CURSOS TÉCNICOS SENAI

Saiba fazer e aconteça no mercado.

Curso Técnico em Manutenção e Suporte em Informática

Redes de Computadores

Curso Técnico em Manutenção e Suporte em Informática

Redes de Computadores

Confederação Nacional da Indústria
Serviço Nacional de Aprendizagem Industrial

Curso Técnico em Manutenção e Suporte em Informática

Redes de Computadores

Rodrigo Willemann
Anderson Rauber da Silva
Daniel Devegili

Florianópolis/SC
2011

Autor
RodrigoWillemann
Anderson Rauber da Silva
Daniel Devegili

Fotografias
Banco de Imagens SENAI/SC
http://www.sxc.hu/
http://office.microsoft.com/en-us/ images/
http://www.morguefile.com/
http://www.bancodemidia.cni.org.br/

Ficha catalográfica elaborada por Luciana Effting CRB14/937 - Biblioteca do SENAI/SC Florianópolis

W699r
Willemann, Rodrigo
Redes de computadores / Rodrigo Willemann, Anderson Rauber da Silva, Daniel Devegili. – Florianópolis : SENAI/SC/DR, 2011.
81 p. : il. color ; 30 cm.

Inclui bibliografias.

1. Redes de computadores. 2. Arquitetura de redes de computadores. 3. Roteadores (Redes de Computação). I. Silva, Anderson Rauber da. II. Devegili, Daniel. III. SENAI. Departamento Regional de Santa Catarina. IV. Título.

CDU 004.7

SENAI/SC — Serviço Nacional de Aprendizagem Industrial
Rodovia Admar Gonzaga, 2.765 – Itacorubi – Florianópolis/SC
CEP: 88034-001
Fone: (48) 0800 48 12 12
www.sc.senai.br

Prefácio

Você faz parte da maior instituição de educação profissional do estado. Uma rede de Educação e Tecnologia, formada por 35 unidades conectadas e estrategicamente instaladas em todas as regiões de Santa Catarina.

No SENAI, o conhecimento a mais é realidade. A proximidade com as necessidades da indústria, a infraestrutura de primeira linha e as aulas teóricas, e realmente práticas, são a essência de um modelo de Educação por Competências que possibilita ao aluno adquirir conhecimentos, desenvolver habilidade e garantir seu espaço no mercado de trabalho.

Com acesso livre a uma eficiente estrutura laboratorial, com o que existe de mais moderno no mundo da tecnologia, você está construindo o seu futuro profissional em uma instituição que, desde 1954, se preocupa em oferecer um modelo de educação atual e de qualidade.

Estruturado com o objetivo de atualizar constantemente os métodos de ensino-aprendizagem da instituição, o **Programa Educação em Movimento** promove a discussão, a revisão e o aprimoramento dos processos de educação do SENAI. Buscando manter o alinhamento com as necessidades do mercado, ampliar as possibilidades do processo educacional, oferecer recursos didáticos de excelência e consolidar o modelo de Educação por Competências, em todos os seus cursos.

É nesse contexto que este livro foi produzido e chega às suas mãos. Todos os materiais didáticos do SENAI Santa Catarina são produções colaborativas dos professores mais qualificados e experientes, e contam com ambiente virtual, mini-aulas e apresentações, muitas com animações, tornando a aula mais interativa e atraente.

Mais de 1,6 milhões de alunos já escolheram o SENAI. Você faz parte deste universo. **Seja bem-vindo e aproveite por completo a Indústria do Conhecimento.**

SERGIO ROBERTO ARRUDA
Diretor Regional SENAI/SC

Sumário

Conteúdo Formativo

Carga horária da dedicação

- Carga horária: 120 horas

Competências

- Executar serviços técnicos em atividades relacionadas à instalação, manutenção e operação da infraestrutura em redes locais com ou sem-fio, de acordo com os padrões de desempenho e funcionalidade da comunicação de dados, respeitando a segurança básica da informação e normas regulamentadoras.

