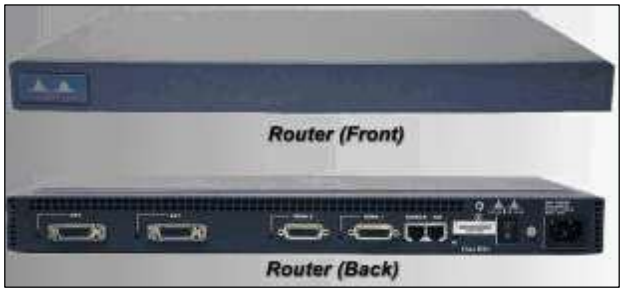
***Switch***

Um **comutador** ou **switch** é um dispositivo utilizado em redes de computadores para reencaminhar módulos (frames) entre os diversos nós. Possuem portas, assim como os concentradores (hubs) e a principal diferença entre um comutador e um concentrador, é que o comutador segmenta a rede internamente, sendo que a cada porta corresponde um domínio de colisão diferente, o que significa que não haverá colisões entre os pacotes de segmentos diferentes — ao contrário dos concentradores, cujas portas partilham o mesmo domínio de colisão. Outra importante diferença está relacionada à gestão da rede, com um Switch gerenciável, podemos criar VLANS, deste modo a rede gerida será divida em menores segmentos.

***Roteadores***

Responsável pela interligação das redes distintas. Permite que um dispositivo de uma rede LAN “X” comunique-se com dispositivos de outra rede LAN “Y”, como se as redes LAN fossem uma só.

Têm a função de decidir o melhor caminho para os "pacotes" percorrerem até o seu destino entre as várias LAN's e dividem-nas logicamente, mantendo a identidade de cada sub-rede.




***Bridge***

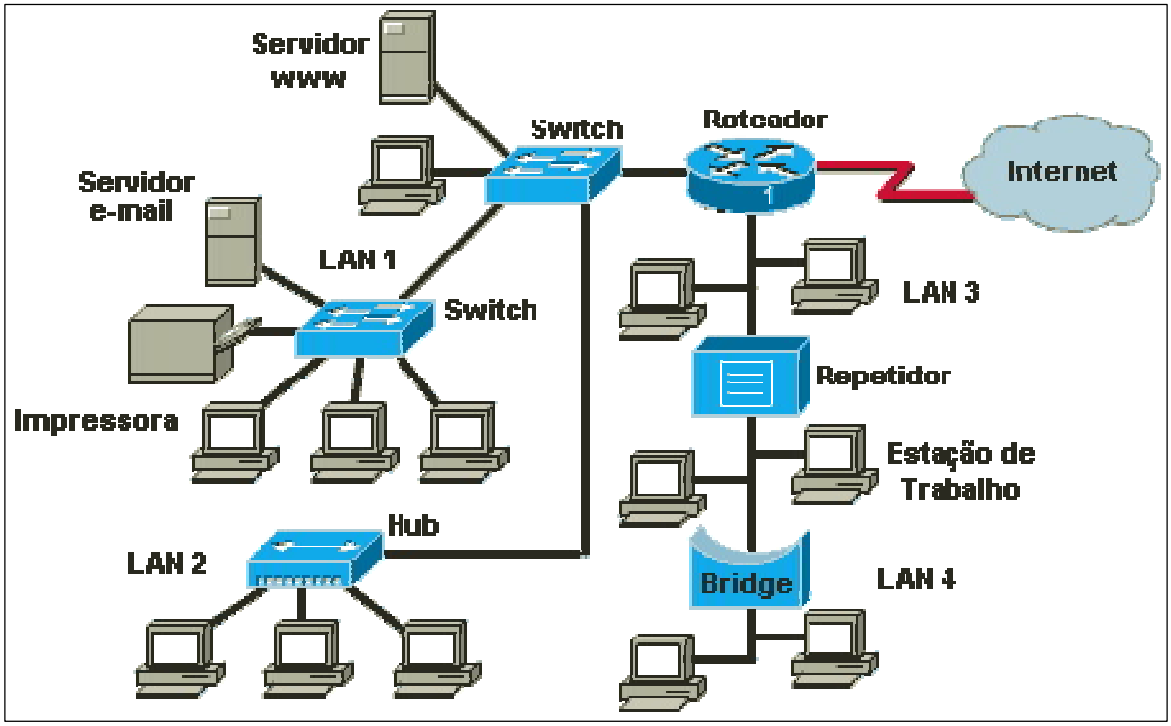
Bridge (ou ponte) é o termo utilizado em informática para designar um dispositivo que liga duas ou mais redes informáticas que usam protocolos distintos, ou iguais, ou dois segmentos da mesma rede que usam o mesmo protocolo, por exemplo, ethernet ou token ring. Bridges servem para interligar duas redes, como por exemplo ligação de uma rede de um edificio com outro.

Uma bridge ignora os protocolos utilizados nos dois segmentos que liga, já que opera a um nível muito baixo do modelo OSI (nível 2); somente envia dados de acordo com o endereço do pacote. Este endereço não é o endereço IP (internet protocol), mas o MAC (media access control) que é único para cada placa de rede. Os únicos dados que são permitidos atravessar uma bridge são dados destinados a endereços válidos no outro lado da ponte. Desta forma é possível utilizar uma bridge para manter um segmento da rede livre dos dados que pertencem a outro segmento.

É freqüente serem confundidos os conceitos de **bridge** e **concentrador** (ou hub); uma das diferenças, como já enunciado, é que o pacote é enviado unicamente para o destinatário, enquanto que o hub envia o pacote em broadcast.

***Gateway***

A interação entre esses dispositivos permite o compartilhamento das informações entre todos os usuários da rede. Veja o exemplo abaixo de uma rede de comunicação de dados que utiliza quase todos os equipamentos descritos anteriormente.




## Atividades

ATENÇÃO! Para garantir a qualidade da aprendizagem, não dê continuidade aos estudos sem antes realizar as atividades encontradas na lista 1 (ATIVIDADE 1).

# UNIDADE 8

*Objetivo: Conhecer Cabeamento estruturado – Entender o Cabeamento Estruturado.*

**Início do estudo do conteúdo do módulo**

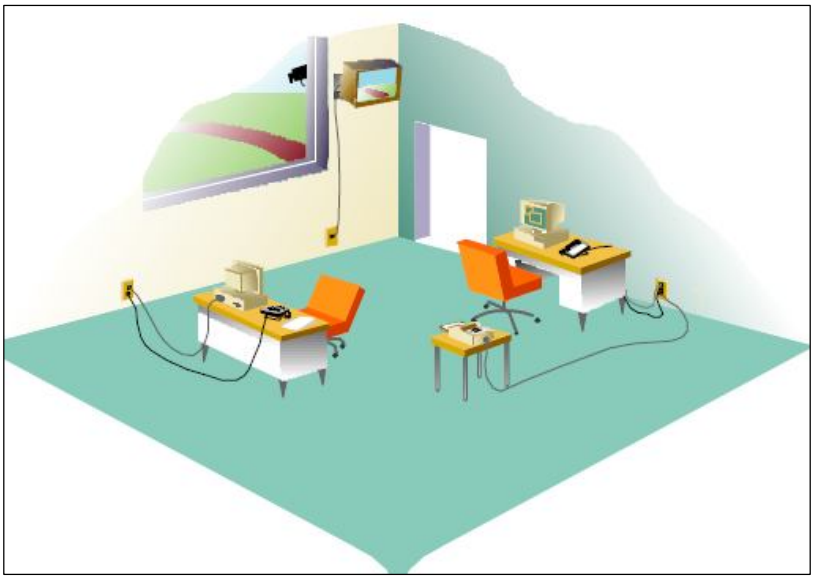
Após a revisão das primeiras cinco unidades – imprescindível para o nivelamento de conhecimentos, começaremos nos aprofundar no objetivo deste módulo.

Em seguida, trataremos um dos assuntos mais importantes deste módulo de estudos – o cabeamento estruturado. É a base para se entender e Projetar uma Rede de Computadores.

***Introdução a Cabeamento Estruturado***

Podemos definir Cabeamento Estruturado como uma infraestrutura flexível que deve suportar a utilização de diversos tipos de aplicações tais como: dados, voz, imagem e controles prediais, independente do fabricante ou do tipo de equipamento.

O objetivo conceitual do Sistema de Cabeamento Estruturado é de criar uma padronização para a diversidade de cabos utilizados nos ambientes residenciais e empresariais independente da sua aplicação. Oferece a seus usuários a possibilidade de usufruir de novos serviços quando necessários (pontos de conexão para dados, voz, imagem, alarmes, monitoração, etc.).



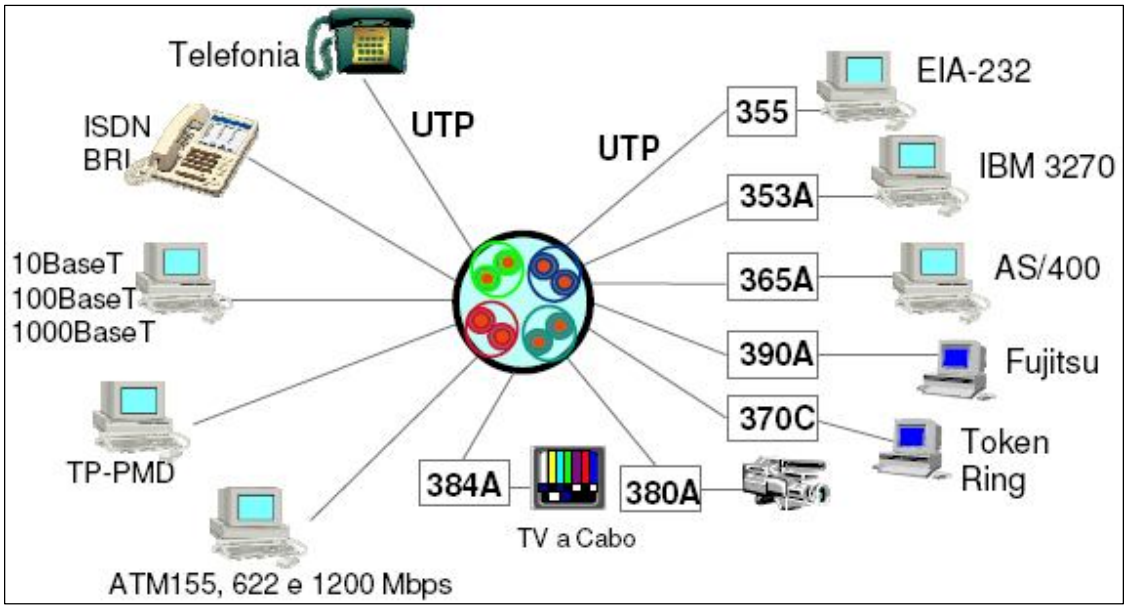
O Sistema de Cabeamento Estruturado visa padronizar as instalações atendendo as diversas necessidades, como rede de dados, telefonia e outras, independente do tipo de equipamento ou fabricante. Visa também solucionar problemas como crescimento populacional, evolução tecnológica, falhas nos cabos ou nas conexões entre outros.

***Por que utilizar o Cabeamento Estruturado?***

- O cabeamento estruturado possui a maior expectativa de vida numa rede (em torno de 15 anos).
- Os problemas de gerenciamento da camada física contabilizam 50% dos problemas de rede, em cabeamentos não estruturados.
- Sistema de Cabeamento Estruturado consiste apenas de 2 a 5% do investimento na rede.

***Vantagens do Cabeamento Estruturado***

- Suporte a diversos padrões de comunicação.
- Permite flexibilidade na mudança de layout.
- Possui arquitetura aberta possibilitando a conectividade entre produtos de diversos fabricantes.
- Aderência aos padrões internacionais.



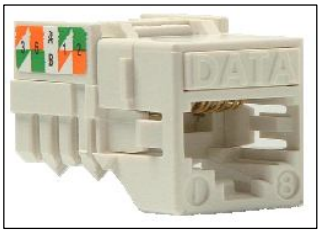

***Dispositivos que podem ser utilizados no Cabeamento Estruturado***

O Cabeamento Estruturado não se restringe apenas às Redes de Computadores. Os seguintes dispositivos também podem ser utilizados:

- Sistema Telefônico / Ramais de PABX
- Redes de Computadores / Computadores Pessoais
- Intercomunicação / Sonorização
- Televisão / TV a Cabo / CFTV

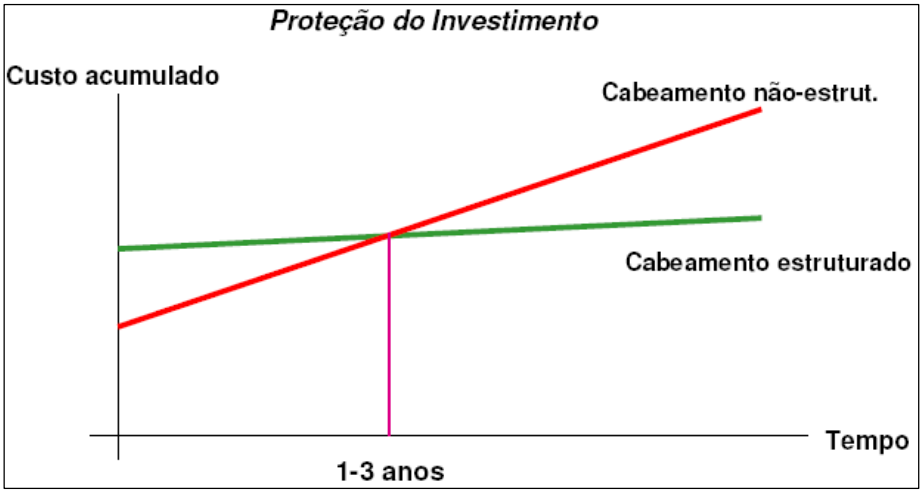
- Controle de Iluminação
- Controle de Acesso / Leitores de Cartão
- Sistemas de Segurança / Detectores de Fumaça
- Controles Ambientais (Ar Condicionado e Ventilação)

Todos estes equipamentos podem ser conectados a um Cabeamento Estruturado, pois utilizam o conector padrão RJ-45, como demonstra a figura a seguir:




***Investimento e Custo***

O investimento inicial em um Projeto de Cabeamento Estruturado, se comparado a um Cabeamento Não Estruturado, é maior. Entretanto, estudos demonstram que, em médio prazo, o Projeto de Rede que Não Estruturado possui Custo Acumulado superior a um Projeto que utiliza Cabeamento Estruturado.



## Fórum

**FÓRUM iI**

O que você pensa sobre cabeamento estruturado? A rede da sua empresa é estruturada? Procure saber com o administrador de redes e poste aqui.

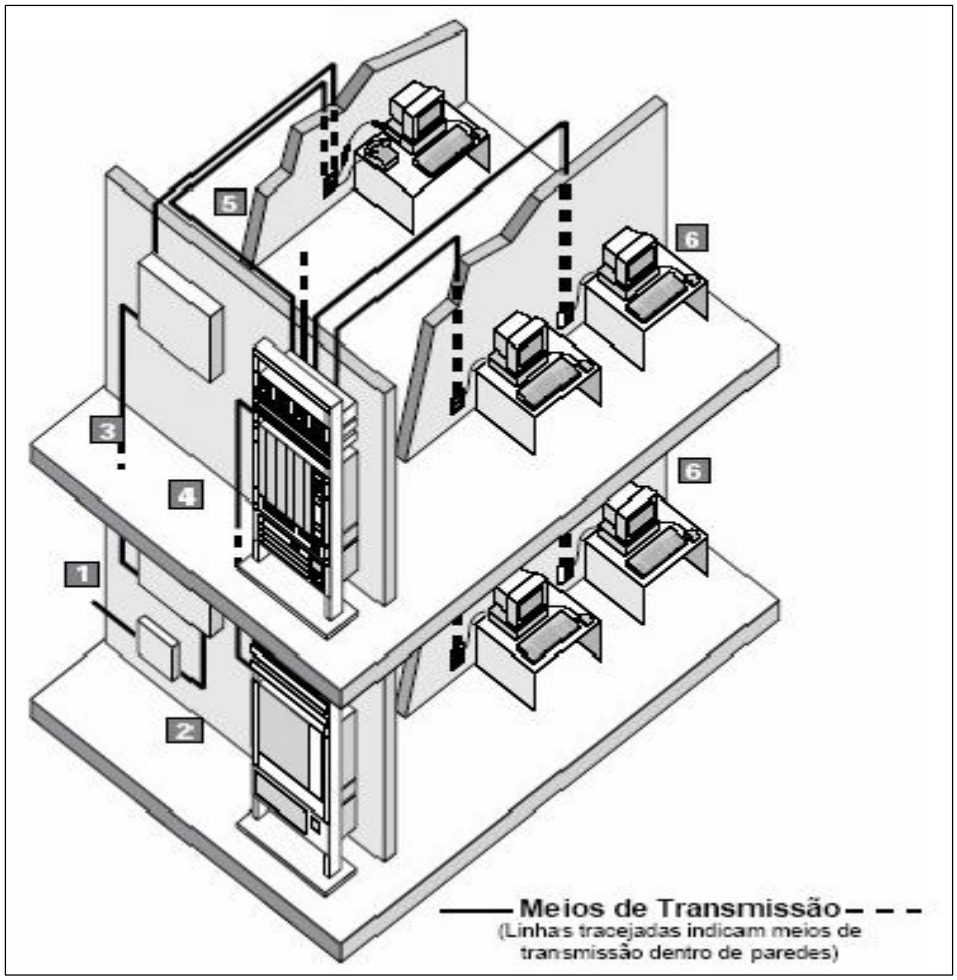
# UNIDADE 9

*Objetivo: Entender melhor Cabeamento estruturado – Subsistemas do Cabeamento Estruturado; Sala de Entrada de Telecomunicações e Sala de Equipamentos.*

**Subsistemas do Cabeamento Estruturado**

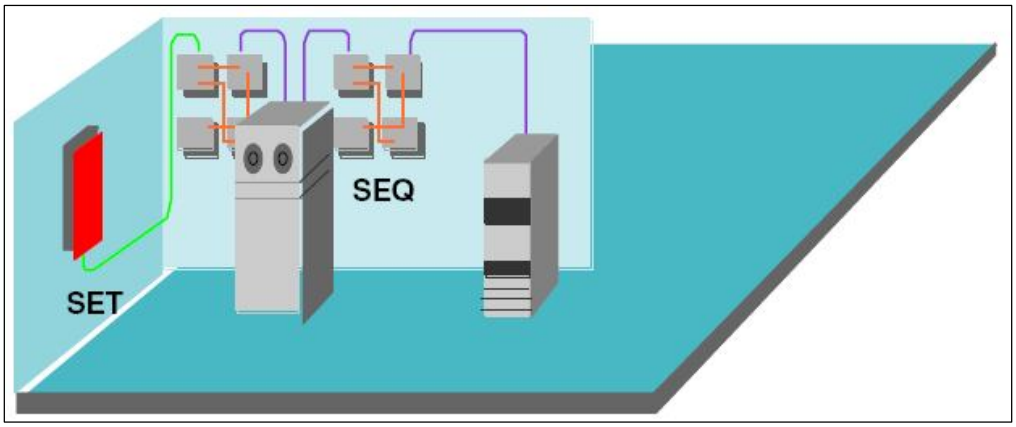
As normas ANSI/EIA/TIA-568-A e ANSI/EIA/TIA-606 dividem a instalação de um Cabeamento Estruturado em seis subsistemas, que são:

1. Sala de Entrada de Telecomunicações (SET)
2. Sala de Equipamentos (SEQ)
3. Rede Primária
4. Armário de Telecomunicações (AT)
5. Rede Secundária
6. Área de Trabalho (ATR)
7. Administração




### *1. Sala de Entrada de Telecomunicações (SET)*

É o ponto pelo qual se realiza a interface entre o cabeamento externo e o interno. Normalmente fica alocado no térreo ou subsolo, abrigando os cabos que vem das operadoras de serviços de telecomunicações ou de outras edificações.



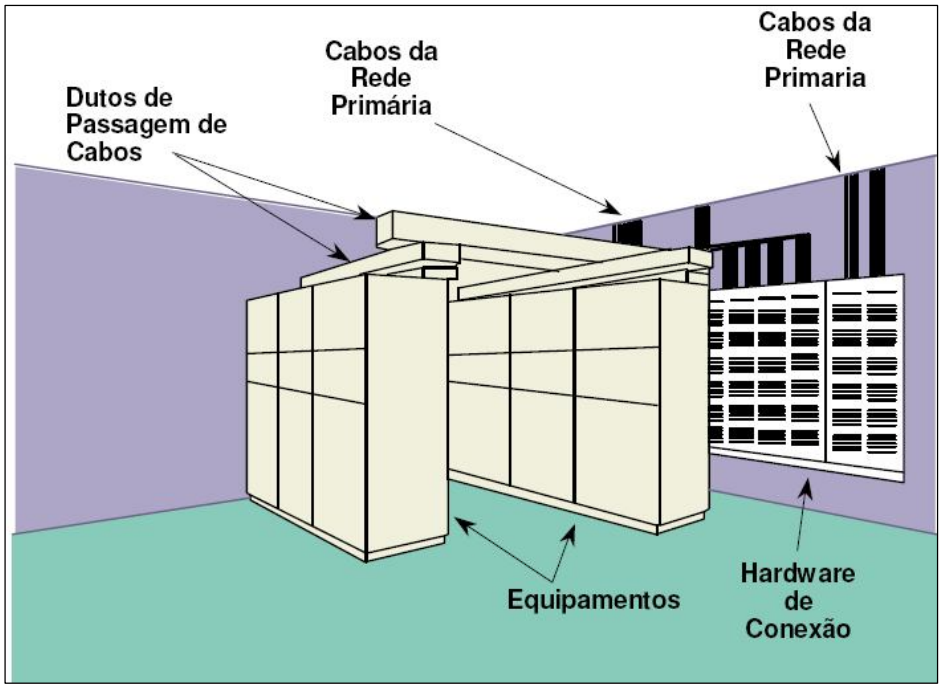

Isola física e logicamente o cabeamento interno do prédio dos alimentadores externos.