Conhecimentos

- Modelo OSI.
- Modelo TCP/IP.
- Camada física.
- Controle de fluxo.
- Domínio de *broadcast*.
- Domínio de colisão.
- Encapsulamento/desencapsulamento.
- Endereçamento físico e lógico.
- Formas de comunicação (banda base, banda larga, simplex e duplex).
- Sistemas de numeração.
- Tecnologia de enlace; protocolo de enlace.
- Tecnologias de rede locais e longa distância.
- Tecnologia de *wlan*.
- Tecnologia de camada de rede.
- Tecnologia de camada física.
- Tecnologia de redes.
- Locais sem-fio.
- Tempestade *broadcast*.
- Trafego de informações na rede.
- Conversão numérica.
- Criptografia (conceito e aplicações dos protocolos).
- Protocolo roteável e roteamento.
- Protocolos utilizados na internet.
- Protoloco ARP e RARP.
- *Spanning tree*.

- Protocolos de autenticação.
- Protocolos de gerencia de rede.
- Protocolo de conexão remota.
- Protocolo de aplicação para telefonia IP.
- Topologia física e lógica.
- Topologia de rede, normas eia/tia, cabeamento estruturado.
- Equipamentos de monitoramento e controle de sinais analógicos e digitais.

Habilidades

- Avaliar o ambiente atual.
- Avaliar a tecnologia disponível.
- Elaborar uma solução adequada ao contexto.
- Interpretar as questões de projeto associadas às camadas 1 a 3 da estrutura ou topologia de uma rede local.
- Descrever o modelo de três camadas de um projeto.
- Descrever as similaridades e diferenças entre os modelos OSI e TCP/IP.
- Identificar os dispositivos usados nas redes.
- Aplicar os protocolos nas redes.
- Descrever a função, as vantagens e desvantagens dos repetidores, *hubs*, *bridges*, comutadores e componentes de rede sem-fio.
- Descrever a função das redes ponto-a-ponto e cliente-servidor analisando as vantagens e desvantagens.
- Identificar roteadores.
- Especificar e configurar forma básica de *Switch Ethernet*.
- Configurar pontos de acesso para rede sem-fio.
- Instalar e configurando equipamentos de gerência dos pontos de acesso.
- Instalar e configurar equipamentos de telefonia IP.
- Configurar basicamente roteadores.
- Utilizar a estrutura dos endereços IP.
- Identificar meios físicos.
- Realizar configuração básica de equipamentos ligados a rede local.

Atitudes

- Pró-atividade.
- Respeitar os prazos e horários propostos.
- Respeitar as normas de segurança.
- Atitudes zelosas perante máquinas e equipamentos.
- Respeitar as práticas de qualidade; ética.
- Trabalho em equipe.
- Responsabilidade sócio-ambiental.

Apresentação

Prezado aluno,

seja bem-vindo a unidade curricular Redes de computadores, onde você iniciará mais uma etapa desta trajetória de estudos, buscando conceitos para desenvolver habilidades profissionais relacionadas a Redes de computadores. Nessa unidade curricular apresentaremos informações técnicas importantes para entender o funcionamento das principais tecnologias aplicadas a redes de computadores, incluindo *hardware* e *software*.

Os profissionais que atuam nesta área podem especializar-se em projetos e engenharia de redes e em gestão e segurança de tecnologias da informação e comunicação. Avaliar as necessidades dos clientes e propor tecnologias para solucionar problemas são algumas das características desses profissionais.

Esteja atento, pois você também conhecerá um conjunto de ferramentas importantes para identificar problemas. Analisar as condições físicas e lógicas da rede é uma das atividades mais importantes para a identificação de problemas. Essa também é uma das atividades do técnico que deverá realizar reparos em redes de computadores.

Contamos com sua dedicação e desejamos sucesso em seus estudos!

Rodrigo Willemann

Formado em Ciências da Computação, é colaborador no SENAI em Jaraguá do Sul desde 2003, tendo participado na definição de vários cursos técnicos na área de informática. Ministrou disciplinas e cursos na área de redes de computadores. Atualmente é coordenador da Academia Local da Cisco e desenvolve projetos em parceria com empresas de diversos segmentos da região, como Gestor de Projetos do SENAI em Jaraguá do Sul.
Já coordenou projetos integradores para o Curso Técnico em Informática e Redes de Computadores. Atua como docente de unidades curriculares relacionadas a Redes de Computadores e Desenvolvimento de *Software*.

Anderson Rauber da Silva

Técnico em Informática com Habilitação em Redes pelo SENAI/SC de Jaraguá do Sul. Com graduação em Tecnologia em Redes de Computadores pelo SENAI/SC de Joinville.
Atua na unidade do SENAI/SC em Jaraguá do Sul como instrutor dos cursos de aprendizagem industrial e responsável técnico das aprendizagens industriais em informática.
É também instrutor de unidades curriculares relacionadas à manutenção de computadores, sistemas operacionais, infraestrutura e gerenciamento de redes de computadores, serviços de rede, *Web design*, desenho e animação.

Daniel Devegili

Tecnólogo em Redes de Computadores, Especialista em Administração de Redes Linux e Pós-Graduando em Redes e Segurança de Sistemas, Daniel Devegili atuou como analista de tecnologia da informação na área de gestão empresarial para empresas do ramo alimentício, desenvolvendo projetos de migração de sistemas, virtualização, políticas de segurança, políticas de *backup* e re-estrutura de sistemas, servidores e infraestrutura de rede.
Ainda no segmento corporativo, desenvolveu e aplicou um projeto de migração de sistema de automação de vendas, realizando apresentações e treinamentos para diferentes equipes de representantes e distribuidores comerciais, alterando de forma significativa, o conceito e prática de vendas.
Na área acadêmica, atualmente desenvolve materiais didáticos, atua como professor de cursos técnicos e aprendizagem industrial no SENAI/SC em Jaraguá do Sul, onde suas principais linhas de pesquisa se concentram em administração de sistemas operacionais e serviços de rede, virtualização de sistemas, automação de tarefas e segurança da informação, além de orientar trabalhos acadêmicos.

Unidade de estudo 1

Seções de estudo

Seção 1 - Introdução
Seção 2 - Modelo OSI e TCP/IP
Seção 3 - Protocolos
Seção 4 - Segurança

Arquitetura de Redes

SEÇÃO 1
Introdução

A velocidade com que as informações estão disponíveis hoje modifica a forma como as pessoas vivem. Isto faz com que muitas oportunidades estejam ao alcance de todos que podem ter acesso às tecnologias da informação. Os métodos de trabalho mudaram, as culturas são compartilhadas entre regiões, nações e continentes, as pessoas se aproximaram, e tudo isso é o reflexo da facilidade com que essas tecnologias são aprendidas e utilizadas.

Hoje, instantaneamente, as informações podem ser trocadas entre pessoas que estão a milhares de quilômetros umas das outras, a um custo muito reduzido. Isto significa segundo uma publicação da Agência Central de Inteligência dos EUA (CIA), pouco mais de 1,5 bilhão de usuários conectados à Internet, em todo o mundo (CENTRAL, 2010).

O funcionamento das redes de comunicação de dados depende de infraestrutura (fios, cabos, transmissores e receptores de radiofrequência, canaletas, dutos, equipamentos eletrônicos etc.) e dos protocolos de comunicação, muitos deles componentes de *softwares*, instalados em diversos tipos de equipamentos.

Todo este conjunto de tecnologias disponibiliza os mais diversos serviços e recursos a todos estes usuários.

Em uma sala de serviços disponibilizados pelas tecnologias da informação e comunicação existem muitos tipos de equipamentos e interfaces de conexão. Os *datacenters*, por exemplo, são salas que oferecem serviços de hospedagem de *sites* e sistemas *Web* para usuários ou empresas. São equipados com diversos servidores e utilizam tecnologias de rede de última geração.

Figura 1: Datacenter CERN
Fonte: Datacenter CERN (2011)

DICA

São muitos os termos e siglas utilizados para identificar os recursos em tecnologias da informação e comunicação. Lembre-se sempre de anotar os mais utilizados e de procurar entendê-los, pois isto irá ajudá-lo a compreender melhor o funcionamento dos serviços mais comuns.

Você certamente já ouviu alguém falar de *Skype*, *Web* ou *e-mail* e deve ser usuário de algum deles.