Principais funções:

- Proteção Elétrica dos Cabos que Chegam da Parte Externa (Cabeamento Campus).
- Aterramento do Cabeamento do Edifício.
- Conexões e Emendas Feitas entre o Cabeamento Externo e Interno do Edifício

### *2. Sala de Equipamentos (SEQ)*

Pode ser uma sala, um quadro ou um armário onde estão localizados os equipamentos ativos do sistema (PBX, vídeo, computadores, etc.), podendo haver suas interligações com sistemas externos.




***Recomendações***

***Localização***

- A SEQ NÃO deve ser localizada abaixo do nível da água
- Deve ser instalada longe de fontes de IEM (Interferência Eletromagnética)

***Ambiente***

- A SEQ deve ter acesso ao HVAC (Heating, Ventilation and Air Conditioning) principal
- A temperatura será controlada de 18 – 24 ºC
- A umidade deve estar na faixa de 30 a 55 %

***Acesso***

- Porta com tamanho mínimo de 90 x 200 cm
- Controle de acesso

***Energia elétrica***

- Deve possuir circuito de alimentação de energia em independente, terminando em uma caixa de força.
- Duas tomadas 110V / 15A

***Construção***

- O teto deve ter uma altura mínima de 2,5 mts
- Os pisos, paredes e tetos deverão ser vedados para reduzir o pó (pisos antiestáticos)

***Incêndio***

- Extintores de incêndio portáteis deverão ser mantidos na SE, próximos à entrada ou saída.
- Sensores (fumaça) e sistema de alarme de incêndio

# UNIDADE 10

*Objetivo:Estudar  Cabeamento estruturado – Subsistemas do Cabeamento Estruturado; Sala de Equipamentos; Sala Cofre.*

**Data Center**

Um Data Center, também conhecido como Centro de Processamento de Dados (Sigla: CPD ), é o local onde são concentrados os computadores e sistemas confiáveis (software) responsáveis pelo processamento de dados de uma empresa ou organização.

Normalmente projetados para serem extremamente seguros, contam com sistemas de última geração para extinção de incêndios, acesso controlado por cartões eletrônicos e/ou biometria, monitoramento 24x7, ar-condicionado de precisão, geradores de energia de grande capacidade e UPS (no-breaks) de grande porte para manter os equipamentos ligados, mesmo em caso de falta de energia.

**Midiateca**

Veja ao vídeo que demonstra os elementos de um Data Center.

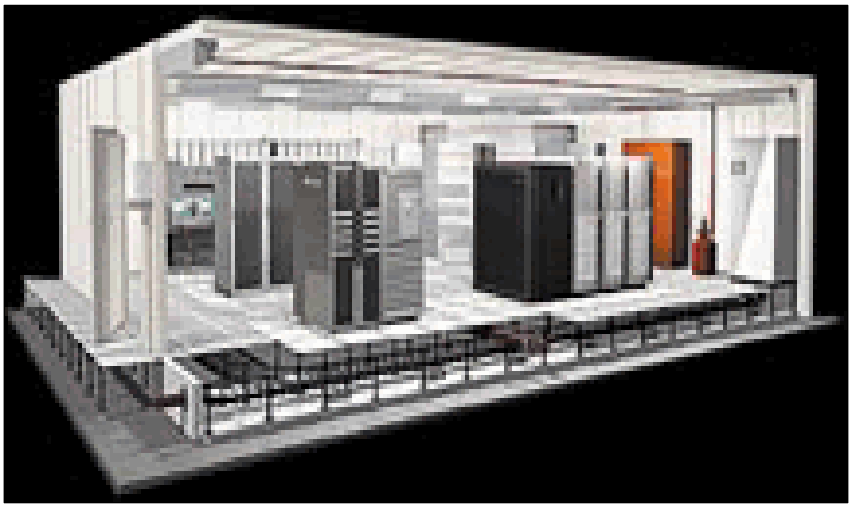
***Sala Cofre***

Dependendo do tamanho da infraestrutura de uma organização, por exemplo, um banco, cada segundo de paralisação do sistema tecnológico resulta em um prejuízo milionário.

Visando atender todas as necessidades de segurança e alta disponibilidade de um data center, assim como garantir uma proteção máxima dos dados e equipamentos de TI contra as principais ameaças físicas, uma solução completa e integrada de infraestrutura segura pode ser baseada em uma sala cofre modular e certificada.

Se o seu projeto de redes envolve um data center nada mais seguro que uma sala cofre para manter a integridade de sua estrutura e dados.

Uma Sala Cofre é uma sala fortificada que pode ser instalada em uma companhia, provendo um local seguro de invasões e outras ameaças. No mundo da TI uma sala cofre geralmente contém equipamentos como servidores de banco de dados, servidores de aplicação, chaves privadas e etc.



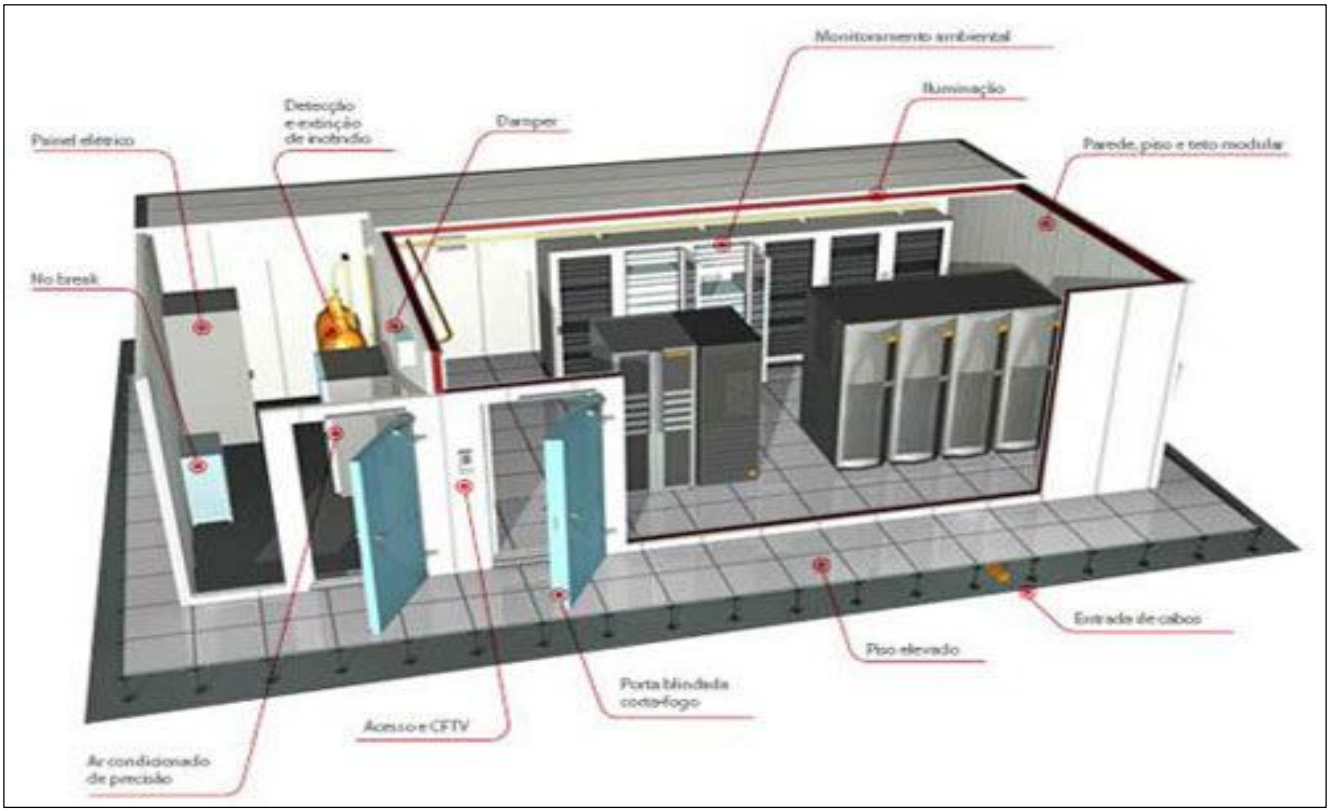
*Exemplo de sala cofre*

As salas cofre são um produto de alta tecnologia e que envolvem custos consideráveis, o que demanda um controle estrito para que não haja problemas de montagem, o que acarretaria um custo elevado.

São ambientes projetados para resistir a vários tipos de catástrofes. Suportam, por exemplo, temperaturas de até 1.200 graus Celsius, inundações, cortes bruscos de energia, gases corrosivos, explosões e até ataques nucleares.

***Riscos Físicos***

- Os principais riscos são: água, poeira, falta de climatização, fumaça/gases, incêndio, furto ou roubo, explosão, queda de energia, vandalismo, magnetismo e intrusão.
- Benefícios
- Integridade da informação e dos dados
- Alta disponibilidade dos equipamentos e infraestrutura de TI
- Alta Segurança física da informação e dos ativos de TI
- Flexibilidade de layout
- Melhor custo-benefício

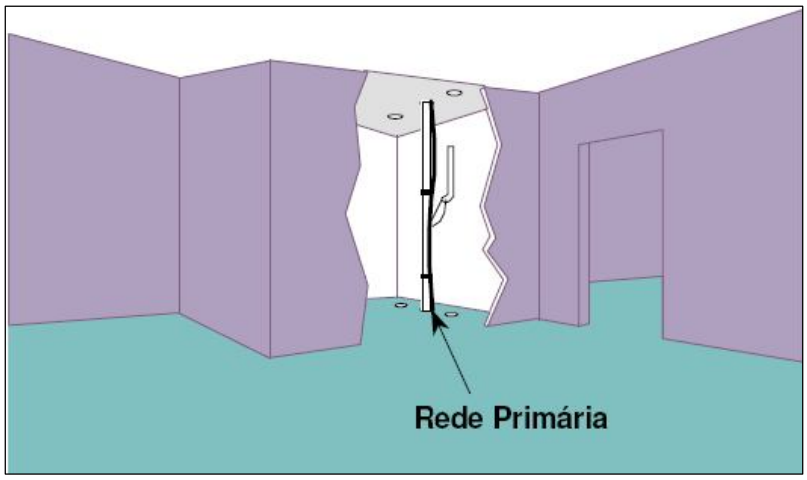


# UNIDADE 11

*Objetivo: Estudar Cabeamento estruturado – Subsistemas do Cabeamento Estruturado; Rede Primária e Armário de Telecomunicação.*

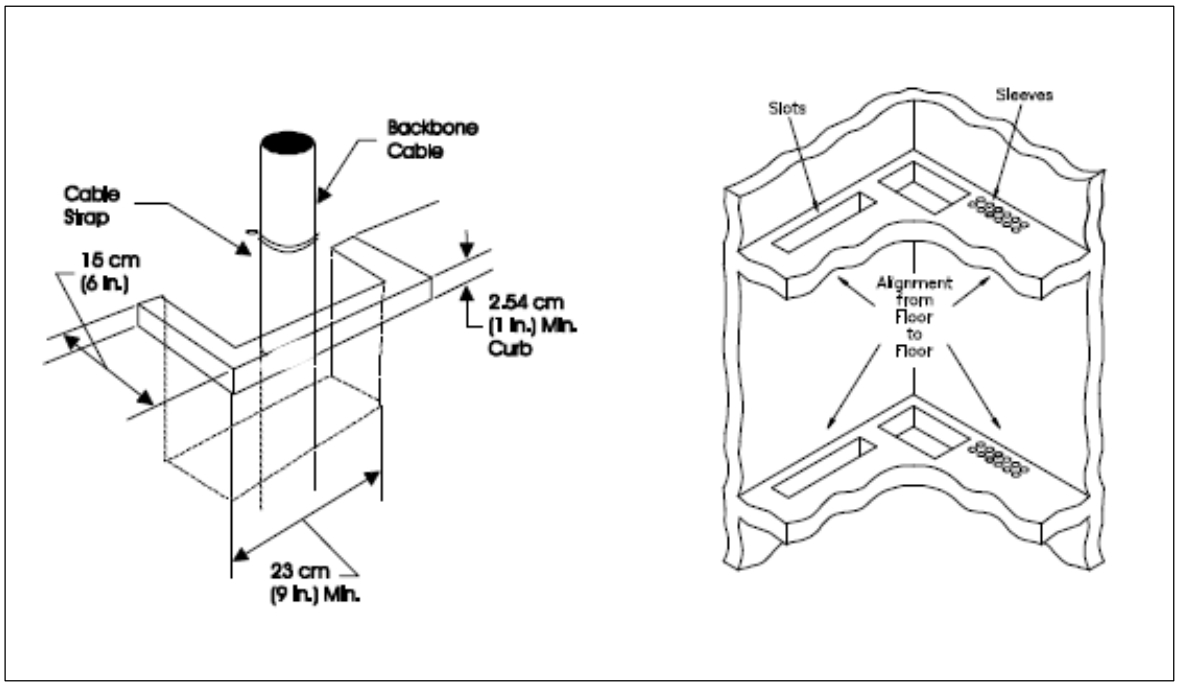
### 3. Rede Primária (backbone ou vertical)

É constituído pelos cabos que interligam a Sala de Equipamentos aos Painéis de Distribuição, Sala de Telecomunicações e Sala de Entrada de Telecomunicação. São denominados cabos primários, formando um conjunto permanente de cabos.



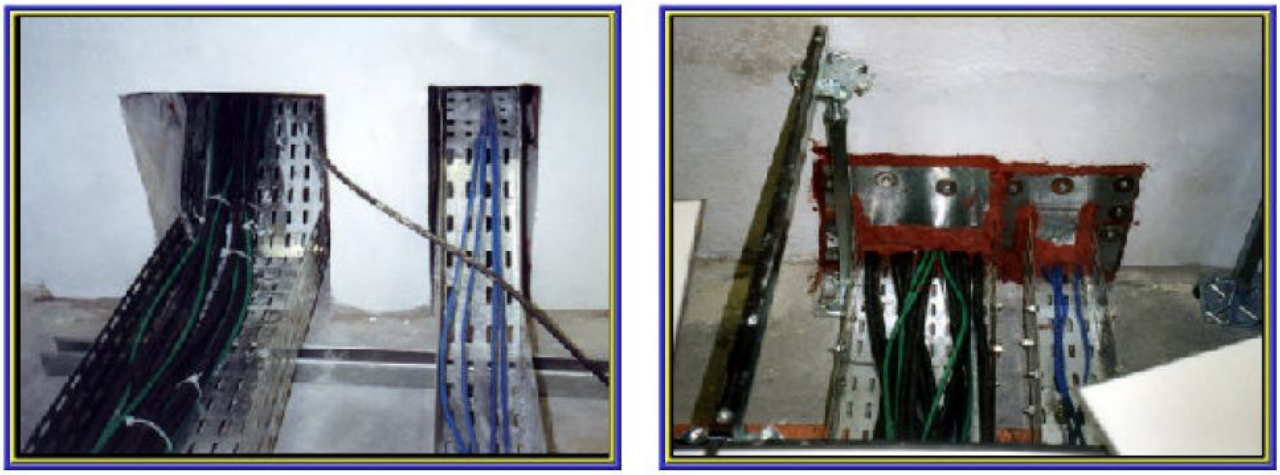

***Recomendações***

- Topologia Estrela
- Não mais que dois níveis hierárquicos de cross connects
- Patch cords para interligação de cross connects com tamanho máximo de 20 metros
- Procure evitar locais com alta incidência de IEM
- Aterramento segundo a norma EIA/TIA-607




***Barreira Contra Incêndio***

Consiste, basicamente, na aplicação de silicone antichamas no canal por onde passa a rede primária, isolando a chama, em caso de incêndio.



ANTES

DEPOIS

### 4. *Armário de Telecomunicações (AT)*

Locais de terminação dos cabos e funcionam como um sistema de administração do cabeamento e alojamento de equipamentos que interligam o sistema horizontal ao backbone (PABX, Switch, Sistema de Vídeo, etc).

***Principais Funções:***

- Concentrador da Rede Secundária
- Recebe, organiza e identifica todos os cabos originários das tomadas de informação.

***Racks***

Os cabos UTP vindos dos diversos pontos são conectados a blocos de distribuição fixos, os Patch Panel que ficam dentro dos racks de distribuição. A ligação dos blocos de distribuição aos hubs e/ou switches se dá através de patch cords. Utilizando-se desta facilidade pode-se ter uma melhor organização, flexibilidade e fácil manutenção.

***Patch Panel***

O Patch Panel é um painel intermediário de distribuição de cabos que fica entre os pontos de conexão de equipamentos e o concentrador (hub/switch).

## Midiateca

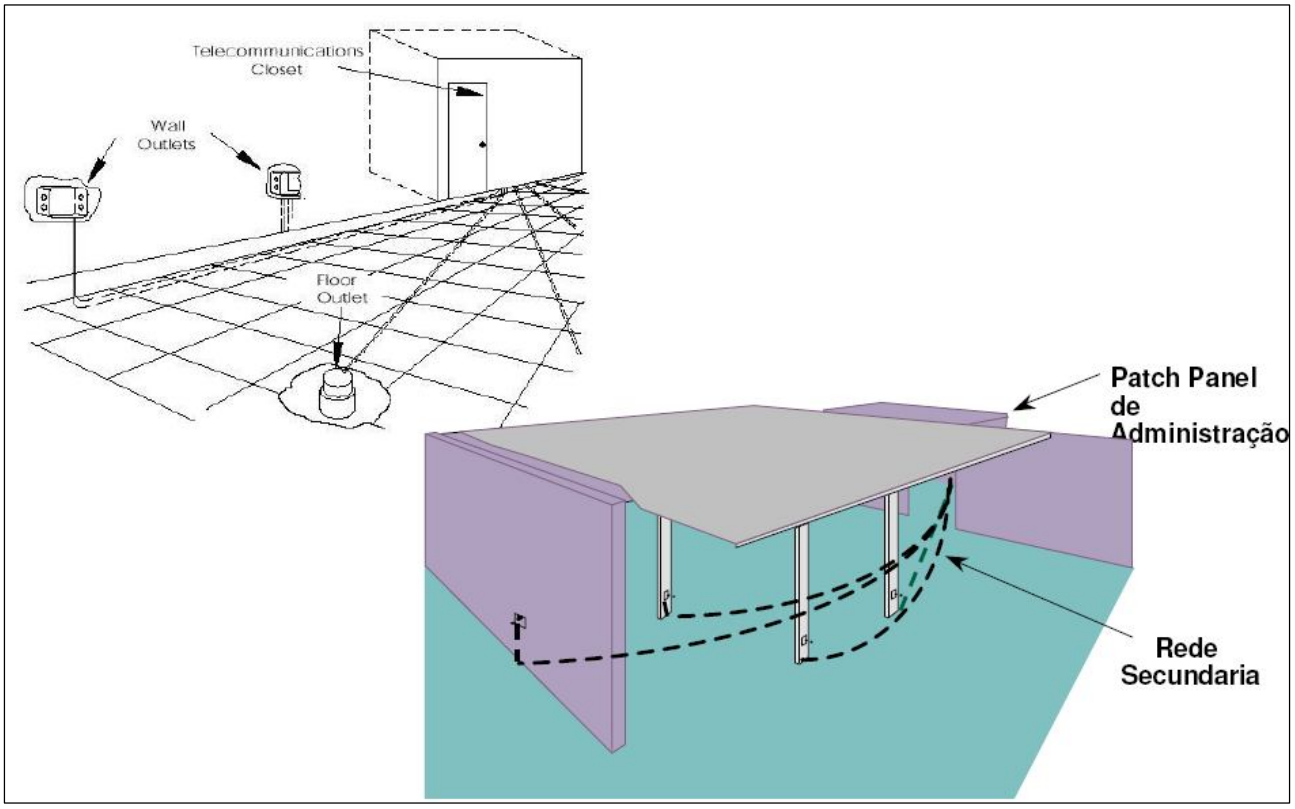
Assista ao vídeo que demonstra a construção de uma sala cofre

# UNIDADE 12

*Objetivo:Conhecer o Cabeamento estruturado – Subsistemas do Cabeamento Estruturado; Rede Secundária.*

## 5. Rede Secundária (ou horizontal)

É constituído pelos cabos que ligam o painel de distribuição (Patch Panel) até o ponto final do cabeamento. São denominados cabos secundários, formando um conjunto permanente; trafegam todos os serviços, voz, dados, imagem, monitoração e etc. Para alterar o serviço empregado a um determinado ponto de rede, basta mudar a configuração no painel de distribuição.



### *Definição*

A Rede Secundária compreende desde a tomada de informação, cabos e dutos até o armário de telecomunicações.