Esses são serviços muito comuns na internet. Serviços são recursos que os usuários conectados às redes podem usufruir. Se o seu computador estiver conectado à rede, poderá compartilhar informações com outros computadores, conversando com outros usuários por meio de mensagens de texto, acessando arquivos em outro computador ou até mesmo, permitindo que outro usuário da rede possa ouvir a mesma música que você está ouvindo em seu computador. Esses recursos estão disponíveis em *softwares* que podem ser instalados em seu computador.

Quando você acessa recursos da rede na empresa onde trabalha, normalmente você precisa se autenticar, ou seja, fornecer um nome de usuário e uma senha, que o identificam nos sistemas da empresa. Este recurso garante a segurança no acesso aos seus dados pessoais, na maioria dos casos fazem parte de serviços disponibilizados em uma intranet. A intranet é de acesso restrito, oferecido apenas a usuários de uma determinada organização.

O principal objetivo da Internet é agilizar a troca de informações entre as pessoas. Muitas ferramentas de comunicação são disponibilizadas gratuitamente, por meio de aplicativos, como por exemplo, o *Skype*. Esse é um *software* utilizado para comunicação entre usuários por meio de mensagens de texto, voz e vídeo. Além disso, esse *software* possui outros recursos.

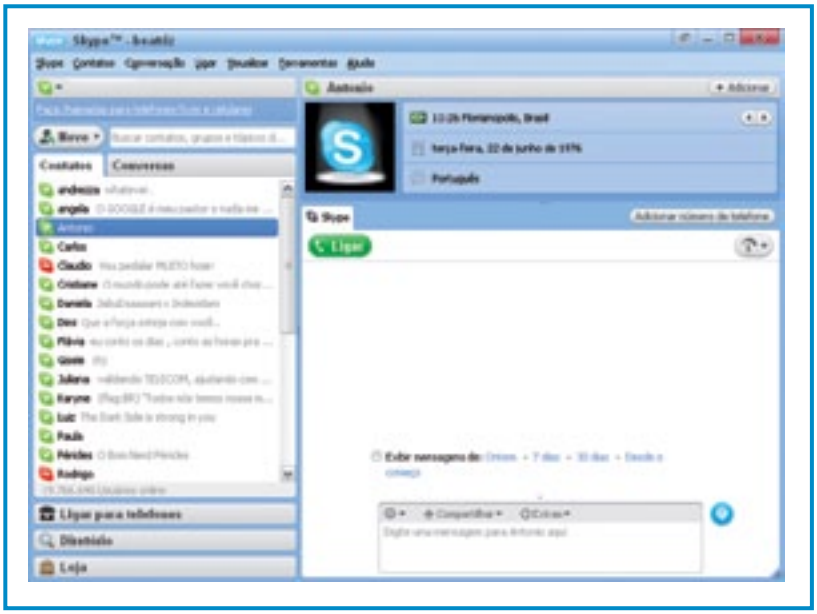


Figura 2: Tela principal da aplicação *Skype*

Fonte: Skype (2011)

Cada aplicação depende de diversos outros recursos. Desde o *hardware,* necessário, pois no caso de uma chamada de vídeo será utilizada uma *webcam*, até o *software* básico, como o sistema operacional.

DICA

Esteja atento aos requisitos de *hardware* e *software* necessários ao funcionamento da aplicação que você precisa.

Neste caso, observe que os demais componentes do computador influenciam na forma como as aplicações funcionam, incluindo critérios de desempenho, aparência e usabilidade. E a partir dessa introdução você já tem embasamento para compreender o próximo assunto. Preparado para esta nova etapa? Então vamos em frente.

SEÇÃO 2
Modelo OSI e TCP/IP

Os modelos, de uma forma geral, são utilizados para representar situações reais. Os modelos de redes apresentam a forma ideal de como uma comunicação entre dois *hosts* deve funcionar.

Qual modelo foi utilizado?

O modelo utilizado para fins de estudo é o OSI (*Open System Interconnection*). Ele foi utilizado como referência na construção de muitos protocolos conhecidos.

Figura 3: Modelo OSI

Este modelo é conhecido por possuir camadas independentes que possuem funções bem definidas e que implementam diversos recursos necessários às aplicações.

O conhecimento sobre os modelos de rede proporciona ao técnico a tomada de decisões na escolha das tecnologias a serem utilizadas na instalação da rede e auxilia na resolução de problemas.

As camadas físicas e enlace do modelo representam todos os dispositivos físicos utilizados na conexão do *host* à rede. Esta camada é implementada por:

- cabos;
- conectores;
- antenas;
- ondas eletromagnéticas;
- forças eletromagnéticas.

Dependendo do meio utilizado para a transmissão dos dados, devemos optar por um conjunto de protocolos que especificam as características de cada um destes componentes.

A partir da camada de rede, a informação pode trafegar por centenas de quilômetros no mesmo formato, sem que as instalações físicas e o cabeamento tenham que ser adaptados para isso. Significa que os equipamentos de rede que utilizam o protocolo IP, por exemplo, são compatíveis nessa camada, mas podem usar diferentes meios de transmissão neste caminho (sem-fio, fibra óptica, par trançado etc.).

> Um modelo que representa atualmente o funcionamento das redes de computadores é o TCP/IP.

Ele foi desenvolvido pelo Departamento de Defesa (DoD) dos Estados Unidos e visa aperfeiçoar as funções das camadas do modelo OSI para facilitar o desenvolvimento de novas tecnologias. As correspondências entre as camadas dos modelos OSI e TCP/IP e as diferenças entre os dois principais modelos você pode observar na figura a seguir.

Figura 4: Comparação entre OSI e TCP/IP – Cisco
Fonte: Wikipedia (2011)

Apesar dos nomes das camadas serem semelhantes, as diferenças são muitas. O modelo TCP/IP (figura 4) foi proposto pela Cisco, um dos maiores fabricantes de equipamentos para redes de dados. No entanto, existem pequenas variações nos protocolos que podem depender de soluções de cada fabricante.

A camada de aplicação do modelo TCP/IP é um exemplo. Ela agrupa as funções das três camadas superiores do modelo OSI:

- aplicação;
- apresentação;
- sessão.

Isto facilita o desenvolvimento dos protocolos para os serviços de rede (tais como: HTTP, FTP, DNS, entre outros).

DICA

No estudo desta unidade curricular você deverá encontrar informações sobre diversos outros protocolos que foram implementados a partir do modelo TCP/IP. Fique atento!

SEÇÃO 3
Protocolos

Um protocolo é uma definição formal de regras que devem ser seguidas pelas aplicações de comunicação de dados. Quando estabelecemos a comunicação com outro usuário da mesma aplicação, diversos protocolos são mobilizados ao longo de toda a rede para permitir a troca dos dados.

Cada protocolo define uma sequência de operações que estabelecem o formato dos dados a serem transmitidos, a origem e o destino das informações e o caminho que essas informações devem seguir para chegar ao seu destino.

Os protocolos abertos permitem que as aplicações possam ser compatíveis e que equipamentos diferentes, com sistemas operacionais diferentes, possam se comunicar.

Em muitas situações, você poderá optar por usar um protocolo ou outro para uma mesma aplicação, em camadas diferentes. Isto significa que essa escolha deve ser feita com base nos recursos que estes protocolos oferecem. Ou seja, para utilizar o *Skype,* você pode fazer a conexão com a Internet utilizando uma linha ADSL (banda larga) ou uma linha discada comum. Neste caso, a opção pela linha discada limitará o recurso de videoconferência que o *software* possui, pois a largura de banda suportada por esses protocolos é menor.

O *Internet Engineering Task Force* (IETF) organiza grupos de estudo sobre padrões para a Internet, definindo as características sobre os protocolos para que as empresas possam utilizar esses padrões ao desenvolver seu produto.
Outra organização importante é a *Institute of Electrical and Electronics Engineers* (IEEE), que organiza os padrões para o desenvolvimento das tecnologias relacionadas com eletricidade e eletrônica.

Para as redes de computadores, o IEEE é responsável por definir, principalmente, como os protocolos das camadas físicas e de enlace devem operar. Isto inclui muitos dos padrões utilizados para telecomunicações.

Conforme Sanches (2005)

A IEEE é um órgão sem fins lucrativos que conta com um grupo de mais de 380 mil membros, seu principal objetivo é desenvolver padrões técnicos com base em um consenso entre várias indústrias, e assim são criados os padrões que devem ser seguidos pelos fabricantes.