### *Componentes*

- Cabos
- Tomada de informação
- Terminações
- Conexões (cross-connects)
- Patch cords (cross-connects)

### *Meios de transmissão*

- Cabo de par trançado, 100 ohms, 4 pares
    - UTP (unshielded twisted pair)
    - ScTP (shielded twisted pair)

- Cabo de fibra ótica
    - 62.5 / 125 µm
    - 50 / 125 µm

***Comprimento***

Cabos e patch cords (UTP)

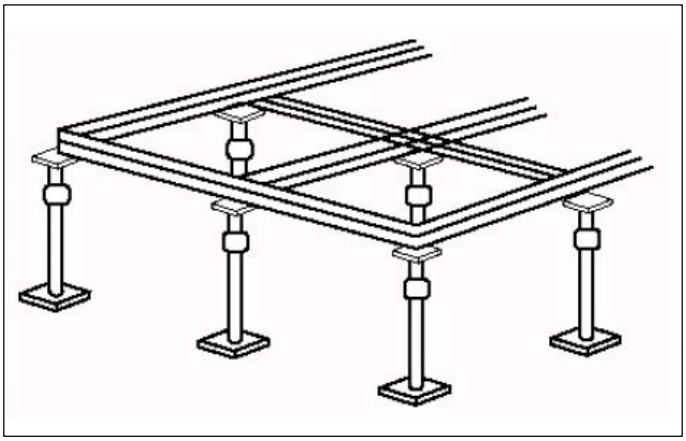
| *Cabo horizontal* | *Patch cord Área de Trabalho* | *Patch cord Tamanho total* |
|---|---|---|
| 90 | 5 | 10 |
| 85 | 9 | 14 |
| 80 | 13 | 18 |
| 75 | 17 | 22 |
| 70 | 22 | 27 |

***Atenção***

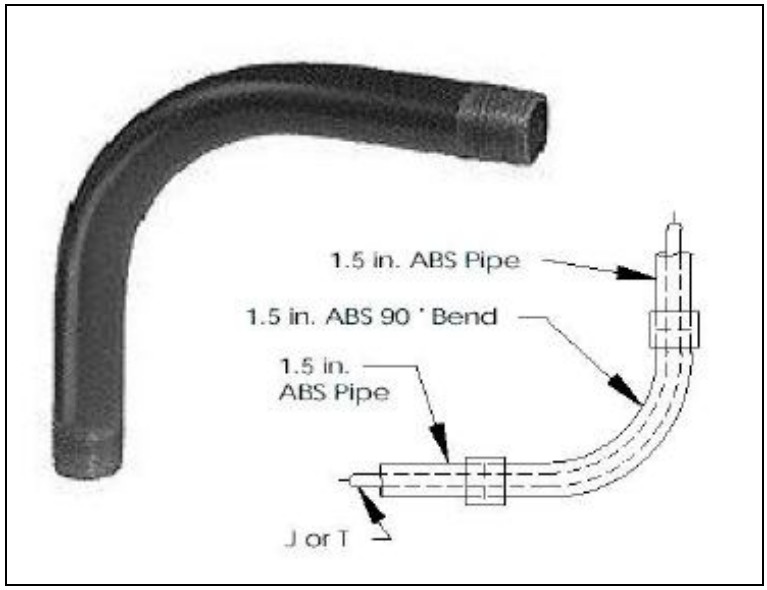
- Nenhum patch cord (UTP) da área de trabalho pode exceder o tamanho de 22 metros
- Qualquer combinação de Rede Secundária e patch cords não pode exceder 100 metros

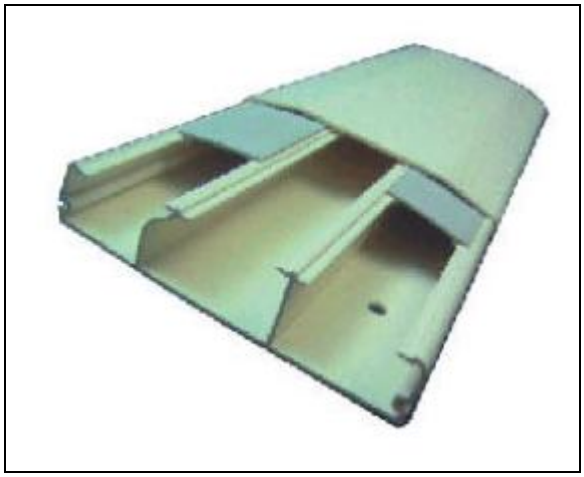
***Percursos Horizontais***

- Sob o piso (piso elevado) – passar os cabos sob o piso elevado é uma excelente opção.

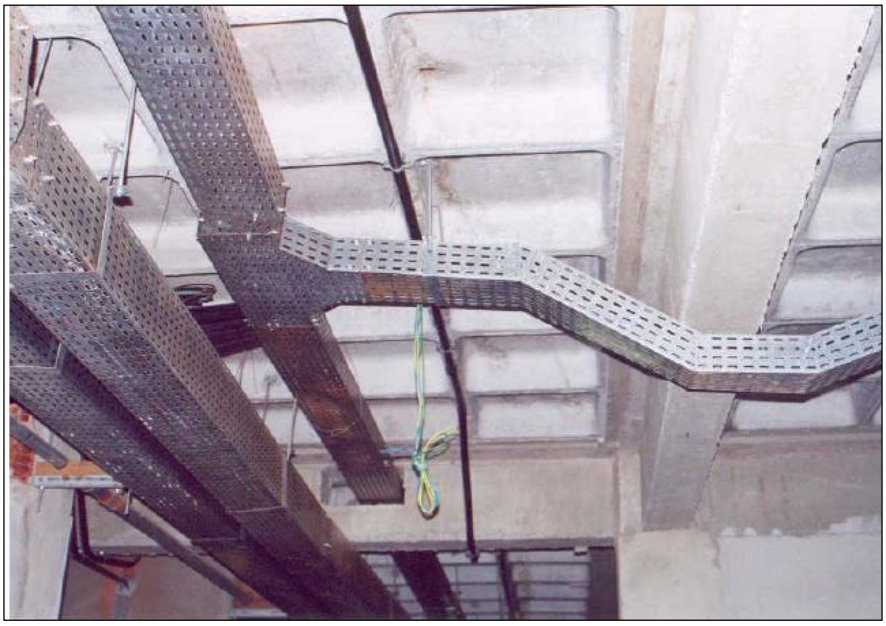


- Dutos e Canaletas – A taxa máxima de ocupação é de 40% da área do duto, canaleta ou eletrocalha.



- Teto – Exemplo de como passar cabos pelo teto.



  - O cabo NÃO poderá ser colocado diretamente em cima do forro
  - O cabo NÃO poderá ser sustentado ou estar preso a fios ou tirantes do teto

***Separação lógica x elétrica***

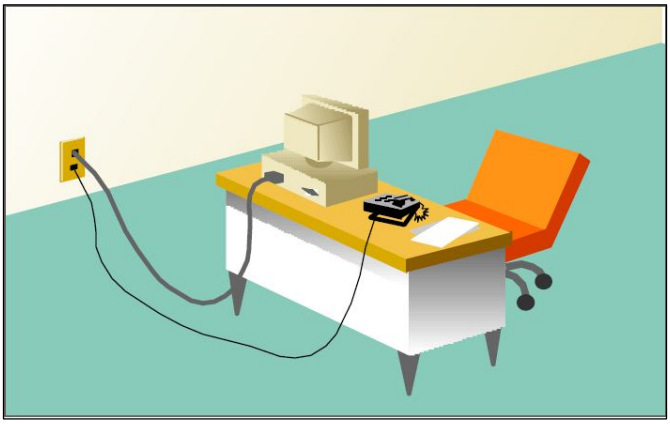
- Antigamente a norma EIA/TIA-569 recomendava uma separação mínima entre lógica e elétrica de 127 mm (para circuitos elétricos até 2KVA)
- A nova revisão da norma não estabelece nenhuma distância mínima, apenas a necessidade de uma separação física entre os cabos de lógica e elétrica.

# UNIDADE 13

*Objetivo:Conhecer o Cabeamento estruturado – Subsistemas do Cabeamento Estruturado; Área de Trabalho e Administração.*

## 6. Área de Trabalho (ATR)

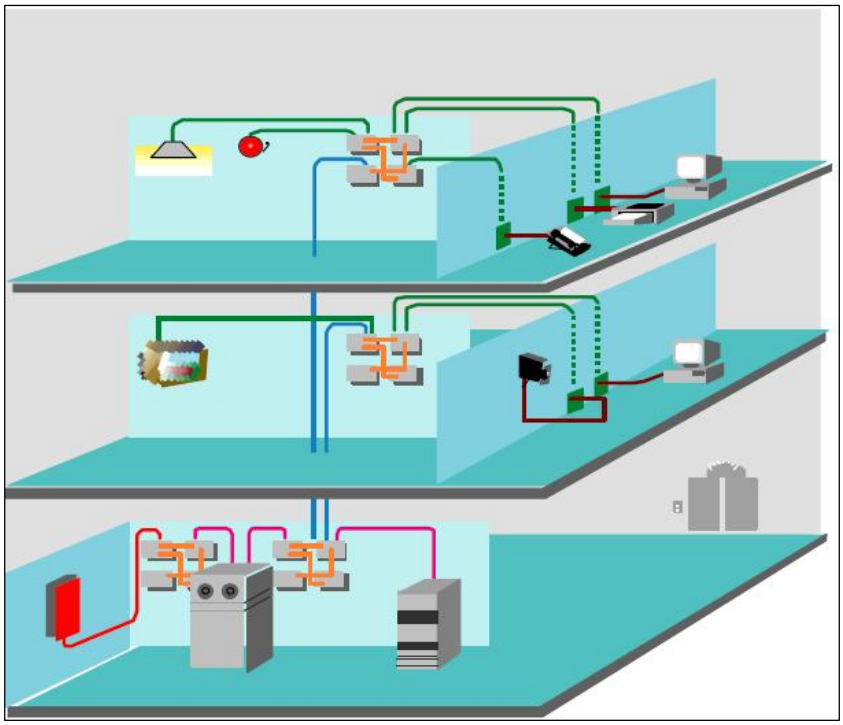
É o local onde estão os pontos finais do cabeamento estruturado, a tomada fixa para a conexão de cada equipamento.



É a área que abrange desde a saída da tomada de informação até a entrada do equipamento que irá utilizar o cabeamento. Uma área de trabalho tem no máximo 10 $m^2$ e possui no mínimo duas tomadas de informação.

***Componentes***

- Computadores, impressoras, telefones
- Patch cords, adaptadores (baluns)
- Câmeras, sensores



### 7. *Administração (Documentação)*

Após a instalação de uma rede estruturada todos os seus elementos devem estar identificados. A documentação deve estar atualizada:

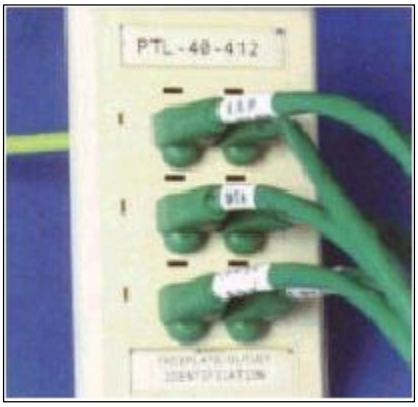
- Plantas
- Desenhos

***Identificação***

A Identificação dos componentes facilita a trabalhos de manutenção, facilita a recuperação de informação, minimiza erros e permite rastrear informações.

Outlets/Faceplates (tomadas RJ-45)

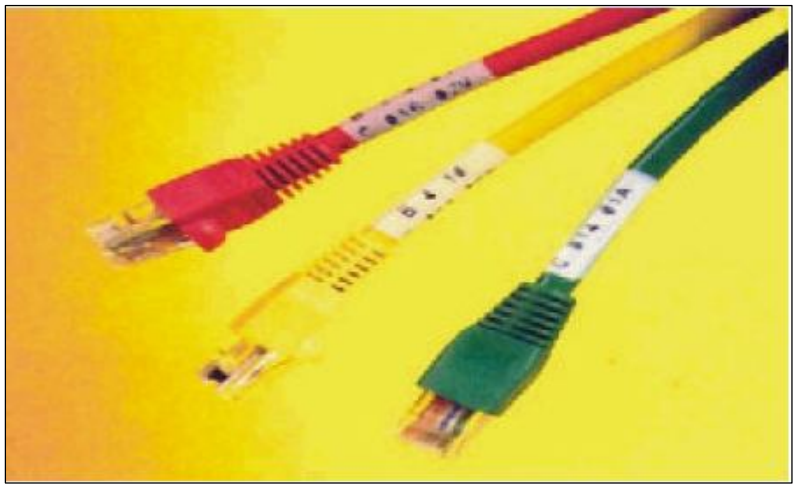
Um identificador deverá ser aplicado em cada ponto de terminação. Toda a terminação deverá ser identificada.




***Identificação de Cabos:***

Subsistemas de cabos como Redes Primárias e Secundárias deverão ser identificados em cada ponta (na ponta do rack a tomada RJ-45).

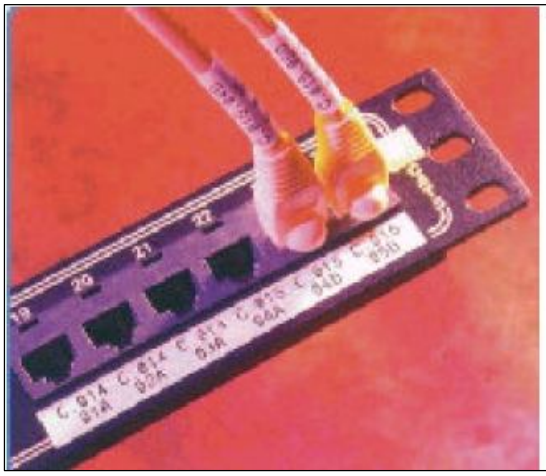
Etiquetas adicionais poderão ser requeridas em localidades intermediárias, como final de conduits e emendas, pois serão pontos de consolidação.

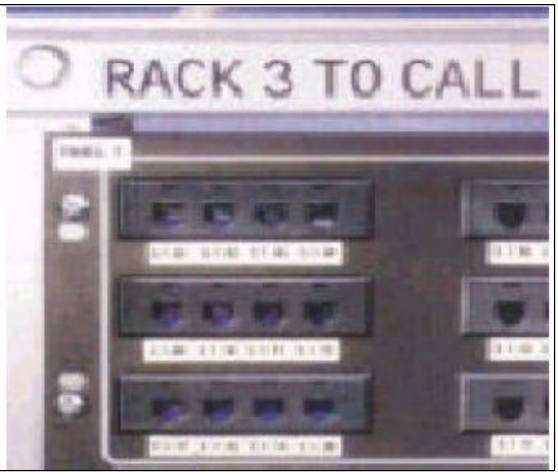


A tabela a seguir mostra o padrão de cores que deve ser adotado.

| Tipo de Terminação | Cor | Observações |
|---|---|---|
| Ponto de demarcação | Laranja | Pontos de Zone Wiring |
| Pontos de entrada | Verde | Conexões de rede e terminação de equipamentos auxiliares |
| Terminação de Equip. | Roxo | Mapeamento de portas de hubs, switches, roteadores e centrais telefônicas |
| Rede Primária Principal | Branco | Rede Primária |
| Rede Primária secundária | Cinza | Rede Primária |
| Estações | Azul | Terminação da Rede Secundária |
| Cabeamento Campus | Marron | Interligação entre prédos |
| Outros | Amarelo | Circuitos auxiliares, Alarmes e segurança. |
| Outros sistemas de Voz | Vermelho | |

Não apenas nos cabos, mas um identificador deverá ser aplicado em cada terminação do hardware.





***Antes e Depois***

Uma rede mal administrada pode causar muita dor de cabeça ao administrador.

## Midiateca

Assista ao vídeo que demonstra os subsistemas de um cabeamento estruturado

# UNIDADE 14

*Objetivo:Estudar o Cabeamento estruturado – Subsistemas do Cabeamento Estruturado; Administração - Plantas e Desenhos.*

**Plantas e Desenhos**

É importante que o administrador da rede mantenha em seu Projeto, plantas e desenhos atualizados de sua rede.

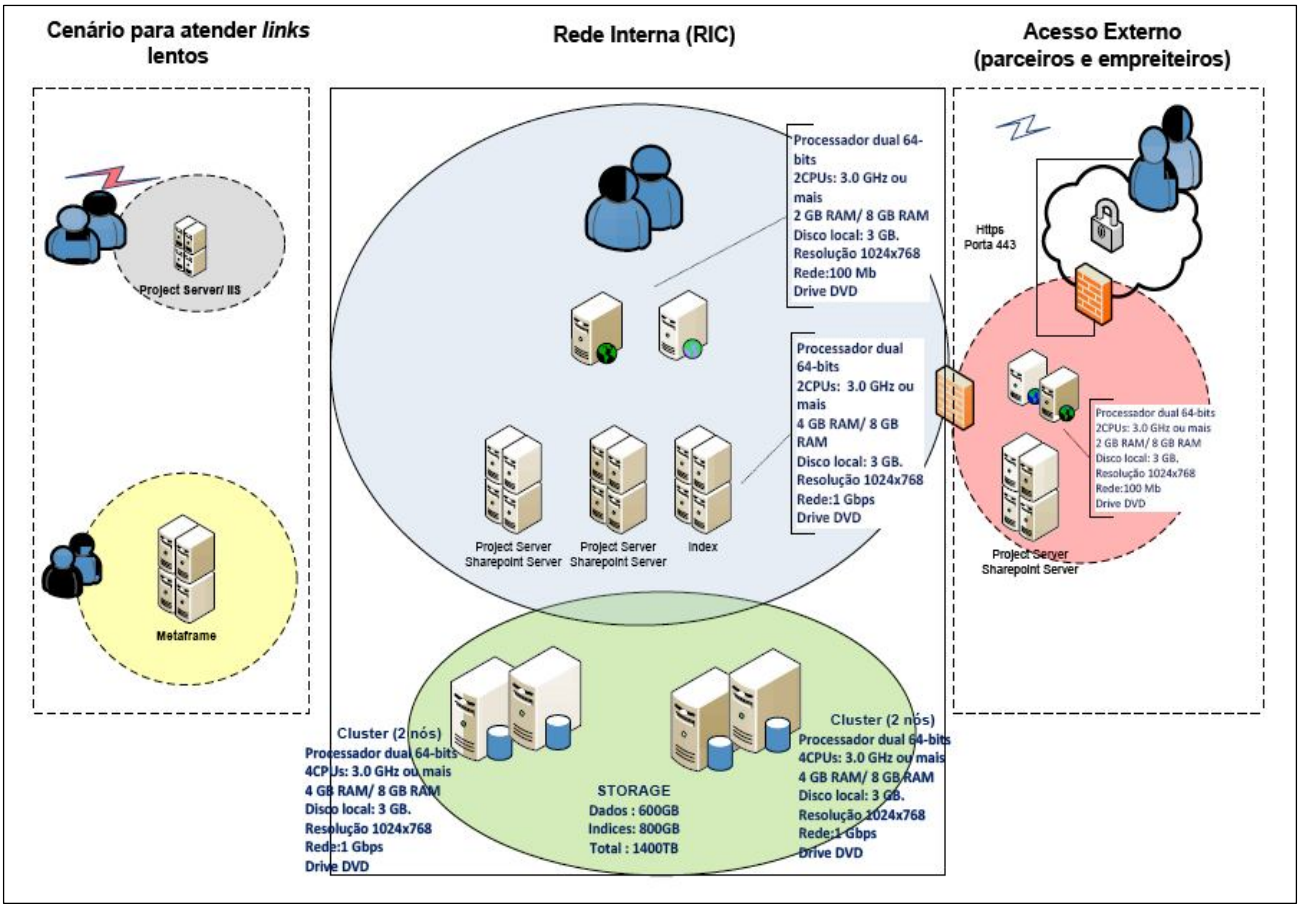
Os elementos básicos de uma documentação são:

***1. Arquitetura Lógica***

Uma visão macro dos principais servidores e sua função na rede. No projeto lógico se busca documentar a organização lógica da rede.

Costuma-se entender por organização lógica:

- A topologia lógica da rede;
- Uma descrição dos protocolos de nível 2 (comutação) e nível 3 (roteamento), incluindo qualquer recomendação sobre o uso desses protocolos;
- Um esquema de endereçamento e atribuição de nomes;
- Um esquema de roteamento;
- Os mecanismos e produtos recomendados para a segurança, incluindo um resumo de políticas de segurança e procedimentos associados;
- Recomendações sobre arquitetura e produtos para a gerência;
- Explicações sobre o porquê de várias decisões tomadas, relacionando as decisões aos objetivos do cliente.