DICA

Acesse os *sites* destas organizações e conheça alguns dos documentos de especificação dos protocolos que serão estudados ao longo desta unidade curricular.

- http://www.ieee.org.br/
- http://www.ietf.org/

SEÇÃO 4
Segurança

Os conceitos relacionados à segurança em redes de computadores partem dos princípios básicos de segurança de qualquer tipo de sistema de informação. Os protocolos utilizados nas redes de dados devem considerar os seguintes fatores.

- **Confidencialidade:** quando os dados somente podem ser lidos por sistemas ou pessoas autorizadas.
- **Autenticidade:** quando é possível garantir que a fonte dos dados é autêntica.

- **Integridade:** quando é garantido que os dados não foram alterados sem autorização durante seu transporte ou manuseio.
- **Disponibilidade:** quando o serviço de entrega de dados está disponível na maior parte do tempo em que é utilizado.

Transferir arquivos entre computadores utilizando a rede é bastante útil em muitos momentos. Mas, é importante que essa transferência tenha uma autenticação, normalmente feita por meio de senhas criptografadas. Você pode, por exemplo, anexar seu arquivo em um *e-mail* ou acessar uma pasta compartilhada em um servidor de arquivos. De qualquer forma, é importante também utilizar o recurso de autenticação (usuário e senha) do serviço de rede para prevenir que usuários não autorizados tenham acesso a arquivos importantes.

Já a confidencialidade pode ser garantida com protocolos que possuem o recurso de criptografia. O uso de criptografia pelos protocolos de rede pode ser dividido em três grupos:

- sem uso de chaves;
- com chaves simétricas;
- com chaves assimétricas.

Existem indícios de que a criptografia foi inventada pelos egípcios há milhares de anos antes de Cristo.

Existem muitos registros históricos de que os povos da era antiga desenvolviam seu próprio código de escrita e evitavam divulgá-lo para que as mensagens não pudessem ser desvendadas por inimigos. Este é o princípio de funcionamento da criptografia. Uma mensagem que requer sigilo pode ser encriptada pelo remetente usando um algoritmo de criptografia e deve ser decriptada (ou decodificada) pelo destinatário ao receber a mensagem usando o mesmo algoritmo.

Para aumentar a segurança da transmissão de dados foram criados outros algoritmos de criptografia que requerem uma chave (ou senha). Esta chave é o código necessário para decifrar a mensagem. A criptografia sem o uso de chaves não é considerada segura, uma vez que conhecendo os diversos algoritmos de criptografia e comparando as mensagens é possível identificar o padrão de códigos.

O uso de chave simétrica é um tipo mais simples, onde todos os integrantes da comunicação devem ter conhecimento da chave de criptografia. Essa chave é conhecida como chave pública e a mensagem é encriptada antes de ser enviada. A chave deve ser de conhecimento do receptor para que o mesmo possa decodificar e ler as informações.

No entanto, se a chave for descoberta por alguém que não está autorizado a ler o conteúdo da mensagem, corre-se o risco de perder a confidencialidade das informações. Para isso, muitos protocolos implementam novos algoritmos de criptografia com uso de chaves assimétricas.

Chave assimétrica funciona com um par de chaves que é gerado:

- chave pública;
- chave privada.

A chave pública pode ser utilizada por qualquer *host* que precisa enviar informações. Essas informações serão encriptadas com a chave pública e enviadas, e somente com o uso da chave privada as informações poderão ser decriptadas e lidas, daí a importância de manter a chave privada no mais absoluto sigilo.

DICA

O tipo de algoritmo utilizado e a distribuição de chaves aos hosts são controlados pelos protocolos de rede que utilizam criptografia. Por isso, no momento de escolher a tecnologia a ser utilizada na implementação de uma rede esteja atento aos requisitos de segurança identificados a partir das necessidades de seu cliente.

Observe a seguir, um exemplo de comnicação de dados utilizando criptografia.

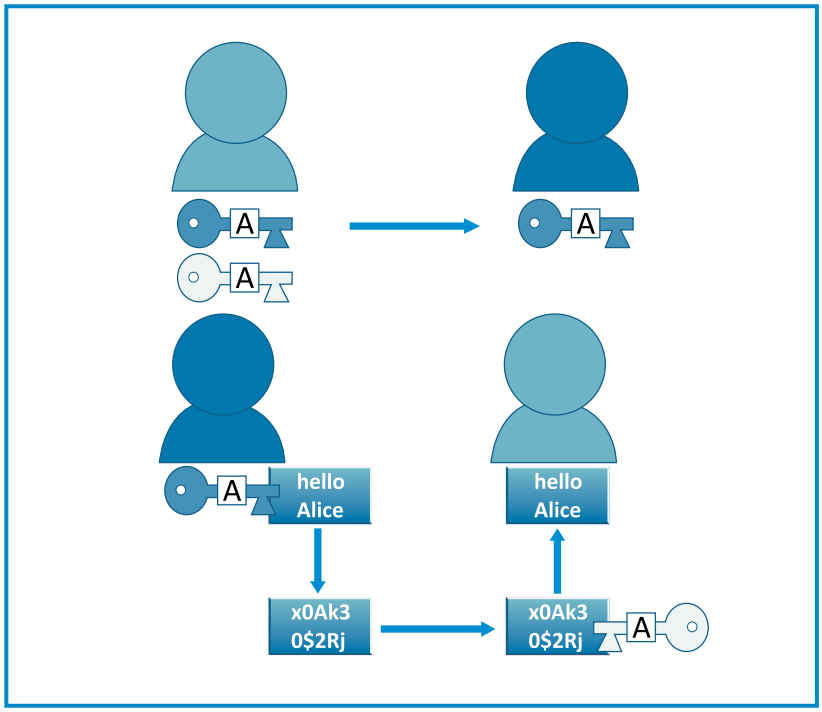


Figura 5: Criptografia assimétrica
Fonte: Sampaio (2004)

- 1° Cada *host* cria seu par de chaves.
- 2° O protocolo do *host* de Alice envia sua chave pública para Bruno.
- 3° O *host* de Bruno encripta a mensagem com a chave pública de Alice.
- 4° Alice recebe a informação criptografada e a decifra utilizando sua chave pública.

A redundância é uma técnica que tem por objetivo evitar que as possíveis falhas no equipamento danifiquem os dados ou que os torne inacessíveis ao usuário. Dentre as tecnologias disponíveis para a transmissão de dados, podemos utilizar caminhos redundantes (vários caminhos físicos aos mesmos destinos).

A técnica de redundância permite melhorar a disponibilidade dos serviços de rede.

Hardware redundante é muito útil em aplicações críticas. Ou seja, um servidor de rede que possui centenas de usuários conectados diariamente não pode se dar ao luxo de parar por algumas horas, ou mesmo minutos. Outros equipamentos de rede também possuem características de redundância. Mas é importante destacar que este recurso encarece significativamente o custo do sistema de *hardware*.

A partir de uma pequena introdução sobre o tema da unidade de estudos, você já pôde conhecer modelos de rede, seus protocolos e como deve ser a segurança em rede. Toda essa teoria alinhada a uma boa prática possibilitará a você uma inserção diferenciada no mercado de trabalho. Então aproveite todas as oportunidades de aprendizagem. Que tal começar agora a próxima etapa, que traz tecnologia de acesso a rede?

Unidade de estudo 2

Seções de estudo

Seção 1 - Camada física
Seção 2 - Camada de enlace
Seção 3 - Cabeamento

Tecnologia de Acesso à Redes

SEÇÃO 1
Camada física

A principal função da camada física é o tráfego de dados, ou seja, é nela que trafegam os *bits* propriamente ditos. Nessa camada nenhum tipo de controle é aplicado com relação à segurança e a integridade dos dados, pois essas são funções das camadas superiores. Essa camada é composta por cabeamento, conectores, placas e amplificadores/replicadores de sinal como o *hub,* por exemplo.

Para que estas informações trafeguem no meio físico alguns padrões precisam ser estabelecidos para o sucesso da comunicação. Na camada física esses padrões são concebidos em sua maioria pelos seguintes órgãos.