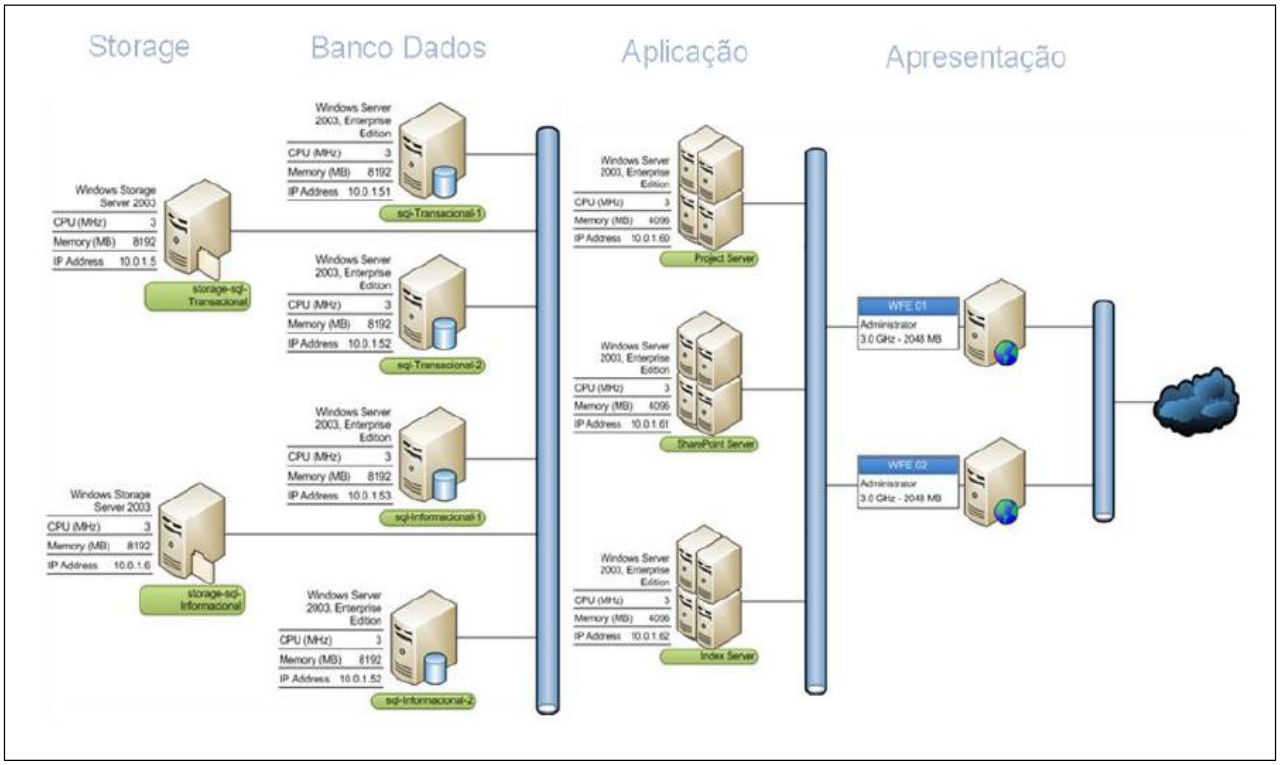

## 2. *Arquitetura Física*

Diferencia-se da Arquitetura Lógica por trazer mais informações sobre os servidores, assim como seus nomes, endereço IP e qualquer outra informação que seja relevante para seu Projeto. No projeto físico costuma-se documentar a organização física da rede.

Por organização física costuma-se entender:

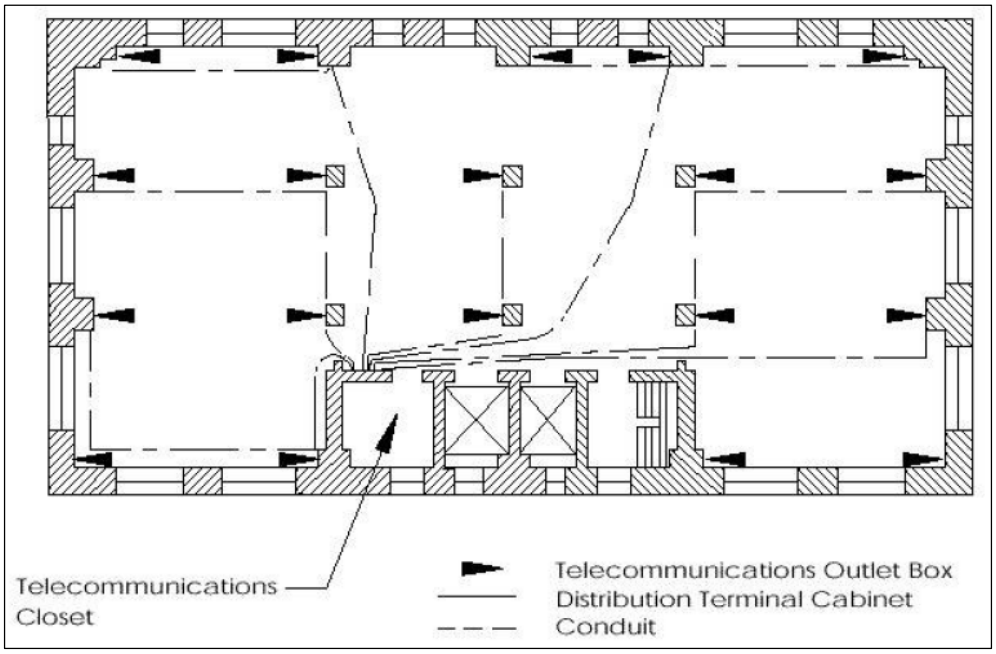
- A topologia física da rede, destacando pontos de interconexão, centros de fiação etc.;
- A especificação das tecnologias de cabeamento e de transmissão utilizadas, com justificativas para cada escolha;

- A especificação dos equipamentos utilizados – máquinas clientes, máquinas servidoras, máquinas de armazenamento de dados (data stores), máquinas de backup (backup), dispositivos de interconexão (concentradores, comutadores, roteadores etc.) – com justificativas para cada escolha;
- A escolha do provedor de acesso à Internet e a forma de conexão ao mesmo;
- Os custos de manutenção mensal (ou anual) de equipamentos e serviços.




### *3. Planta Baixa*

Normalmente criada por andar. Identifica os locais onde serão instalados os pontos (tomadas RJ-45), assim como todos os subsistemas do cabeamento estruturado.




### *4. Identificação Patrimonial (Especificação dos Equipamentos)*

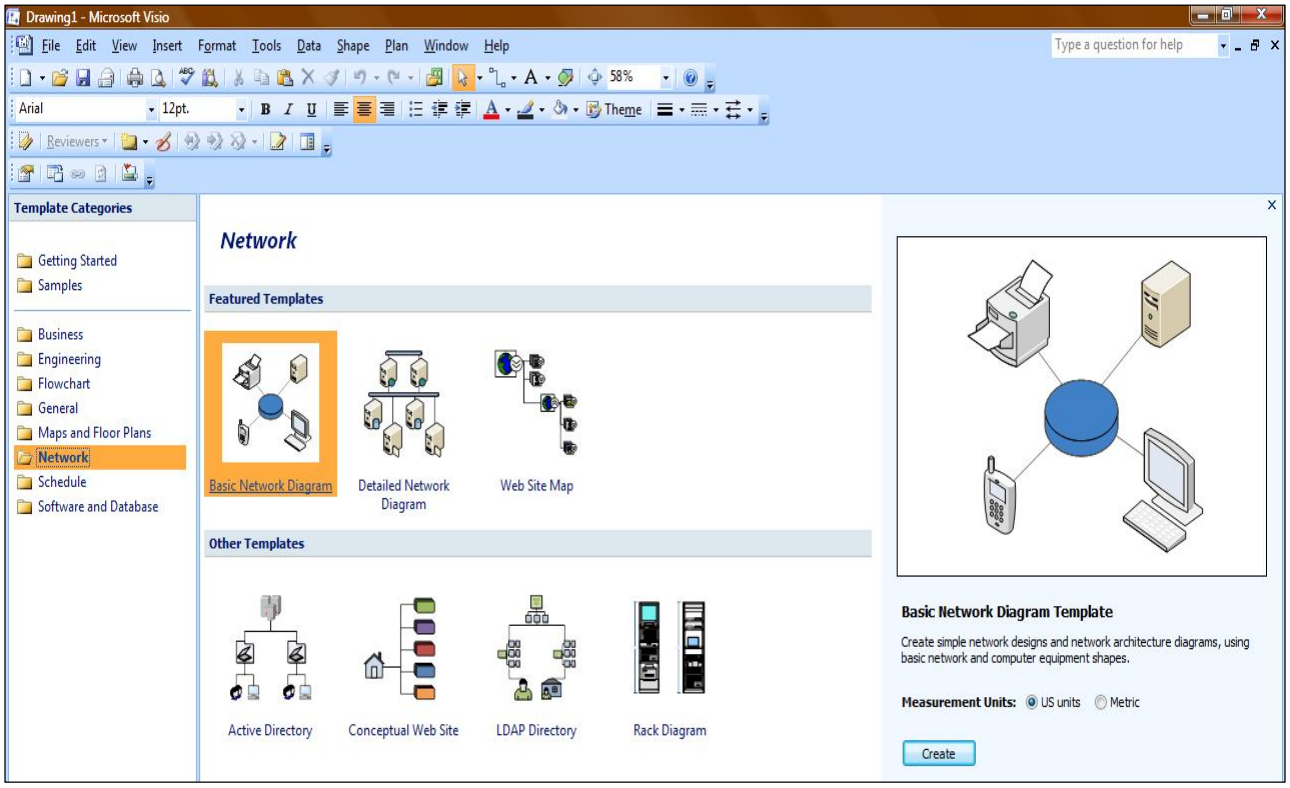
É importante criar uma Identificação Patrimonial dos dispositivos da sua Rede. Você pode fazer este controle em uma simples planilha Excel, ou através de vários sistemas disponíveis no mercado.

| Tipo | Nome | Configuração | Localização | Código de Barras |
|---|---|---|---|---|
| PC | PC-001 | Processador Pentium<br>1GB Memória RAM | 1º Andar<br>Baia 32 | 000.000.000-00 |
| ROTEADOR | CISCO XX | 2 PORTAS | 2º Andar<br>RACK “A” | 000.000.000-00 |
| ... | | | | |

## 5. *Ferramental para criação dos desenhos*

Todos os desenhos e plantas demonstradas neste módulo foram criados a partir do software Microsoft Visio.

Recomenda-se que esta ferramenta seja adquirida para auxiliá-lo na documentação da sua Rede.



Temos aqui então uma divisão entre topologia lógica e topologia física:

- A topologia lógica descreve como as informações devem transitar ao longo da rede, o formato dos dados, etc. É a forma como os protocolos (conjuntos de regras que organizam a comunicação) operam no meio físico;
- A topologia física refere-se à disposição dos cabos e componentes do meio físico, descrevendo onde cada nó da rede está situado fisicamente em relação aos demais, como é feita a distribuição da mídia de conexão (cabeamento de cobre, fibra óptica, wireless, etc) e mostra a configuração geral da rede através da planta de localização dos equipamentos.

# UNIDADE 15

*Objetivo: Analisar as considerações finais sobre Cabeamento Estruturado - Contornando problemas de ruído - Aterramento.*

## Ruídos

Os ruídos gerados pelas falhas nos sistemas de energia elétrica são os maiores causadores de defeitos em redes de computadores, podendo resultar em defeitos de hardware e mesmo perdas de dados e erros em programas.

O ruído trata-se de um sinal indesejável, constituído por sinais aleatórios e, por serem aleatórios, esses sinais interferem nos circuitos eletrônicos provocando algum sintoma de mau funcionamento.

Conhecido como Interferência Eletromagnética (EMI) e Interferência por Rádio Frequência (RFI), o ruído elétrico pode ser causado por diversos fatores.

### *Formas de ruído*

Existem dois formatos básicos de ruído que afetam as redes de comunicação: o ruído branco e o ruído impulsivo. O ruído branco, também conhecido como ruído térmico, é provocado pela agitação dos elétrons nos condutores metálicos. Seu nível é função da temperatura, sendo uniformemente distribuído em todas as frequências do espectro. Na prática, é mais danoso à comunicação de dados do que à de voz.

Já o ruído impulsivo é do tipo não contínuo, consistindo em pulsos irregulares de grandes amplitudes, sendo de difícil prevenção. A duração destes pulsos pode variar de alguns até centenas de milisegundos. É provocado por distúrbios elétricos externos ou por falhas em equipamentos (indução nos circuitos eletrônicos).

O ruído impulsivo é o causador da maior parte dos erros de transmissão em sistemas de comunicação. Sua medida se realiza pela contagem do número de vezes que, em um determinado período de tempo, os picos ultrapassem um nível pré-fixado. É altamente prejudicial para as transmissões de voz e dados.

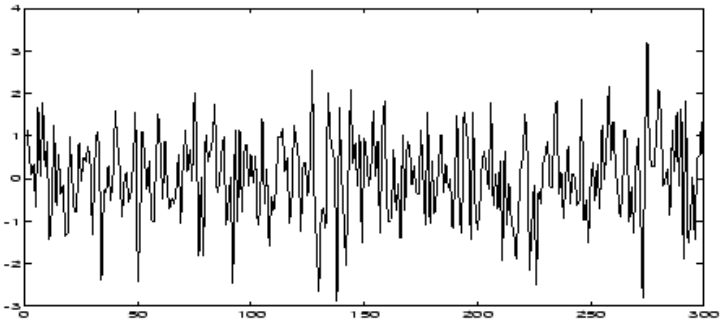
***O que causa o ruído?***

O ruído pode ser gerado por fenômenos naturais como descargas atmosféricas (raios), reações químicas ou por equipamentos elétricos ou eletrônicos. Por exemplo, nos computadores, as fontes de alimentação são chaveadas, ou seja, existe um elemento que liga e desliga uma corrente elétrica em alta velocidade. Essas fontes chaveadas geram ruído e também são sujeitas a ruídos externos.

Os ruídos se classificam em ruídos de modo comum e ruídos de modo diferencial.

***Ruídos de modo comum*** - São aqueles que se propagam pelas linhas de fase e neutro simultaneamente, fechando o circuito pelo plano de terra. É este o principal tipo de ruído, responsável por cerca de 80% dos problemas em equipamentos de redes de computadores.

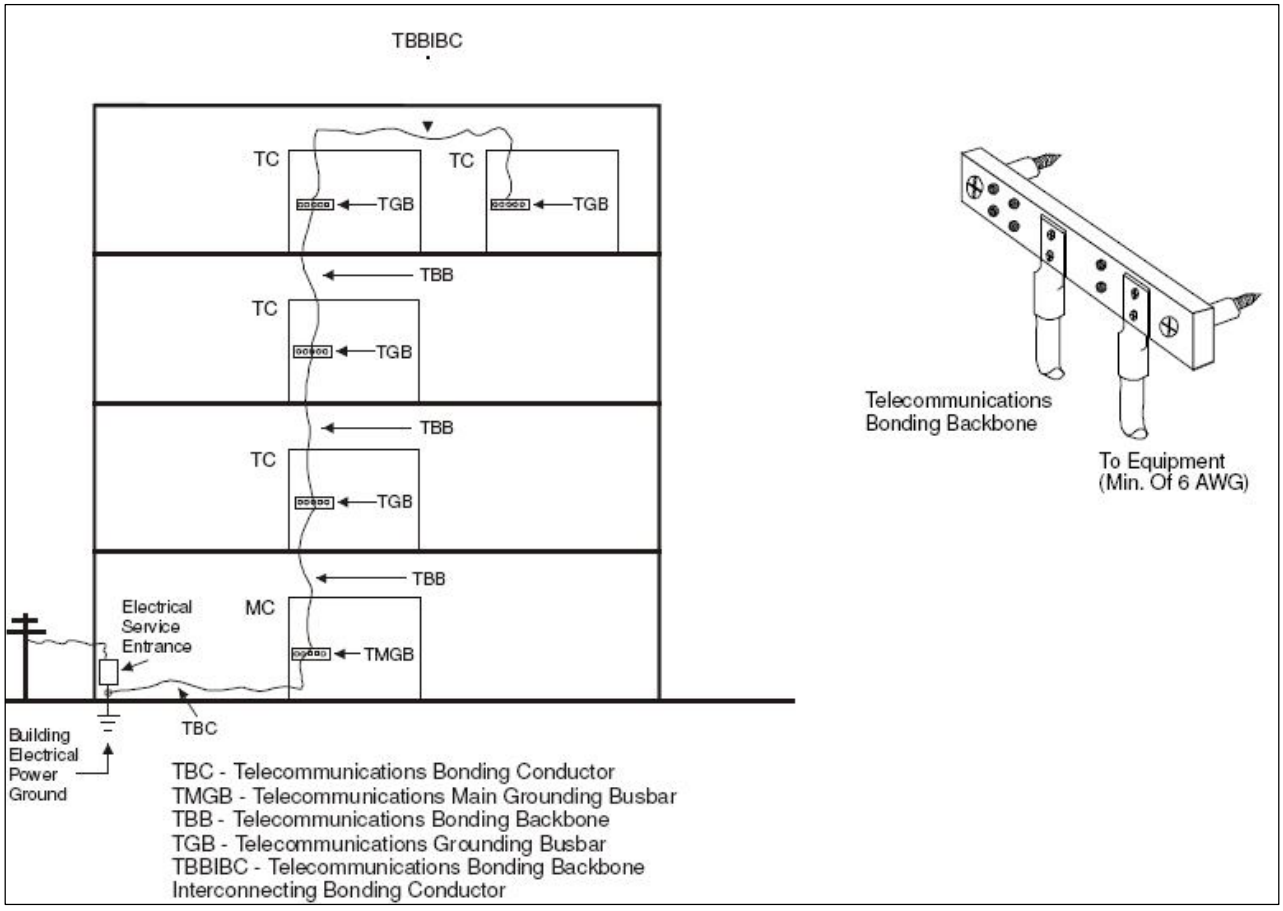
***Ruídos de modo diferencial*** - Este tipo de ruído se propaga apenas pela linha de fase, fechando o circuito pelo neutro ou pelo plano de terra. Em computação, é o que menos afeta os equipamentos.




*Exemplo de ruído branco*

### *Soluções para ruídos*

Algumas providências básicas podem ser tomadas para evitar que o ruído afete o funcionamento dos equipamentos eletrônicos ou mesmo uma rede de computadores inteira. Os métodos de redução de ruídos elétricos mais utilizados nos sistemas de cabeamento das redes de computadores envolvem o balanceamento dos níveis de tensão nas extremidades dos cabos, a blindagem das estruturas por onde passa o cabeamento e, principalmente, o cuidado com o aterramento.



Cuidados mais genéricos envolvem providências como, por exemplo, não ligar aparelhos sensíveis na mesma linha de alimentação onde estão ligados aparelhos de maior potência, tais como: ar-condicionado, geladeiras, fornos elétricos, lâmpadas incandescentes com controladores eletrônicos, máquinas de lavar e outros. Nesse caso, o ideal é separar uma linha de alimentação específica, com seu próprio disjuntor para ligar os equipamentos mais sensíveis.

Uma solução importante é a utilização de filtros de linha e filtros supressores de ruído. Um filtro de linha tem como função proteger o hardware do computador e equipamentos eletrônicos em geral, contra surtos e picos de energia, sendo que alguns modelos também estão preparados para a filtragem de ruídos elétricos. A posição ideal dos filtros supressores no circuito (não os de linha) é o mais próximo possível dos pontos onde o ruído é gerado. Isto significa que cada circuito capaz de gerar ruído deve ter seu próprio filtro.

Os melhores filtros comerciais vêm embutidos em caixas metálicas que servem de blindagem para evitar que o ruído se propague para fora por radiação. Sempre se deve ter o cuidado de verificar as características e a procedência dos produtos antes de instalar em uma rede.

## Atividades

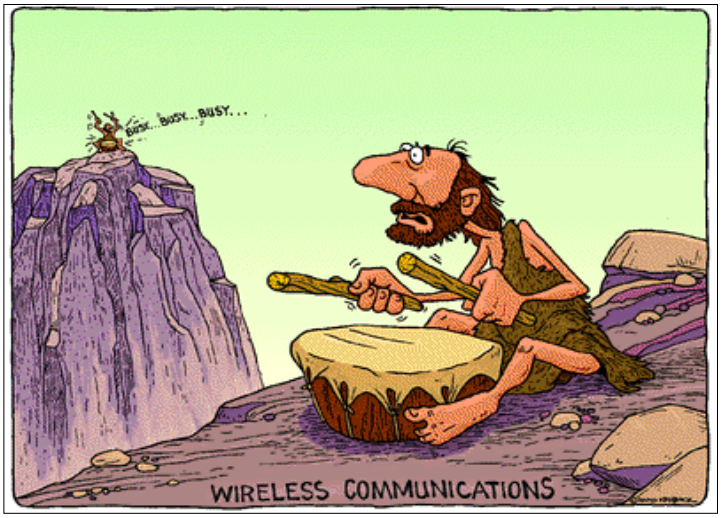
ATENÇÃO! Para garantir a qualidade da aprendizagem, não dê continuidade aos estudos sem antes realizar as atividades encontradas na lista 2 (ATIVIDADE 2).

# UNIDADE 16

*Objetivo:Aprender sobre  Redes sem Fio - compreender o conceito de redes sem fio.*

**Conceito**

Uma rede sem fio, também conhecida como tecnologia Wireless LAN – WLAN (sem fios) é um tipo de rede que permite a conexão entre diferentes pontos, utilizando ondas de rádio, sem a necessidade do uso de cabos.




Na grande maioria das vezes a etapa mais complicada na instalação de uma rede de computadores é a passagem de cabos pelos locais onde ficam os pontos da rede. Essa tarefa pode exigir desde obras civis e instalação de pisos elevados até mesmo deixar dutos ou canaletas à mostra, prejudicando o visual do ambiente.

Os produtos wireless estão ganhando mais espaço no mercado de redes locais graças à redução dos seus preços e às facilidades oferecidas, como rapidez na instalação e mobilidade propiciada aos usuários. Isso sem contar a vantagem adicional oferecida quanto à preservação do investimento, uma vez que, no caso de mudança de endereço, não é

necessário um novo investimento em cabeamento, como aconteceria em uma rede com cabeamento estruturado.

Um dos principais padrões sem fio no momento é o Wi-Fi (Wireless Fidelity), que corresponde à especificação 802.11b do IEEE e que inclui o protocolo de segurança WEP (Wired Equivalency Protocol).

Os locais onde os equipamentos Wi-Fi estão comumente disponíveis para prover acessos à internet são conhecidos como "hotspots". Atualmente, os principais fabricantes de equipamentos móveis incorporam em seus modelos mais novos a tecnologia Wi-Fi.

Uma rede sem fio pode conectar dois ou mais equipamentos entre si através de uma arquitetura ponto-a-ponto (peer-to-peer), compartilhando uma conexão de internet, impressoras de rede, transferência de arquivos, etc.

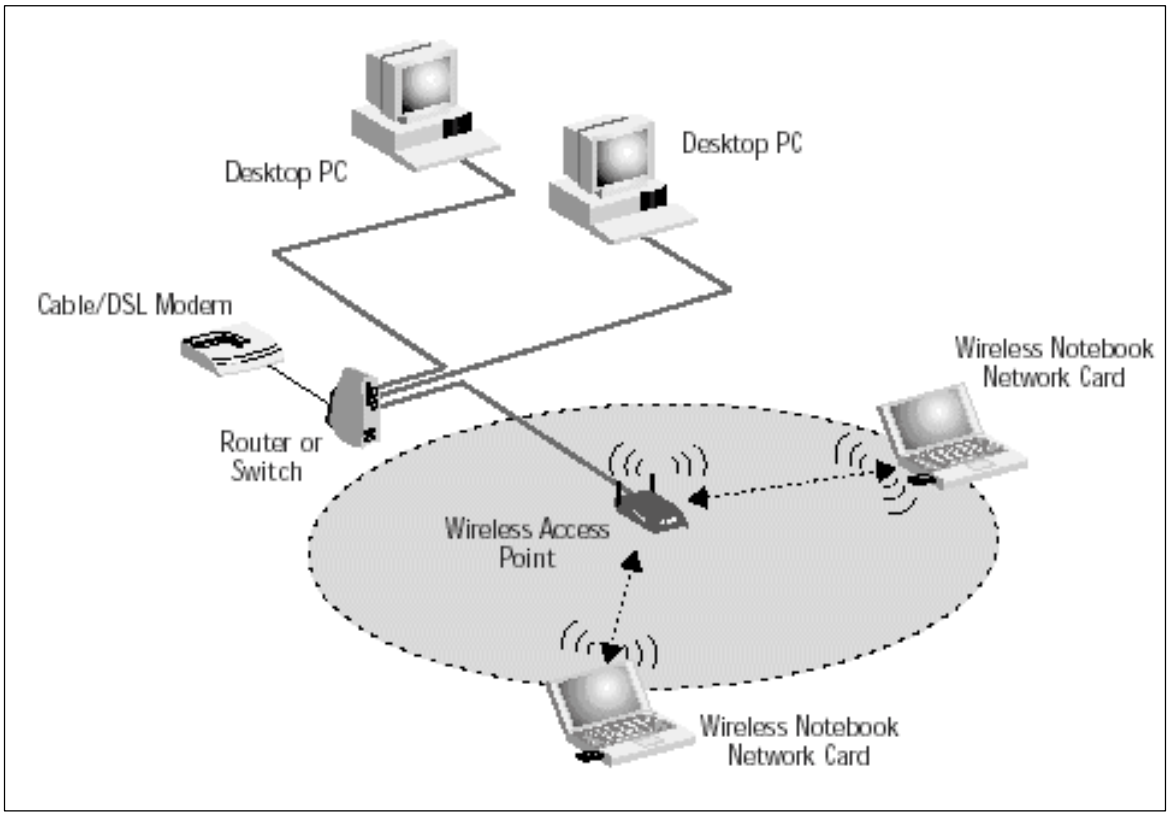

***Benefícios das redes sem fio***

- Mobilidade dos equipamentos de rede
- Instalação rápida, simples e flexível

- Redução de custo (as despesas de instalação podem ser significativamente menores comparadas a redes cabeadas)
- Instalação em áreas de difícil acesso
- Escalabilidade e confiabilidade

***Como funcionam as WLANs***

Num ambiente típico, como o mostrado na figura a seguir, um ponto de acesso (access point) é conectado a uma rede local Ethernet convencional (com fio). Os pontos de acesso não apenas fornecem a comunicação com a rede convencional, como também intermediam o tráfego com os pontos de acesso vizinhos, num esquema de micro células com roaming, semelhante a um sistema de telefonia celular.



# UNIDADE 17

*Objetivo:Conhecer mais sobre  Redes sem Fio - tipos de redes sem fio, características do padrão IEEE e suas especificações.*

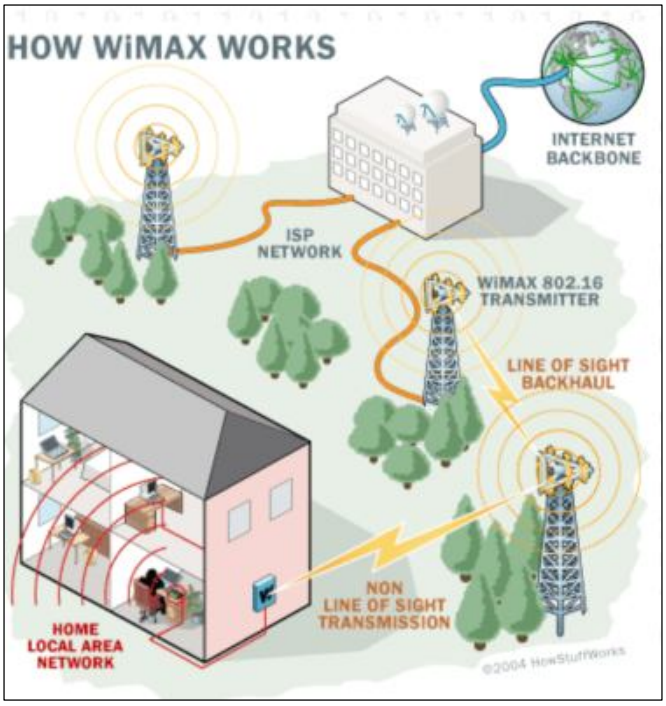
**Há quatro tipos principais de redes sem fio:**

***Rede pessoal sem fio (WPAN)*** - Tecnologia Bluetooth - As redes pessoais sem fio são redes de pequeno alcance que utilizam tecnologia BluetoothTM , comumente usada para interconectar dispositivos compatíveis próximos. Uma WPAN possui alcance típico de 9 metros (30 pés). Assim como a WLAN, o alcance da WPAN pode variar.

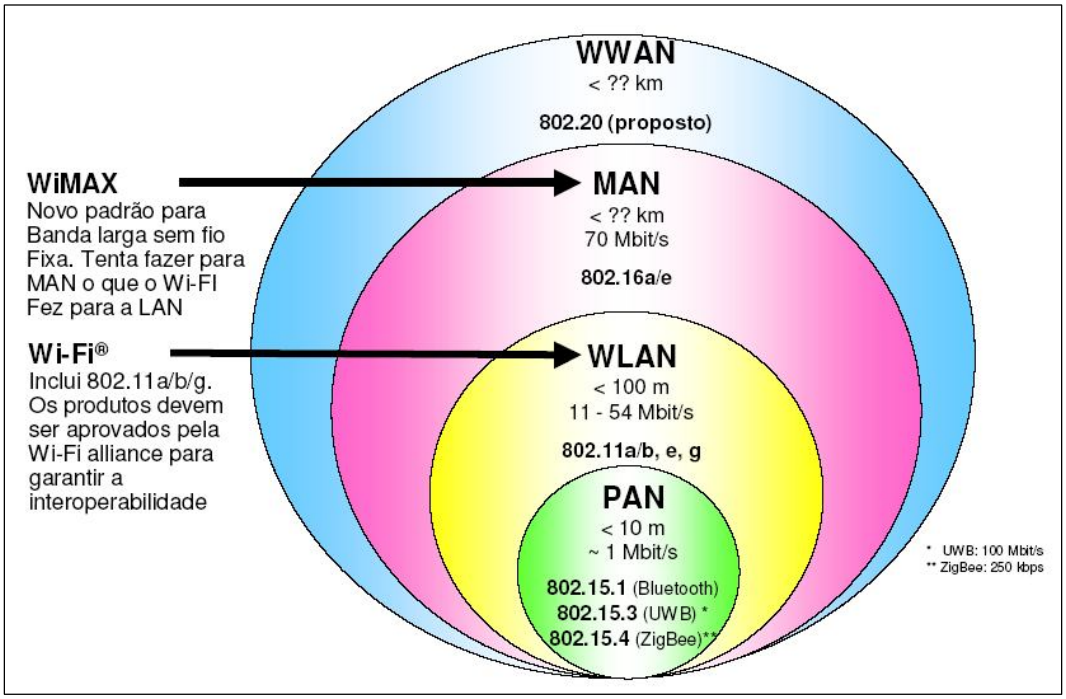
***Rede local sem fio (WLAN)*** - Uma WLAN pode ser criada em sua casa para uso pessoal. Esse tipo de rede sem fio é usado frequentemente para acessar a Internet. O alcance de uma WLAN pode ser de até cerca de 90 metros (300 pés). Esse alcance pode variar em função do número de usuários, interferência, barreiras de transmissão (como paredes e material de construção), entre outros fatores.

***Rede Metropolitana sem fio (WMAN)*** – Tecnologia WiMax  (padrão 802.16) - é um dos últimos padrões de banda larga para rede MAN  (Metropolitan Area Network/Rede de Área Metropolitana) definido pelo IEEE, em certo aspecto muito similar ao padrão Wi-FI (IEEE 802.11) já muito difundido.

O padrão WiMAX tem como objetivo estabelecer a parte final da infraestrutura de conexão de banda-larga (last mile) oferecendo conectividade para mais diversos fins: por exemplo uso doméstico, hotspot e empresarial. Oferece conexão de até 75 Mbps em um raio de 50 km.




Rede de banda larga móvel ou Rede remota sem fio (WWAN) - A Rede remota sem fio ou de banda larga móvel utiliza sinais de telefone móvel. As redes de banda larga móvel normalmente são fornecidas e mantidas por provedores de serviços de telefones móveis (celulares) específicos.



As duas tecnologias utilizadas nas redes sem fio são:

1. ***Luz***

    - Laser
    - Infravermelho

2. ***Radiofrequência***

    - Bluetooth (IEEE 802.15.1)
    - WLAN – Wireless Lan (IEEE 802.11)
    - Wi-Fi (IEEE 802.11b)
    - WiMAX (IEEE 802.16)


***Padrão IEEE 802.11 (WLAN)***

As redes locais sem fio (WLANs) usam um padrão de indústria conhecido como 802.11. Dentro da faixa de alcance dos dispositivos 802.11, muitos são certificados pela Wi-Fi Alliance para interoperabilidade de produtos da rede local sem fio.

***Especificações do 802.11***

O **802.11(b)** é a variedade mais comumente empregada em locais residenciais, comerciais e públicos.

- Transmissão (máxima) de 11 megabits por segundo (Mbps)
- Radiofrequência na banda de 2,4 GHz

O **802.11(g)** pode oferecer transmissão de dados um pouco mais rápida que o 802.11(b)

- Compatibilidade com o 802.11(b)
- Até 54 Mbps com outros dispositivos 802.11(g) em condições ideais
- Radiofrequência na banda de 2,4 GHz

O **802.11(a)** pode oferecer até 54 Mbps com outros dispositivos 802.11(a) em condições ideais.

- Radiofrequência na banda de 5GHz
- Determinados dispositivos 802.11(a) são dispositivos "de banda dupla". Alguns dispositivos de banda dupla são compatíveis com dispositivos 802.11(b) e 802.11(g).
- Dispositivos de banda simples 802.11(a) não são compatíveis com dispositivos 802.11(b) ou 802.11(g).

# UNIDADE 18

*Objetivo:Conhecer as Redes sem Fio - Compreender quais são os elementos de hardware de uma rede sem fio WLAN.*

**Elementos de Hardware de rede Wireless**

Os elementos essenciais para montar uma rede sem fio:

1. Placa de rede sem fio

2. Access Point (AP's)

**Dica**

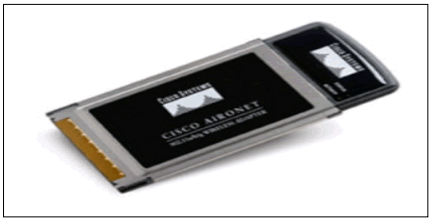
Todos os equipamentos devem ser homologados pela Anatel

A relação de equipamentos homologados você encontra no site www.anatel.gov.br

## 1. *Placa de Rede*

Faz a interface entre a estação de trabalho e a rede. Podem ser do tipo:

- Cartão PCMCIA (para computadores portáteis)




- Adaptador USB

- Adaptador PCI


## 2. *Access Point*

É um dispositivo que atua como ponte entre uma rede sem fio e uma rede tradicional. O Access point é um aparelho que transforma o tráfego da rede convencional (via cabos) em

sinal de rádio Wi-Fi. Por meio de Access Points, usuários de PDAs ou notebooks equipados com Wi-Fi podem acessar a rede local da empresa ou navegar pela Internet.

Todo sinal Wi-Fi é proveniente de um Access Point (Ponto de acesso). Os pontos de acesso podem operar no padrão 802.11a, 11b ou 11g. Em alguns casos, o aparelho é compatível com mais de um padrão.

O Access Point implementa o gerenciamento da rede sem fio: monitora erros, tráfego, nível de sinal e acessos não autorizados.

Configuração Access Points

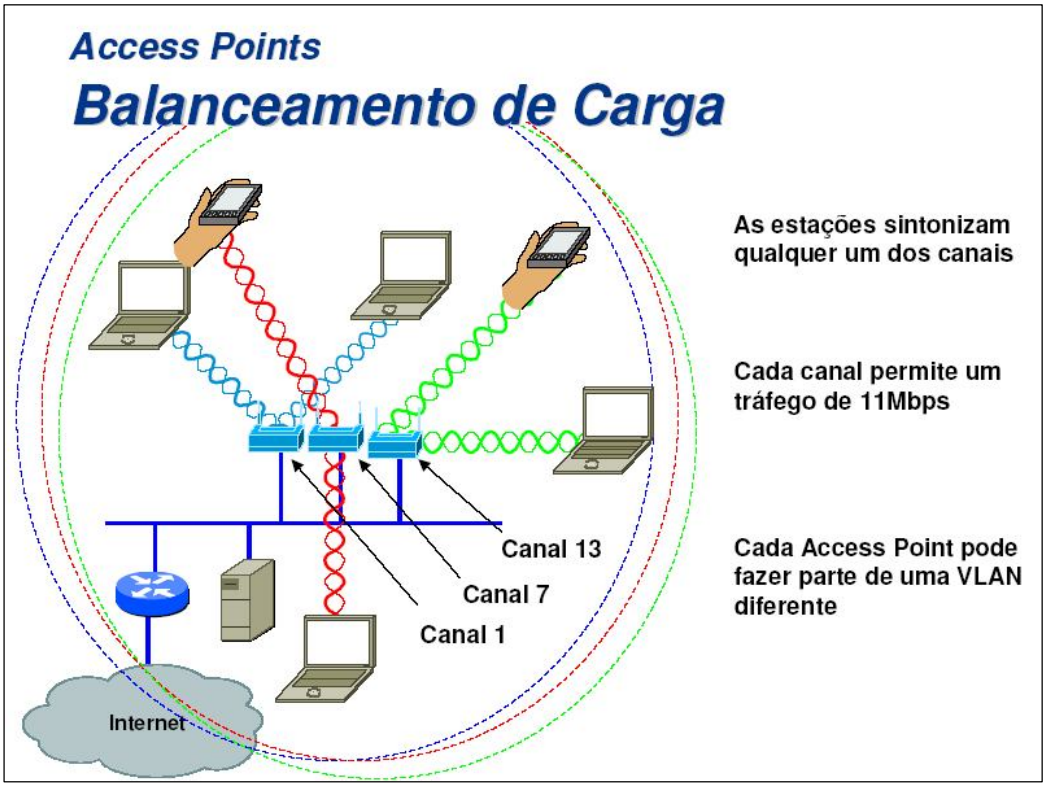
- A interface de configuração de um Access Point pode ser via HTTP (web), Telnet, SNMP ou Interface serial;
- Pode implementar parâmetros de segurança como:
    - SSID: Service Set Identifier
    - WEP: Wired Equivalent Privacy
    - EAP: Extensible Authentication Protocol

- O Access Point também pode fornecer serviços de rede, como:
    - DHCP: Dynamic Host Configuration Protocol
    - NAT: Network Address Translation
    - Firewall
    - Autenticação e autorização

***Para melhorias de velocidade:***

Algumas ações podem ser tomadas para otimizar o uso da rede sem fio, por exemplo:

- Faça redução na área de cobertura de cada Access Point
- Reduza a relação Cliente x Access Points
- Utilize de Balanceamento de carga



## Estudo Complementar

Veja em Estudo Complementar um passo a passo de como configurar uma rede sem fio

## Fórum

**FÓRUM iII**

O que você acha da qualidade da conexão utilizando access point? Essa tecnologia já está madura o suficiente para substituir a rede cabeada?

# UNIDADE 19

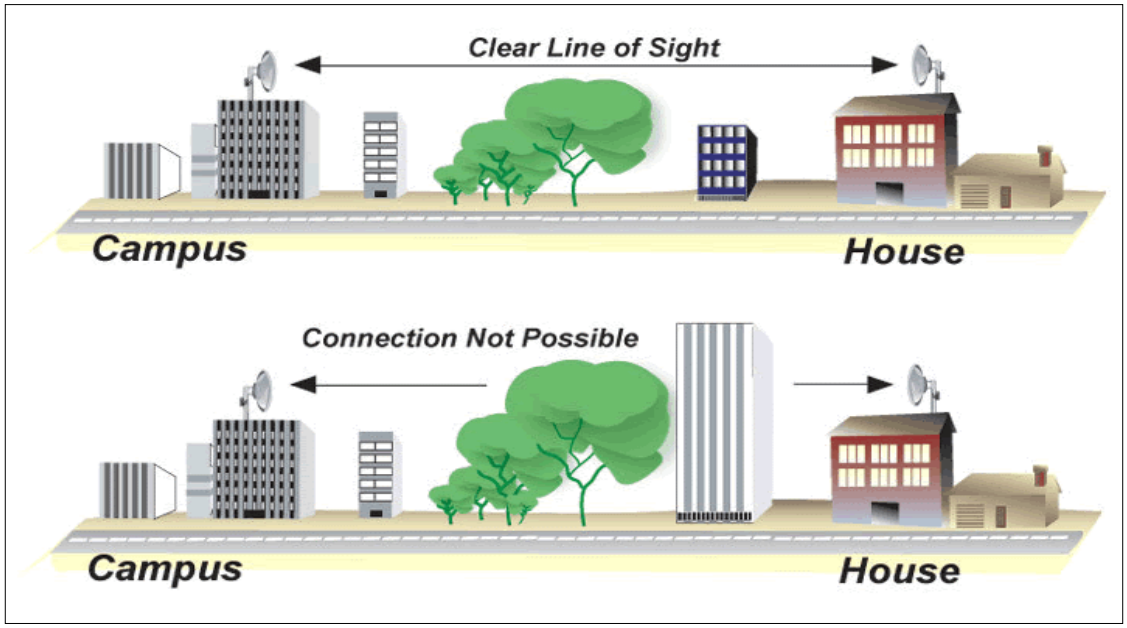
*Objetivo: Compreender as Redes sem Fio - Compreender o conceito de Visada e antenas adequadas para cada situação.*

**Visada**

Nos casos em que há a necessidade de se interligar dois pontos (por exemplo, dois prédios da mesma empresa) que estejam acima do alcance do Access Point, utilizam-se antenas para amplificar o sinal e garantir a conexão.

Visada nada mais é que a capacidade de enxergar cada antena, conforme ilustrado na figura a seguir.

A visada requer uma elipse livre de obstáculos entre as antenas. Não basta “ver” a outra antena, é preciso ter uma visão “ampla”, pois, por exemplo, a vegetação pode crescer e bloquear a visão em alguma época do ano.



***Antenas***

Parte fundamental para o bom funcionamento do sistema sem fio. Podem ser classificadas como:

1. ***Interna / Externa*** – quanto à localização

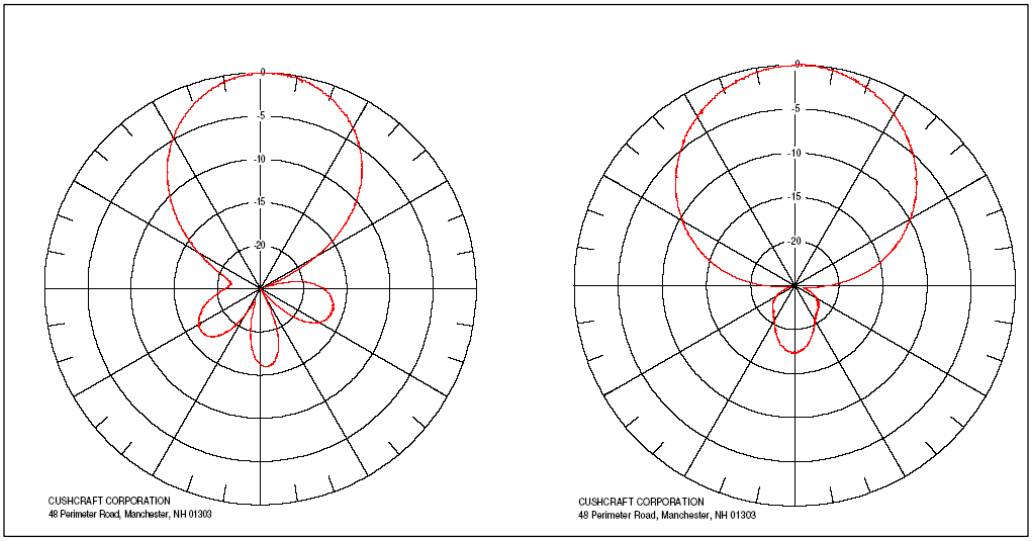
Antena Externa

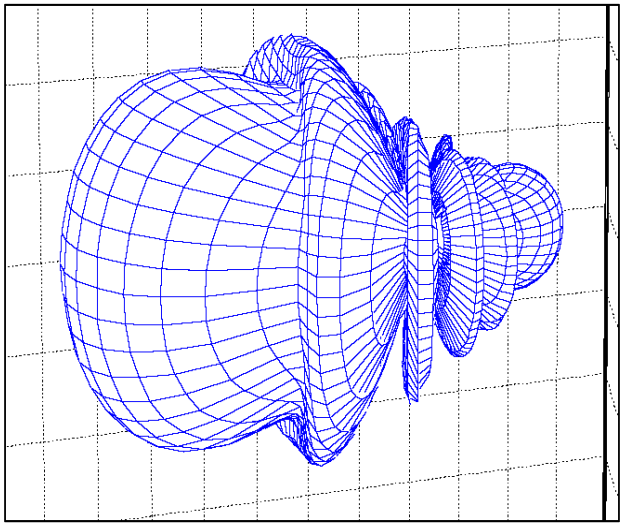
Antena Interna

2. ***Direcional / Omnidirecional*** – quanto ao padrão de irradiação.

***Direcional***

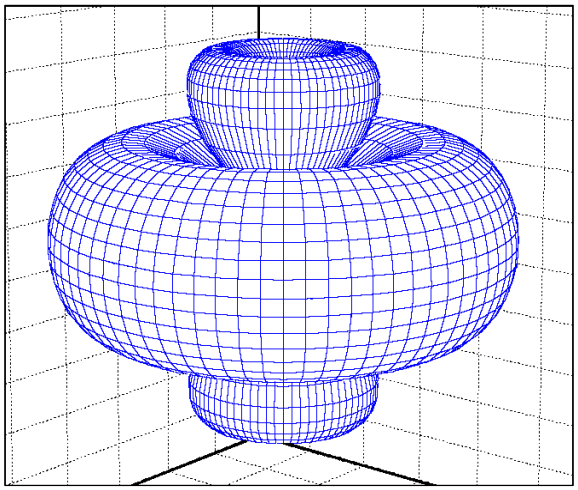
Caracteriza-se por concentrar o sinal em uma única direção. As mais utilizadas e conhecidas são as parabólicas.



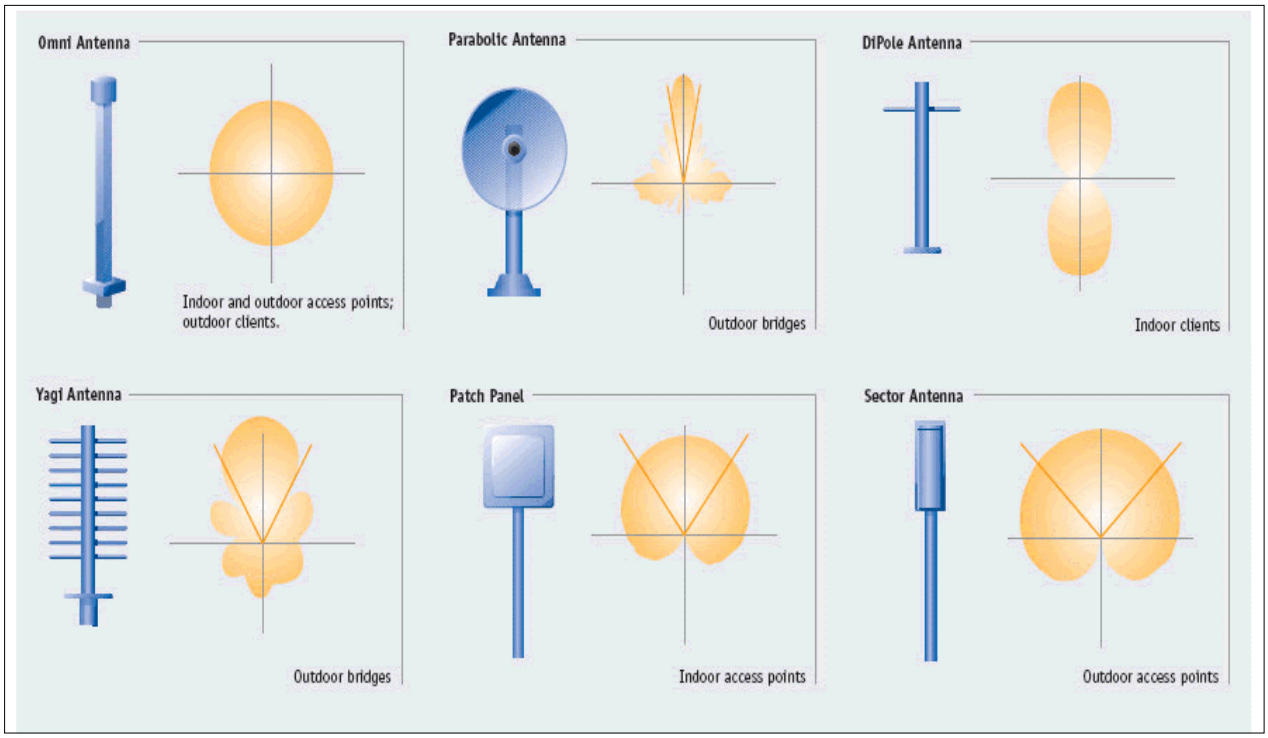



***Omnidirecional***

Transmitem 360 graus em torno do seu eixo e também são conhecidas como Dipolo. A antena de um Access Point é um exemplo prático de uma antena Omnidirecional.



Resumo dos Padrões de Irradiação e Tipos de Antenas



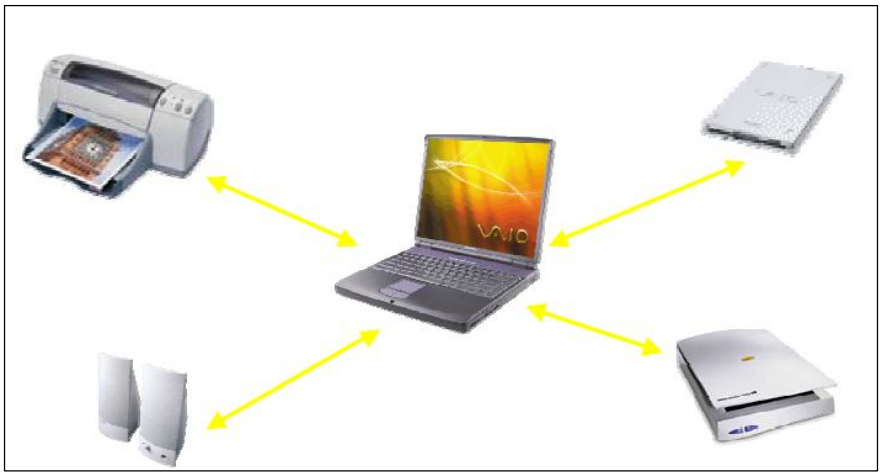
# UNIDADE 20

*Objetivo: Explorar as tecnologias Bluetooth e WiMax.*

**Bluetooth IEEE 802.15.1**

O objetivo inicial da tecnologia Bluetooth era substituir os cabos e conexões, via Infravermelho na conexão de periféricos com o PC.

O Bluetooth é a principal tecnologia das PANs (Personal Area Nerworks).



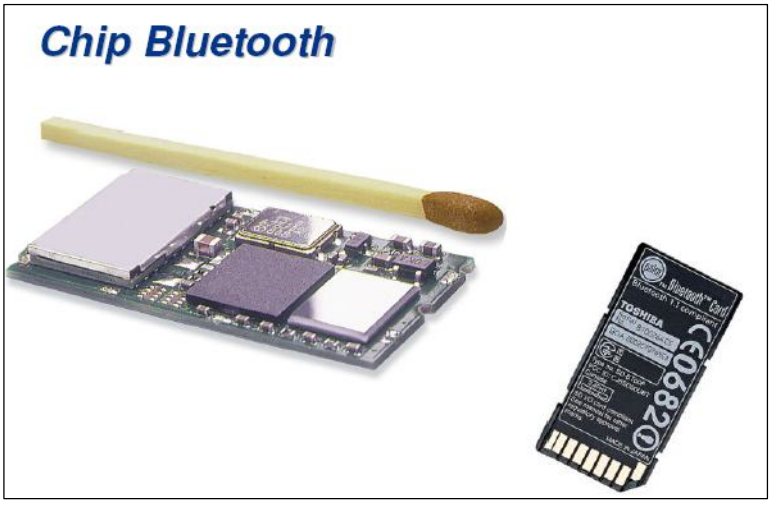
Algumas características:

- Padrões
    a. Tecnologia inicialmente desenvolvida pela Ericsson

b. v 1.0 publicado em 1999

c. v 1.1 publicado em 2001

- Acesso compartilhado ao meio
- Velocidade de 1 Mbps (nominal)
- 720Kbps (real)

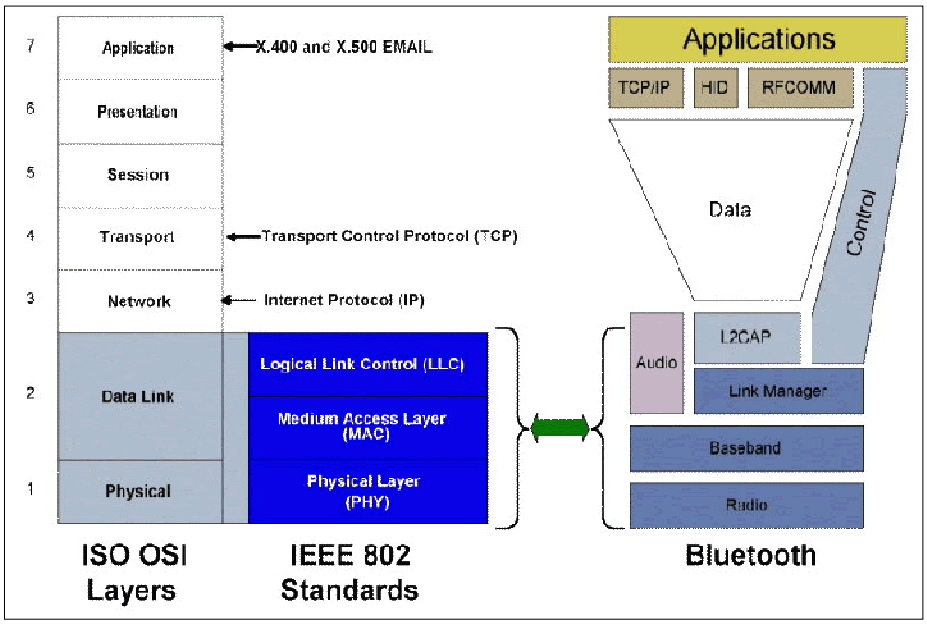



***Vantagens***

- Solução viável, de baixo custo, para redes de curto alcance
- Popularização de dispositivos com chips Bluetooth
- Suporta tráfego de voz, dados, gráficos e vídeo
- Facilmente integrada aos protocolos de comunicação

***Desvantagens***

- Limite do número de dispositivos conectados
- Alcance bastante restrito




*Bluetooth X Modelo OSI*

***WiMax IEEE 802.6***

A especificação IEEE 802.16, teve início em 2001 e atende ao objetivo de implementar acesso de banda larga sem fio em diversas situações:

- IEEE 802.16d – acesso fixo
- IEEE 802.16e – acesso móvel

Houve uma associação de diversos fornecedores para desenvolvimento do padrão. Nesta associação encontramos gigantes como AT&T, Intel, Nokia, Proxim, RADNET, Siemens, Vcom e o IEEE.

Algumas características da tecnologia WiMax:

- Alcance de até 50 KM* (previsão)
    - No limite de distância exige visada
    - 5 a 8 Km sem visada
- Velocidade de transmissão de 75 Mbps* (previsão)
- Permite a conexão de milhares de clientes em uma única célula
- Implementa QoS (Qualidade de Serviço)
    - Permite tráfego multimídia
    - Voz, Dados e Imagem
- Opera na faixa de freqüência de 2 a 11 GHz
    - Possibilidade de interoperar com outros padrões (interoperabilidade)

# UNIDADE 21

*Objetivo:Saber mais sobre a  Vulnerabilidade das Redes sem fio.*

**Vulnerabilidades**

As redes de computadores baseadas em tecnologias wireless estão se tornando uma realidade para um grande conjunto de instituições e empresas. Entretanto, as redes sem fio apresentam uma série de vulnerabilidades que tem sua origem na concepção dos padrões adotados.

Ao contrário das redes cabeadas, as redes sem fios são de transmissão não guiada num meio comum e acessível a todos, dentro do raio de ação das antenas. Neste cenário, caso a rede não tenha configurados mecanismos mínimos de segurança, o acesso a essa rede fica imediatamente disponível a quem esteja dentro do raio de ação dos APs, com um terminal compatível com a tecnologia utilizada.

***Ataques***

Os ataques mais comuns em redes sem fio referem-se à obtenção de informações sem autorização, acesso indevido à rede e ataques de negação de serviço. Estes ataques possuem graus de dificuldade dependentes das características de implantação da rede, o que significa dizer que, para que uma rede sem fios possua as mesmas características de segurança de uma rede com fios, existe a necessidade de inclusão de mecanismos de autenticação de dispositivos e confidencialidade de dados.

***Como se proteger?***

Afinal, com um transmissor irradiando dados através de uma rede em todas as direções, como impedir que uma pessoa mal intencionada possa se conectar a ela?

Recentemente, o IEEE ratificou um novo padrão, o 802.11i, que traz todas as premissas de segurança intrínsecas aos protocolos IEEE 802.11b, 80211a e 802.11g, entre elas a melhoria do método de criptografia WEP (Wireless Equivalent Privacy), que se destina a fornecer às redes sem fio o mesmo nível de segurança das redes convencionais com cabeamento.

***WEP***

As normas iniciais Wi-Fi previram um mecanismo denominado de WEP (Wired Equivalent Privacy) para garantir privacidade da informação. Este sistema baseia-se num segredo partilhado, só conhecido entre os terminais e os APs.

O WEP apresenta deficiências técnicas, sendo possível quebrá-lo em pouco tempo, recorrendo a recursos computacionais modestos. Por isso, a configuração de proteção WEP não deve ser considerada uma medida de segurança suficiente para suster um indivíduo motivado para penetrar a rede. Algumas medidas simples de segurança:

Configurar WEP – apesar das suas vulnerabilidades, ter WEP é melhor do que não ter qualquer proteção. De preferência, a chave deve ser alterada regularmente, em especial quando se pretende revogar as permissões de acesso de um utilizador. Só se deve utilizar o WEP se não for possível atualizar os equipamentos para WPA ou WPA2, descritos mais à frente.

Esconder o SSID (Service Set Identifier) - com esta medida evita-se que o AP anuncie a rede. O intruso terá, portanto mais dificuldade em conhecer o identificador da rede a que se associar.

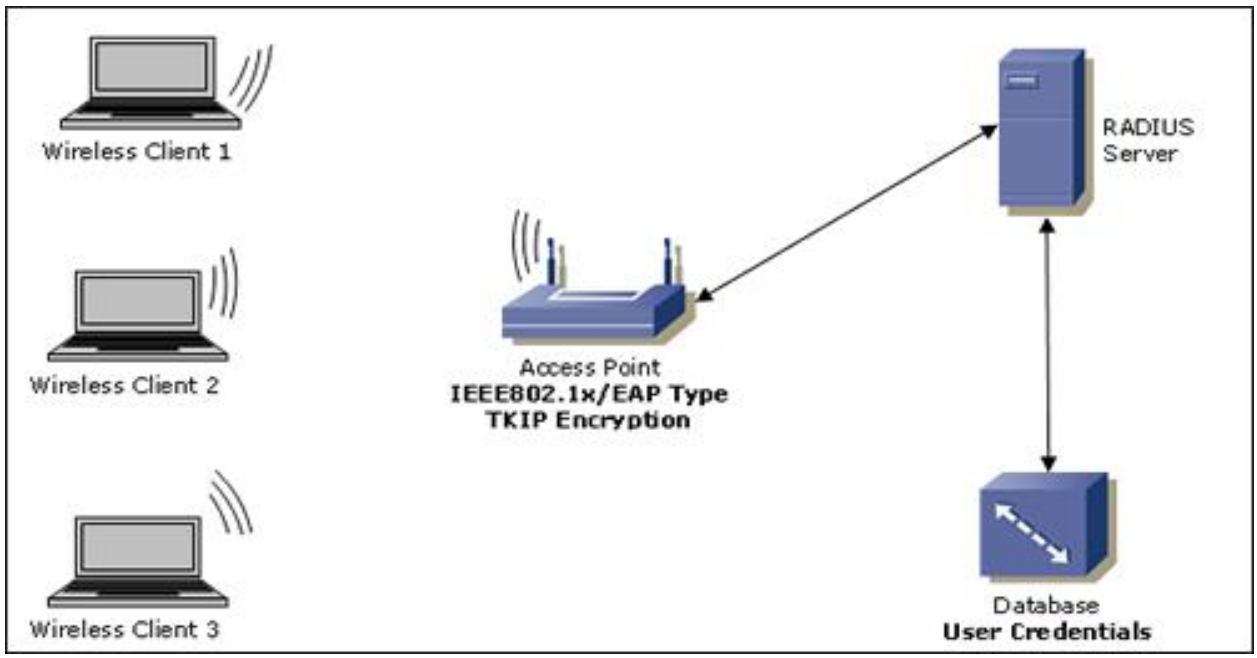
Filtragem dos endereços MAC – conhecendo-se de antemão os endereços MAC dos computadores que acedem à rede é possível configurar o AP para permitir acesso apenas a

esses MACs. Um intruso poderá, porém mudar o ser endereço MAC para coincidir com um endereço MAC que saiba ser permitido na rede.

Desligar os APs quando não estiverem em uso – com esta medida reduz-se o tempo de exposição da rede a ataques, sendo também mais provável detectar utilizações anômalas da rede, como, por exemplo, tráfego extraordinário no AP, que se pode detectar pelo piscar mais frequente da luz avisadora de atividade de rede.

### *WPA ou WPA2 - Wi-Fi Protected Access*

O WPA foi criado para substituir o WEP que, como foi referido, tem vulnerabilidades de segurança graves. Sempre que possível deve usar-se WPA2 ou WPA como mecanismo de segurança, exigindo que novos equipamentos tenham capacidade WPA2, ou atualizando os equipamentos existentes para essa tecnologia.



O WPA2 quando configurado e utilizado corretamente, designadamente do que diz respeito a escolha de chaves ou passwords, não apresenta vulnerabilidades de segurança conhecidas atualmente.

O WPA e WPA2 são semelhantes havendo, porém exceções, designadamente no algoritmo de cifra, onde o WPA2 apresenta um algoritmo mais forte, o AES, do que o WPA.

Em alguns casos é possível configurar WPA2 nos dispositivos físicos existentes através de atualização de software, no Sistema Operacional, nos drivers ou no firmware das placas.

# UNIDADE 22

*Objetivo:Compreender a  Aplicação de redundância e contingência.*

**Projeto de rede seguro**

O projeto bem sucedido de uma rede de computadores pode ser representado pela capacidade desta em oferecer os serviços essenciais requeridos por seus usuários e por preservar os seus principais componentes na eventual ocorrência de falhas.

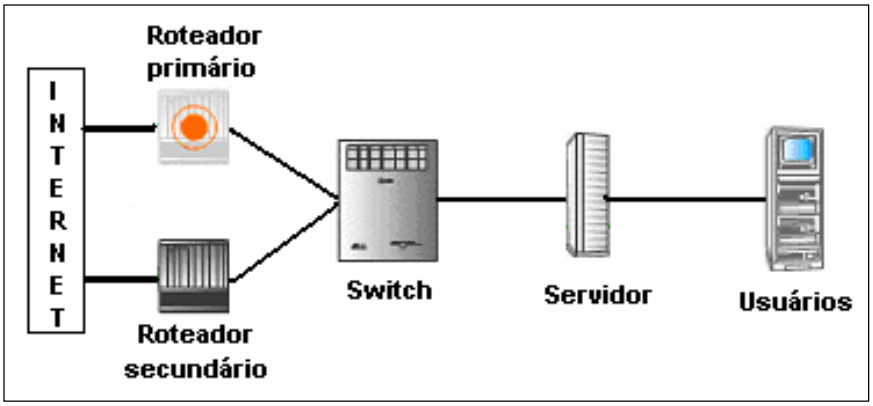
***Redundância***

O termo redundância descreve a capacidade de um sistema em superar a falha de um de seus componentes através do uso de recursos redundantes, ou seja, um sistema redundante possui um segundo dispositivo que está imediatamente disponível para uso quando há falha no dispositivo primário do sistema.

Uma rede de computadores redundante caracteriza-se, pois, por possuir componentes como sistemas de ventilação e ar condicionado, sistemas operacionais, unidades de disco rígido, servidores de rede, links de comunicação e outros, instalados para atuarem como backups das fontes primárias no caso delas falharem.

Um exemplo bem conhecido de um sistema redundante em redes de computadores é o RAID (Redundant Array of Independent Disks).

Neste exemplo a seguir, caso ocorra uma falha no roteador primário, imediatamente o secundário entrará em atividade de forma a manter o funcionamento ininterrupto da comunicação da rede local com o ambiente externo (Internet).




Um bom exemplo de redundância está em múltiplas estações de trabalho usadas para monitorar uma rede. A perda de uma estação não prejudica a visualização ou a operação do sistema. Nesse caso, um servidor de banco de dados (igualmente redundante) garante que nenhuma informação seja perdida, na hipótese de falha do servidor primário.

Podemos ter também a redundância física de um subsistema de alimentação de energia, e a contingência operacional proporcionada pela redundância de equipamentos. Quanto maior a vulnerabilidade de um sistema dentro de uma rede, maior a redundância necessária para garantir a integridade dessa rede.

***Contingência***

Define-se contingência como a possibilidade de um fato acontecer ou não. É uma situação de risco existente, mas que envolve um grau de incerteza quanto à sua efetiva ocorrência. As ações de contingenciamento são encadeadas, e por vezes sobrepostas, de acordo com procedimentos previamente acordados no projeto da rede.

As condições necessárias para a existência de uma contingência são: possibilidade de um acontecimento futuro resultante de uma condição existente, incerteza sobre as condições operacionais envolvidas e a resolução destas condições dependerem de eventos futuros.

O objetivo da contingência é implantar, conectado à estrutura de rede de computadores, um plano de acesso seguro, eficiente e gerenciado, capaz de restabelecer as funções críticas numa situação excepcional.

### *Planos de contingência*

Trata-se do conjunto de procedimentos e medidas de segurança preventivas, previamente planejadas, a serem adotadas após a ocorrência de uma falha, que permitem o restabelecimento da rede de comunicação em caso de situações anormais (falha de hardware, base de dados corrompida, perda de link de comunicação, destruição de prédios, entre outras), com o objetivo de minimizar os impactos da mesma.

Na implementação do plano devem ser avaliados os principais riscos que podem fazer o sistema parar. Para isso, deve-se proceder ao levantamento dos impactos dessa parada em cada área de negócio e estimar quanto tempo levaria para restabelecer o processamento para cada risco e para cada área.

Os planos de contingência estão subdivididos em três módulos distintos e complementares: plano de administração de crise, plano de continuidade operacional e plano de recuperação de desastres.

### *Objetivos do plano de contingência*

O principal objetivo de um plano de contingência é dar providência imediata invocando os procedimentos de recuperação dos sistemas corporativos, considerando o tempo de espera previsto para restabelecimento da atividade definido pelos gestores do sistema.

De forma global, as ocorrências de falhas mais comuns são: Vírus, perda de disco rígido, perda de um servidor da rede ou de uma ligação de rede, alteração/atualização de software, falha de sistema de suporte (ar condicionado e/ou de energia, por exemplo), avarias mecânicas do hardware, etc.

Um plano de contingência deve ser desenvolvido por uma equipe de trabalho que envolva todas as áreas de conhecimento e de negócio da empresa a qual o plano de contingência diz respeito, ser avaliado periodicamente e estar disponível em local reservado e seguro, mas de fácil acesso ao pessoal autorizado.

# UNIDADE 23

*Objetivo:Conhecer  O que é uma VLAN?*

**VLAN**

A sigla VLAN Virtual expande a rede de área local. Uma VLAN é uma lógica de rede local (ou LAN) que se estende para além de uma única rede local tradicional para um grupo de segmentos LAN, dado configurações específicas. Porque uma VLAN é uma entidade lógica, a sua criação e configuração são feitas totalmente em software.

***Identificando uma VLAN***

Uma vez que uma VLAN é um conceito de software, identificadores e configurações de uma VLAN devem ser devidamente preparados para que possa funcionar como esperado. Frame colorir é o processo utilizado para garantir que VLAN membros ou grupos sejam devidamente identificados e processados.

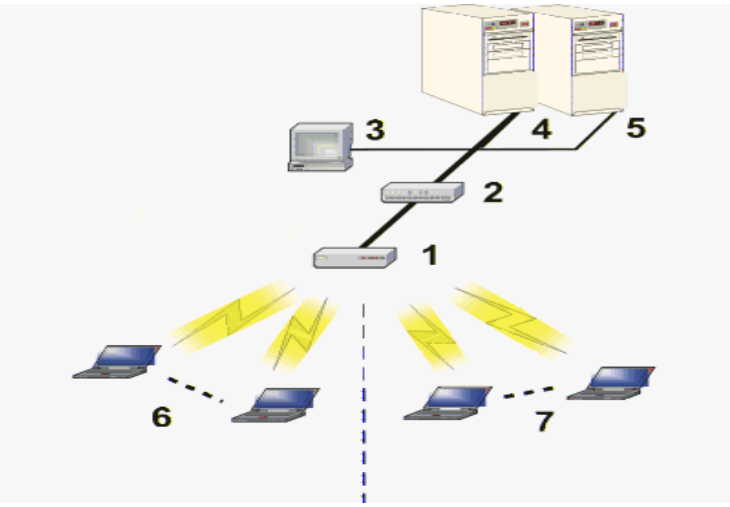
Com moldura colorir, pacotes são dadas a boa VLAN ID, na sua origem, para que eles possam ser devidamente tratados, uma vez que passam através da rede. A VLAN ID é então usada para permitir a comutação e encaminhamento motores para tornar as decisões apropriadas, tal como definidos na configuração da VLAN.

As Redes locais virtuais (VLANs) são agrupamentos lógicos de host da rede. Definidos por configurações de software, outros membros ou recursos da VLAN parecem (aos clientes) estar no mesmo segmento físico, sem importar onde estão conectados no segmento LAN ou WAN lógico. Eles simplificam o fluxo de tráfego entre clientes e seus recursos restritos ou frequentemente usados.

As VLANs agora vão mais além, chegam até o sinal do ponto de acesso. Os clientes podem ser segmentados em sub-redes sem fio por meio da atribuição de SSID e VLAN. Um cliente pode acessar a rede conectando-se a um AP configurado para suportar seu SSID/VLAN atribuído.

Os dispositivos do AP estão plenamente preparados para VLAN; contudo, por padrão, o suporte à VLAN está desativado. Antes de ativar o suporte à VLAN, determinadas definições de rede devem ser configuradas e alguns recursos de rede como uma chave de alerta de VLAN, um servidor RADIUS e possivelmente um servidor DHCP devem estar disponíveis.

Os dados marcados da VLAN são coletados e distribuídos pela(s) interface(s) sem fio de um AP, com base no Nome da rede (SSID). Uma porta Ethernet no ponto de acesso conecta uma célula ou rede sem fio a um backbone com fio. Os pontos de acesso se comunicam por meio de um switch compatível com a VLAN que analisa os cabeçalhos dos pacotes marcados pela VLAN e direciona o tráfego às portas apropriadas. Na rede com fio, um servidor RADIUS autentica o tráfego e um servidor DHCP gerencia os endereços IP da(s) VLAN(s). Recursos como servidores e impressoras podem estar presentes e um hub pode incluir vários APs, ampliando a rede em uma área maior.



Os itens numerados correspondem aos seguintes componentes:

1. Ponto de acesso ativado para VLAN
2. Switch de alerta da VLAN (IEEE 802.1Q uplink)
3. Gerenciamento de AP por host com fio (SNMP, interface da Web ou CLI)
4. Servidor DHCP
5. Servidor RADIUS
6. VLAN 1
7. VLAN 2

**Dica**

Saiba mais sobre VLAN em:

http://pt.wikipedia.org/wiki/Vlan

# UNIDADE 24

*Objetivo: Entender o uso de um Firewall.*

**Conceito de Firewall**

Um firewall pode ser definido como uma coleção de componentes ou mesmo um sistema colocado entre duas redes de comunicação que possui as seguintes propriedades:

- Todo o tráfego de dentro para fora dessa rede e vice-versa deve passar pelo firewall;
- Só o tráfego definido pela política de segurança da rede é permitido a passar pelo firewall;
- O próprio sistema do firewall deve ser altamente resistente a qualquer tentativa de invasão.

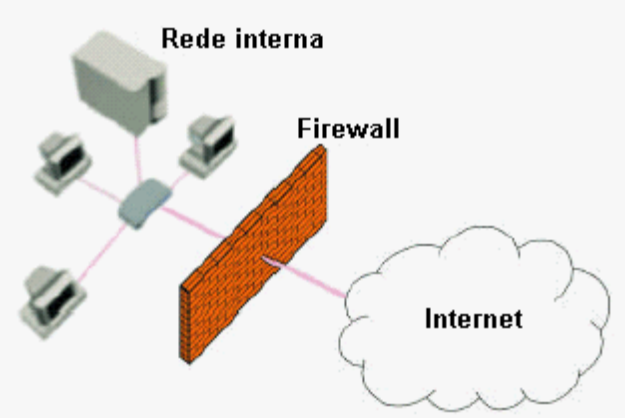
Dessa forma, o firewall é um mecanismo utilizado para proteger uma rede interna (confiável) de outra rede externa (não confiável). Um firewall assegura que não há possibilidades de acesso à rede externa (por exemplo, Internet) a partir da rede interna, nem vice-versa, a não ser que se passe por esse ponto. Ele verifica e filtra todas as conexões vindas da rede externa para a rede interna e vice-versa através de um único ponto de acesso seguro.

Os firewalls podem se apresentar em três tipos:

***Filtros de pacotes*** – é o tipo mais comum de firewall e tem como objetivo permitir ou negar a entrada de um determinado pacote de informações em uma rede, levando em consideração o endereço IP ou a porta de origem e de destino;

***Inspeção de pacotes com informações de estado*** - além de desempenhar as funções do filtro de pacotes, inspecionam o estado da conexão, ou seja, apenas aquelas conexões previamente estabelecidas e válidas que cumprem as condições configuradas pelo firewall têm acesso à rede;

***Aplicativos de Firewall e de Proxy*** - são os mais complexos, pois varrem todos os dados que passam por eles, descartando os perigosos ou não autorizados, não permitindo que a rede interna fique exposta.




*Exemplo de aplicação de firewall*

***Segurança de conteúdo***

A segurança de conteúdo permite a um administrador bloquear o acesso a sites da web com base no URL ou no endereço IP. A segurança de conteúdo com base em firewall funciona mantendo uma tabela extensiva de endereços da web, para os quais o administrador de rede deseja negar acesso. Em geral, essa tabela pode conter URLs completos ou pode filtrar sites baseados em palavras-chave.

O método de bloquear sites por palavras-chave pode se tornar um inconveniente uma vez que permite bloquear outros sites não relacionados com a palavra em questão.

Digitar uma URL completa para bloquear cada site não desejado seria quase impossível. Poderia haver milhares de endereços que poderiam considerar censuráveis.

ACESSO NÃO PERMITIDO

Por essa razão, a maioria dos firewalls que fornecem conteúdo de segurança não apenas lhe permitirá editar sua própria tabela de bloqueio de URLs, mas também comprará listas de um fornecedor de ferramentas de seleção de URLs.

## Dica

Saiba mais sobre Firewall em:

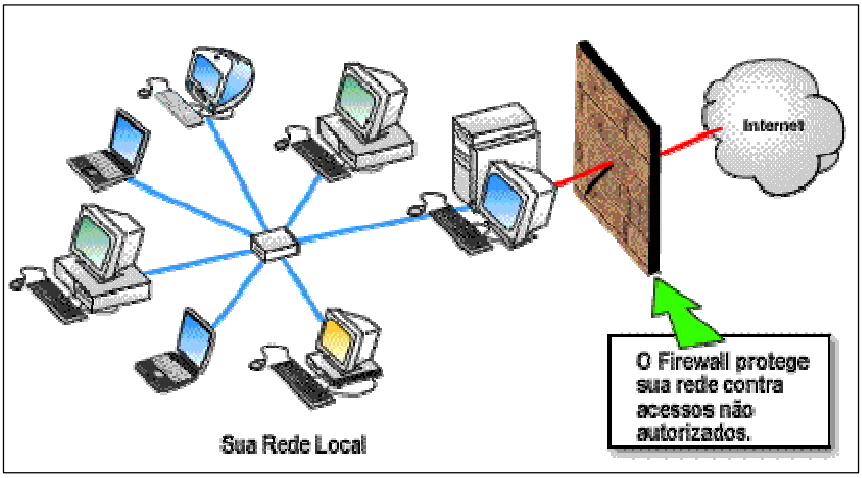
http://pt.wikipedia.org/wiki/firewall

# UNIDADE 25

*Objetivo: Entender os Proxies.*

**Proxies**

Um servidor proxy é usado como um gateway central através do qual todos os usuários acessam a Internet.




*Exemplo de Proxy*

Tendo em vista que todos os usuários devem passar por um servidor proxy antes de alcançarem a Internet, várias operações podem ser executadas sobre eles antes e durante uma sessão da Internet. Em vez de restringir os locais que os usuários podem visitar on-line, alguns clientes devem restringir quem pode usar a Internet.

Um servidor proxy pode ser configurado para permitir ou negar acesso à Internet com base em configurações individuais ou de grupo. É possível configurar um grupo de usuários e

permitir apenas as pessoas desse grupo acessem a Internet. Isto daria ao cliente o controle sobre quem na empresa poderia usar os recursos da World Wide Web.

Para muitos clientes, esse pode ser um curso de ação interessante. Em vez de se preocupar em bloquear os sites, o acesso é concedido a usuários confiáveis. Se houver abuso do privilégio, o acesso do usuário à Internet poderá ser negado completamente.

Para alguns clientes, a colocação de usuários em grupos para determinar o acesso à Internet pode ser uma sobrecarga administrativa. É mais uma interface de servidor para manter e uma lista de usuários completamente diferentes para atualizar.

Cliente preocupado com o tempo de administração necessário para manter permissões de grupos em um servidor proxy têm outra opção. Muitos servidores proxy podem também manter uma lista de usuário individual.

O servidor proxy pode estabelecer sua lista de usuários a partir do sistema operacional. Assim, fica mais fácil indicar nas preferências individuais de usuários de rede se eles devem ter acesso à Internet. Essa parece ser a configuração mais comum para servidores proxy.

Como os servidores proxy atuam sobre usuários individuais, o servidor precisa manter uma tabela listando todos os usuários e suas permissões relacionadas. Esta tabela fornece a base para a função mais útil de um servidor proxy: rastrear a utilização on-line.

Tendo em vista que todas as solicitações da Internet passam pelo servidor proxy, e como o servidor proxy mantém uma tabela com uma entrada para cada usuário, podemos deduzir que o servidor proxy também pode ser usado para rastrear as visitas on-line de cada usuário.

**Dica**

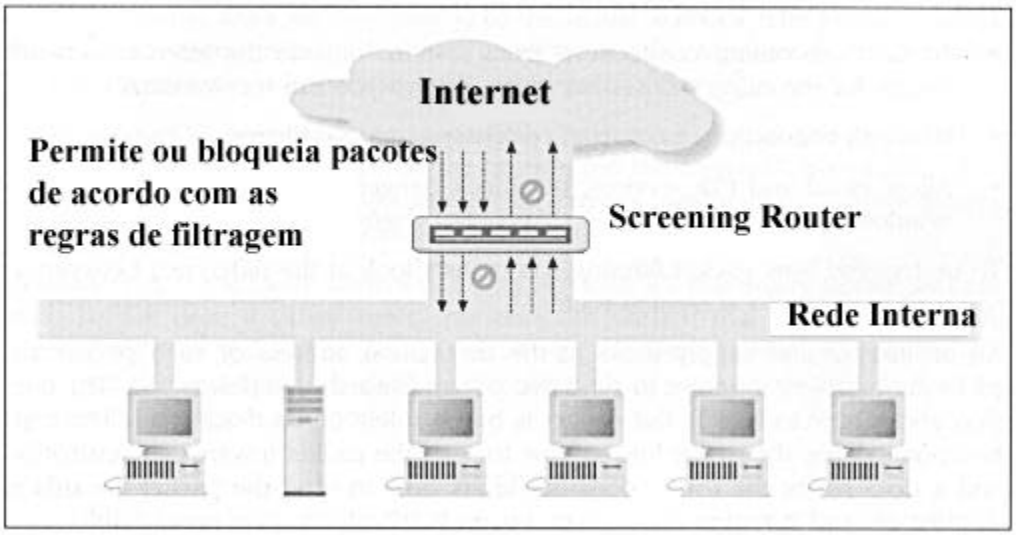
Saiba mais sobre proxies em:

http://pt.wikipedia.org/wiki/Proxy

### *O uso de Proxies e Firewalls juntos*

A grande vantagem do uso de Firewalls e Proxies juntos é que eles não interferem um com o outro. Como os dois produtos funcionam em diferentes fases do acesso do usuário, eles podem ser implementados na mesma rede.

Usando uma firewall e um servidor proxy, o cliente pode ter o controle sobre quem tem acesso à Internet sobre o que o usuário pode fazer depois de acessá-la. Esse tende a ser o nível mais confortável de segurança interna da Internet quem um cliente pode ter. O proxy impede que os usuários não desejados obtenham acesso a recursos da Internet, enquanto o firewall os impede de usar a Web para outros além dos aprovados.



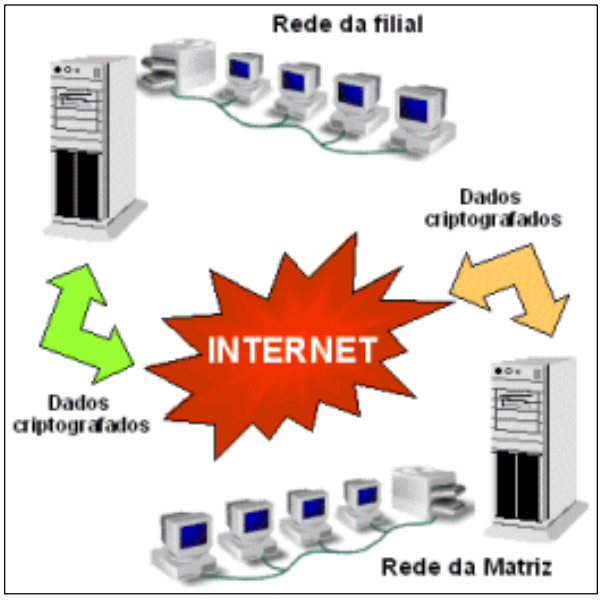
# UNIDADE 26

*Objetivo: Entender as Redes Privadas Virtuais – VPN.*

**VPN**

A comunicação entre uma matriz, suas filiais, fornecedores, distribuidores, clientes e usuários forma uma infraestrutura que corresponde à base dos ambientes de negócios das empresas.

Nesse cenário, as Redes Privadas Virtuais (Virtual Private Networks - VPN's) representam uma alternativa interessante para essa comunicação por possibilitarem a racionalização dos custos de manutenção das redes corporativas ao permitirem que as conexões dedicadas existentes, de custo mais elevado, sejam substituídas por conexões públicas mais seguras e com um custo operacional mais acessível.

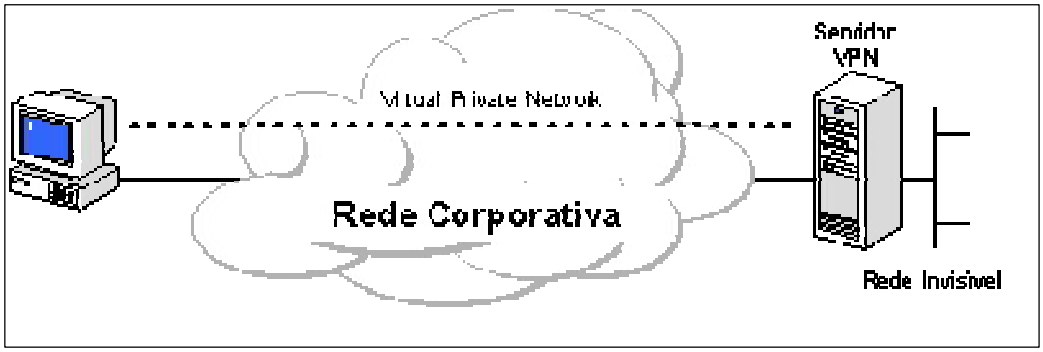



Os conceitos fundamentais de uma VPN são a criptografia e o tunelamento, onde a criptografia garante a autenticidade, a integridade e o sigilo das informações e o tunelamento permite a utilização da rede pública para o tráfego seguro dessas informações.

A ideia básica é utilizar, a partir da rede pública de telecomunicações, "túneis" de criptografia entre pontos autorizados, criados através da Internet ou outras redes existentes (públicas ou privadas) para a transferência de informações, de modo seguro, entre redes ou usuários remotos. Com esse recurso, redes situadas em locais geograficamente distintos podem, através de um link de comunicação, se conectar a um provedor de acesso, possibilitando o fluxo de informações de forma segura.

A segurança é a primeira e mais importante função de uma VPN. Uma vez que dados privados serão transmitidos pela rede pública, que é um meio de transmissão inseguro por natureza, eles devem ser protegidos de forma a não permitir que sejam modificados ou interceptados.

Com a utilização de uma VPN, um administrador de rede pode definir, por exemplo, quais usuários estarão credenciados a acessar determinados recursos da rede e quais usuários não terão acesso a esses mesmos recursos.




Os requisitos de segurança por sua vez podem ser divididos em dois grupos principais, os quais são independentes entre si, podendo ser utilizados de forma conjunta ou separada, de acordo com a necessidade de cada implementação:

Autenticação e Integridade - A autenticação garante que os dados recebidos correspondem àqueles originalmente enviados, assim como garante a identidade do emissor. Já a integridade significa que os dados transmitidos chegam íntegros ao seu destino, eliminando a possibilidade de terem sido modificados no caminho sem que isto pudesse ser detectado;

Confidencialidade - Apenas os usuários autorizados devem entender o conteúdo transportado. Pessoas não autorizadas, mesmo tendo capturado o pacote, não poderão ter acesso às informações nele contidas. O mecanismo mais usado para prover esta propriedade é chamado de criptografia.

No desenvolvimento de soluções de rede também é desejável que facilidades de controle de acesso às informações e aos recursos corporativos sejam implementadas.

Uma VPN deve dispor de recursos que permitam o acesso de clientes remotos autorizados aos recursos da LAN corporativa, bem como viabilizar a interconexão de LANs para o compartilhamento de recursos e de informações, assegurando a privacidade e a integridade de dados ao atravessar a rede pública, bem como da própria rede corporativa. As características mínimas desejáveis para uma VPN sob o aspecto da segurança são as seguintes:

Autenticação de Usuários - Verificação da identidade do usuário, restringindo o acesso às pessoas autorizadas. Deve dispor de mecanismos de auditoria, provendo informações referentes aos acessos efetuados to tipo "quem acessou, o quê" e "quando ocorreu o acesso";

Gerenciamento de Endereços - O endereço do usuário na rede privada não deve ser divulgado, devendo-se adotar endereços fictícios para o tráfego externo;

Criptografia de Dados - Os dados devem trafegar na rede pública ou privada em formato cifrado e, caso sejam interceptados, não deverão ser decodificados, garantindo a privacidade da informação. O reconhecimento do conteúdo das mensagens deve ser exclusivo dos usuários autorizados;

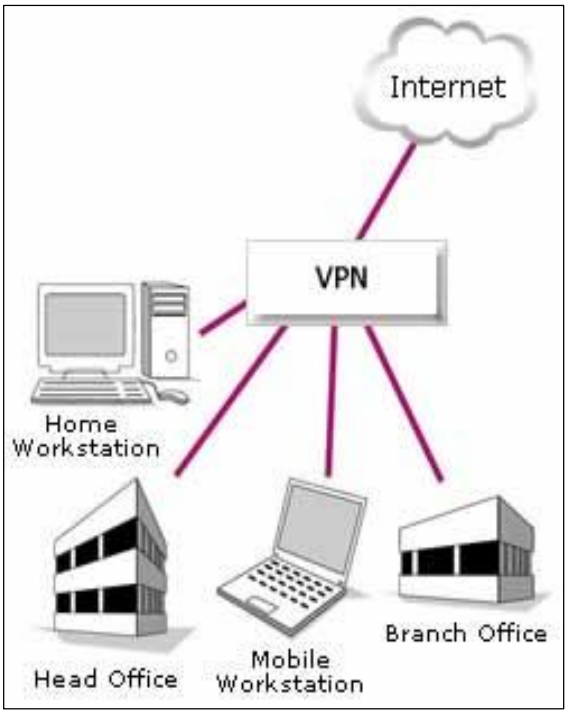
Gerenciamento de Chaves - O uso de chaves de segurança nas mensagens criptografadas deve funcionar como um segredo compartilhado exclusivamente entre as partes envolvidas. O gerenciamento de chaves deve garantir a troca periódica das mesmas, visando manter a comunicação de forma segura;

# UNIDADE 27

*Objetivo: Conhecer as Limitações de uma VPN.*

**Limitações**

Atualmente é cada vez mais crescente a utilização da Internet como meio para a troca de informações nas empresas. Consequentemente, a demanda por segurança e confidencialidade das informações teve que acompanhar esse crescimento, originando uma solução eficiente e de excelente custo benefício conhecida como redes VPN (Virtual Private Network) que, entretanto, apresenta algumas limitações.



Como as redes de computadores atuais, por menores que sejam, apresentam uma variedade significativa de equipamentos em termos de tipos, quantidades e configurações, é praticamente impossível conseguir um ambiente absolutamente seguro.

Considerando a disposição geográfica e quantidade dos seus elementos constituintes, aliados aos aspectos de segurança requeridos para cada sistema local, a administração de uma rede utilizando VPN pode se tornar uma tarefa complexa. Essa complexidade pode aumentar ainda mais com o aumento do número de equipamentos, tornando difícil manter um mínimo de segurança para a rede privada.

### *Falhas na VPN*

As falhas em redes de comunicação utilizando VPN estão ligadas ao risco envolvido em determinadas configurações em função do investimento feito na solução, mas que se traduzem em riscos calculados.

Como a principal motivação para a constituição de VPN's é financeira, é muito comum configurar em um gateway da VPN serviços que não fazem parte do contexto de segurança, como servidores de e-mail e Web, com o objetivo de reduzir custos operacionais na contratação de links dedicados ou redes de pacotes. Essa atitude acaba por comprometer a segurança porque os equipamentos passam a ficar sujeitos aos ataques externos à rede e infecção por vírus através de e-mails ou conexão com a Internet.

Outra falha em VPN acontece devido à forma como a segurança é tratada (ou menosprezada) dentro da política de segurança adotada nas empresas. Pesquisas recentes demonstraram que a maioria dos ataques sofridos nas empresas não ocorre sobre os elementos da VPN, como o firewall, por exemplo, mas direcionados aos servidores de fax, de web (a exploração de falhas em servidores web é uma das práticas mais utilizadas na Internet), modems para acesso remoto e estações de usuários utilizando uma senha-padrão que nunca foi modificada.

As pesquisas também apontaram que os maiores problemas dentro de um ambiente controlado com firewall, VPN, etc, são os que ocorrem dentro da própria infraestrutura da rede. Esses problemas tornam a rede vulnerável a outros tipos de falhas consideradas altamente críticas e não calculadas, que podem expor a rede a ataques do tipo negação de serviço - DoS (Denial of Service) - identificação remota de serviços ativos e manipulação da configuração do firewall, entre outros.

Pior que não ter segurança nos sistemas é possuir uma falsa impressão de segurança. A segurança de uma rede não é apenas uma questão técnica, envolve também aspectos gerenciais e humanos. Não adianta adquirir uma série de equipamentos de hardware e software sem treinar e conscientizar o nível gerencial da empresa.

Os riscos podem ser identificados, quantificados e então reduzidos, mas não é possível eliminá-los completamente. Por esse motivo, deve-se considerar a existência de uma equipe especializada, treinada para gerenciamento e suporte das conexões, a fim de garantir agilidade na recuperação dos serviços no caso de falhas ou de interrupção da rede.

**Dica**

Saiba mais sobre VPN em:

http://pt.wikipedia.org/wiki/Vpn

# UNIDADE 28

*Objetivo: Compreender uma DMZ.*

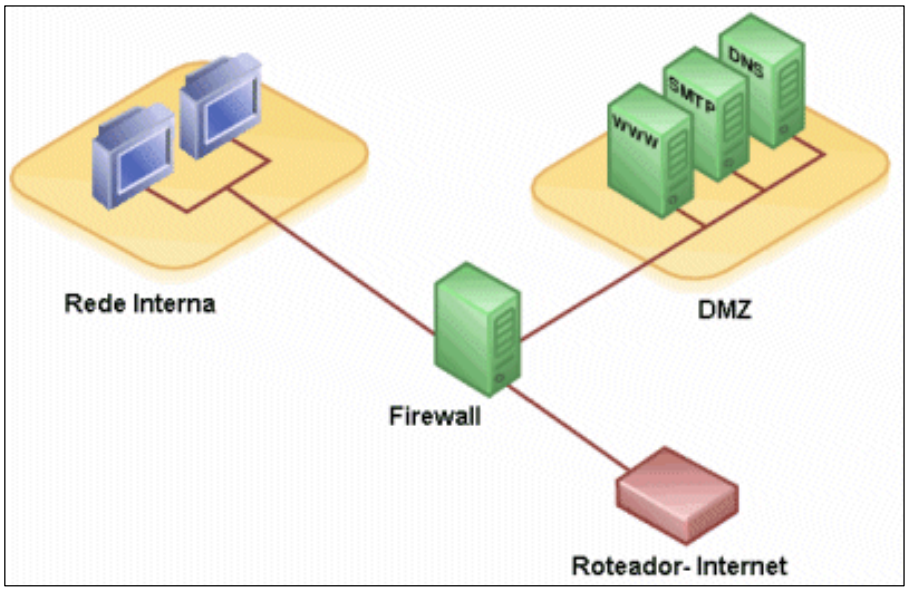
**DMZ**

DMZ é abreviação para ***D*** E ***M*** ilitarized ***Z*** um.

Uma DMZ ou ainda "Zona Neutra" corresponde ao segmento ou segmentos de rede, parcialmente protegido, que se localiza entre redes protegidas e redes desprotegidas e que contém todos os serviços e informações para clientes ou públicos.

A DMZ pode também incluir regras de acesso específico e sistemas de defesa de perímetro para que simule uma rede protegida e induzindo os possíveis invasores para armadilhas virtuais de modo a se tentar localizar a origem do ataque.

Um DMZ geralmente contém servidores que prestam serviços aos usuários da Internet, tais como web, ftp, e-mail (SMTP, POP3 e IMAP4), e servidores de DNS. Embora esses servidores devam ser abertos a partir de um acesso limitado à internet, eles também devem ser protegidos por um firewall.



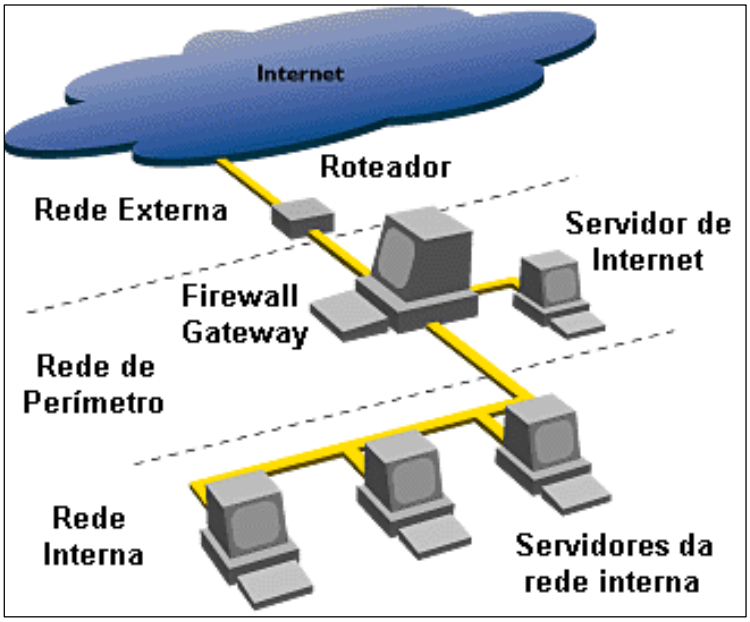
Podemos ter dois tipos de DMZ's: a interna, só acessada pelo usuário da rede interna e a DMZ externa, acessada por qualquer usuário da Internet. Este conceito aliado ao de VLAN's também permite a implantação de DMZ's privadas, ou seja, a possibilidade de DMZ's específicas para cada cliente de hosting ou para a hospedagem de servidores.

Resumindo, as DMZ's são sub-redes onde se hospedam os servidores/serviços de um provedor, protegidos contra ataques da Internet por um firewall.

***Rede de Perímetro***

O termo rede de perímetro refere-se a um segmento de rede isolado no ponto em que uma rede corporativa alcança a Internet. As redes de perímetro destinam-se a criar um limite que permite a separação do tráfego entre redes internas e externas.

Com este limite, é possível categorizar, colocar em quarentena e controlar o tráfego da rede de uma empresa. A segurança de perímetro é proporcionada por um dispositivo de perímetro, como um firewall, por exemplo, que inspeciona os pacotes e as sessões para determinar se devem ser transmitidos para a rede protegida ou a partir dela ou ser abandonados.



***Como criar uma DMZ?***

O mais simples método de criação de uma DMZ é utilizar um firewall com três ou mais interfaces de rede. A cada interface é atribuído um papel específico:

- Confiáveis rede interna
- DMZ rede
- Externo redes não confiáveis (a Internet)

A utilização de uma porta Ethernet card no seu firewall irá permitir que você crie uma rede nesta configuração, ou até mesmo permitir que você crie uma rede separada em duas DMZ's.

Separar o seu DMZ hosts em múltiplas DMZ's irá contribuir para limitar os danos que podem ocorrer se um dos seus DMZ hosts estiver comprometido.

Um firewall irá normalmente ser configurado para proteger a rede interna da Internet.

Para criar uma DMZ, o firewall também deve aplicar as regras para proteger a DMZ a partir da Internet e das regras para proteger a rede interna da DMZ.

Isto tornará mais difícil para um atacante penetrar na sua rede interna.

## Dica

Saiba mais sobre DMZ em:

http://pt.wikipedia.org/wiki/DMZ_(computação)

## Atividades

ATENÇÃO! Para garantir a qualidade da aprendizagem, não dê continuidade aos estudos sem antes realizar as atividades encontradas na lista 3 (ATIVIDADE 3).

# UNIDADE 29

*Objetivo: Conhecer o Passo a passo na elaboração do projeto de redes.*

**Conceito de Gerenciamento de Projeto**

Como em qualquer outro Projeto, a Implementação de uma Rede deve seguir uma Metodologia para garantir o sucesso de todo o ciclo.

Um projeto é um esforço temporário empreendido para criar um produto, serviço ou resultado exclusivo.

Portanto, a implementação de uma Rede deve ser encarada como um Projeto, definindo escopo, prazo, custo, papeis, risco, comunicação, aquisições, qualidade e a integração entre todos estes conhecimentos. O responsável pelo projeto de implementação de uma rede, deve possuir uma visão holística e se preocupar com todos os elementos de um Projeto.

Por questões de semântica, não devemos confundir o Gerente de Projetos, que será o responsável pela criação do Plano de Projeto de Rede e seu gerenciamento, com o Projetista de Rede, que será o responsável com habilidades técnicas para criar o Projeto de Redes.

Convenhamos que, em muitos casos, acabamos acumulando os dois papeis, quando ainda não auxiliamos na montagem física da rede.

Neste módulo de estudos, iremos abordar apenas a criação do PROJETO DE REDES, e não o PLANO DE GERENCIAMENTO DE PROJETOS. Entretanto, os conceitos de Gerenciamento de Projetos não devem ser ignorados.

**Dica**

Saiba mais sobre Gerência de Projetos em:

http://pt.wikipedia.org/wiki/Gerência_de_projetos

http://pt.wikipedia.org/wiki/Projeto#Ciclo_de_Vida_de_Projeto

***Estrutura de Gerência de Projetos***

Para implementar um novo projeto de rede de computadores é necessário compreender e caracterizar com precisão a rede existente, traçando um perfil das suas necessidades atuais e futuras.

É necessário avaliar os dados não-técnicos relacionados com os objetivos, metas e restrições impostas ao projeto pelo seu solicitante. Essas informações são essenciais para a perfeita compreensão das tendências de crescimento esperado para o negócio, da estrutura da empresa e as políticas que poderão afetar o andamento do projeto.

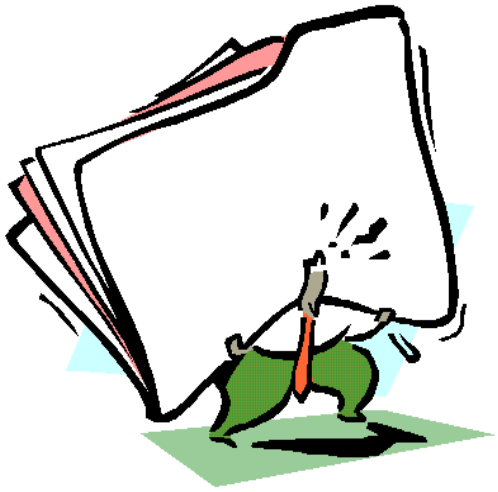
As informações técnicas disponíveis sobre a situação atual da rede, fazendo uma distinção entre as informações administrativas e os dados técnicos também devem ser consideradas.

### *Analisar o perfil do cliente*

Avaliar e compreender as informações sobre o perfil do solicitante ajuda a caracterizar o tipo do negócio e as possíveis restrições, além de permitir um conhecimento inicial das necessidades de uma nova rede ou da melhoria de uma rede atual. Os dados levantados, referentes ao perfil do cliente, auxiliam a determinar alguns pontos importantes que guiarão a execução do projeto.

Considerando que um projeto de rede de computadores normalmente se assemelha com a estrutura corporativa do cliente e deve atender a esta, um organograma ou outro documento similar será de grande importância para a compreensão da estrutura da rede. Neste caso, as informações mais relevantes dizem respeito à hierarquia e a forma como as áreas da empresa interagem umas com as outras.

Outra informação importante diz respeito à estrutura geográfica, ou seja, como a empresa está distribuída geograficamente e a influência dessa disposição sobre a estrutura da rede corporativa. Essa avaliação auxilia na caracterização das principais comunidades de usuários e localização dos aplicativos de rede.



# UNIDADE 30

*Objetivo:Conhecer os  Pontos importantes na elaboração do projeto de redes.*

**Etapas de um projeto de rede**

Para descrever com maior precisão a situação de uma rede pode-se adotar uma lista que inclui etapas que facilitam a análise:

1. ***Caracterização das aplicações do cliente*** – esta etapa envolve a criação de uma tabela detalhada que tem como objetivo documentar todas as aplicações que utilizarão a rede. Deve apresentar alguns campos essenciais como o nome da aplicação, o tipo da aplicação (banco de dados, internet, e-mail, etc), número de usuários que a utilizam, número de hosts ou servidores para cada aplicação, entre outros.

2. ***Caracterização dos protocolos de rede*** – funciona de forma semelhante à coleta de informações sobre as aplicações. Para tanto, outra tabela deve ser criada incluindo informações sobre os protocolos em execução na rede, o tipo de protocolo (roteamento, LAN, de servidor, etc), número de usuários, número de hosts ou servidores que os utilizam, entre outros.

3. ***Identificação dos possíveis gargalos*** – nessa etapa deve-se procurar identificar os possíveis enlaces ou segmentos que sejam parcial ou totalmente utilizados, em virtude do tráfego de broadcast / multicast que passará por eles.

4. ***Identificação das restrições do projeto*** – é necessário documentar e identificar os dados não-técnicos do cliente, pois essas informações têm impacto no processo de construção e implementação do projeto de rede.

5. ***Caracterização do desempenho da rede*** – significa determinar os tempos de resposta entre os hosts, dispositivos e aplicações utilizadas.

6. ***Confiabilidade da rede existente*** – a análise da confiabilidade da rede existente deve ser cuidadosamente planejada a fim de obter dados confiáveis sobre o tráfego da rede.

7. ***Caracterização das ferramentas de gerenciamento*** – é necessário documentar as ferramentas de gerenciamento, bem como as ferramentas introduzidas para coletar as informações para o projeto de rede.

A avaliação dos objetivos comerciais do cliente constitui a primeira etapa a ser cumprida para a elaboração do projeto de uma nova rede de computadores. Por esse motivo é necessário coletar, organizar e documentar todas as informações obtidas, o que permitirá uma abordagem ampla que facilitará a identificação das necessidades de desempenho e os problemas que a rede de computadores deverá solucionar.

### *Aspectos importantes*

Além da tecnologia, é preciso considerar uma série de outros fatores coadjuvantes na implementação do projeto de uma rede de computadores. Os desafios englobam questões como qual tecnologia a adotar, compatibilidade entre equipamentos novos e existentes, suporte técnico, obsolescência, confiabilidade e performance esperados, entre outros.

Um dos grandes desafios enfrentados pelo projetista de redes ainda é fazer com que cada componente se conecte a todos os outros. Conexões com pontos remotos podem apresentar problemas de lentidão, tornando-se de manutenção difícil e dispendiosa.

Outros problemas com protocolos de rede, largura de banda de transmissão e gerenciamento da rede combinam-se para fazer da implementação da parte lógica um verdadeiro desafio. O que acontece na verdade é que os padrões raramente conseguem

acompanhar o passo da evolução nas tecnologias de redes. A funcionalidade e a velocidade de uma solução adotada hoje pode não ser mais tão vantajosa num futuro próximo.

Existem diversas topologias e layouts de rede. Um projetista deve considerar todas as possibilidades e parâmetros relacionados ao projeto, entre eles: custo, performance, segurança, escalabilidade, crescimento tecnológico, TCO, ROI, gerenciamento, entre outros.

***Total Cost of Ownership (TCO):*** É o resultante de todos os custos pertinentes a um projeto de redes em sua totalidade. Projeto, instalação, hardware, software, infraestrutura, etc, determinam "parcialmente" o TCO. Quando projetando redes é necessário idealizar as necessidades atuais e um possível crescimento tecnológico, além do aumento da demanda por performance, escalabilidade, segurança e fácil gerenciamento/administração da rede.

Return Of Investment (ROI): Assim como o TCO, o ROI deverá ser cuidadosamente planejado para evitar desperdícios, através de um planejamento de metas para atingir resultados concretos. Existem inúmeras ferramentas que poderão ser utilizadas para definir o ROI de um projeto.

Também é necessário considerar outros pontos importantes sobre a infraestrutura de rede, verificando desde o cabeamento novo ou já existente (especialmente sobre os padrões Ethernet), até as distâncias, limitações, regras gerais, entre outros itens.

Ao mesmo tempo, é possível encontrar redes onde outros elementos não foram considerados pelos projetistas por limitações orçamentárias, ou seja, basicamente o fator "custo" ainda é o principal elemento levado em consideração no momento de se projetar e executar a infraestrutura de uma rede de computadores.

Mesmo considerando essas limitações, algumas etapas fundamentais não podem ser negligenciadas durante o projeto sob pena de impactar negativamente na performance final da rede. Dentre esses itens, a seleção das tecnologias e dispositivos, tanto para redes de campus quanto para redes corporativas e os testes e a documentação de toda a rede, não podem ser esquecidos de forma alguma.

Da seleção adequada das tecnologias de rede, que podem ser desde Ethernet, Fast Ethernet ou ATM, por exemplo, nas redes de campus e Frame Relay e ISDN, nas redes corporativas e da escolha dos dispositivos de rede como roteadores, switches, servidores, etc, até o próprio cabeamento, é que teremos os parâmetros necessários para avaliar a disponibilidade e a performance do sistema como um todo.

Uma vez implementada a infraestrutura, serão os resultados dos planos de testes do piloto da rede que fornecerão os subsídios necessários para a otimização do projeto e a documentação final do que realmente foi implantado (também conhecido como As Built).

# GLOSSÁRIO

Caso haja dúvidas sobre algum termo ou sigla utilizada, consulte o link Glossário em sua sala de aula, no site da ESAB.

# BIBLIOGRAFIA

Caso haja dúvidas sobre algum termo ou sigla utilizada, consulte o link Bibliografia em sua sala de aula, no site da ESAB.