- *International Organization for Standardization* (ISO).
- *Institute of Electrical and Electronics Engineers* (IEEE).
- *American National Standards Institute* (ANSI).
- *International Telecommunication Union* (ITU).
- *Electronics Industry Alliance/Telecommunications Industry Association* (EIA/TIA).
- Autoridades de telecomunicações nacionais, como a *Federal Communication Commission* (FCC) nos EUA.

Os meios por onde as informações trafegam desde a origem até o destino pode ser de três formas:

- redes sem-fios;
- cobre;
- fibra.

Os conceitos mais técnicos serão abordados em seções seguintes. Primeiramente você precisa ter claro como se dá a comunicação nas três formas.

- Via rede sem-fio utiliza a atmosfera como meio de comunicação.
- O cabeamento de cobre como o próprio nome sugere é feito por meio de cabeamento onde seu núcleo é composto por cobre.
- Os meios baseados em fibras são tubos microscópios por onde trafega luz, a composição desses tubos normalmente e feita por plástico ou sílica.

> Independentemente do meio utilizado, rede sem-fio, cobre ou fibra ambos têm a mesma função, sinalizar/representar a linguagem binária (0 e 1)

O próximo assunto também é camada, porém, agora é camada de enlace. Acompanhe atentamente todo o conteúdo para que possa contribuir para sua vida profissional.

SEÇÃO 2
Camada de enlace

Assim como a camada física a camada de enlace também possui órgãos para o desenvolvimento de seus protocolos.

- *International Organization for Standardization* (ISO).
- *Institute of Electrical and Electronics Engineers* (IEEE).
- *American National Standards Institute* (ANSI).
- *International Telecommunication Union* (ITU).

As principais determinações da camada de enlace são.

- Quais são os nós envolvidos na comunicação.
- Quando a comunicação entre os nós individuais inicia e quando termina.
- Se ocorreram, ou não, erros durante a comunicação.
- Quais são os próximos nós que se comunicarão.

A seguir conheça as principais tecnologias utilizadas na camada de enlace.

ISDN

É um conjunto de protocolos que foram desenvolvidos por uma empresa da área telefônica homologada pela ITU (*Internacional Telecommunication Union*).

O protocolo ISDN está presente nas camadas física, enlace e rede do modelo OSI.

Conforme Diógenes (2004, p. 148)

> O ISDN é um serviço digital, projetado para rodar sobre a infraestrutura de rede pública existente (PSTN – *Public Switched Telephone Network*). A grande vantagem do ISDN é o suporte a dados, voz e vídeo, através de uma largura de banda bem maior que a oferecida pela telefonia analógica atual.

Neste sentido, as linhas de ISDN são compostas, basicamente, por dois canais de comunicação dispostos pela portadora. Os de 64 Kbps, mais conhecidos como canais B (*Bearer*), que são responsáveis pela transmissão de tráfego na rede, como dados, voz e vídeo. O outro é o canal de dados que pode ser de 16Kbps ou de 64Kbps, denominado de D (*Data*). Este tem a função de controlar o fluxo de sinalização e prover o controle de erros durante a comunicação.

Entendeu a diferença entre os dois canais?

Para que se possa implementar o ISDN foram definidos dois métodos de acesso. Um deles é o BRI (*Basic Rate Interface*) que faz o acesso básico e o segundo, o PRI (*Primary Rate Interface)*, provê o acesso primário. Vamos conhecer cada um deles?

BRI

É composto com 2B+D, ou seja, uma largura de banda de 128 Kbps, já que cada B equivale a 64Kbps.

> O BRI é o modelo mais utilizado no momento, pois, pode atingir desde pequenas e médias empresas até usuários residenciais.

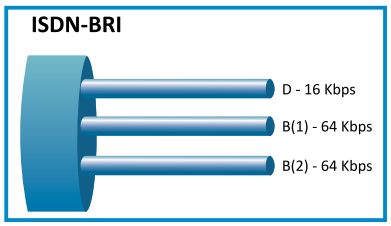


Figura 6: Exemplo de ISDN BRI
Fonte: Infowester ([200?a])

PRI

Pode ser chamado de T1 e E1. O T1 terá 23 canais do tipo B de 64Kbps, com um canal D. Este modelo é utilizado nos Estados Unidos, Canadá e Japão. Já o E1, possui 30 canais B de 64Kbps e um D, sendo utilizado no Brasil e na Europa.

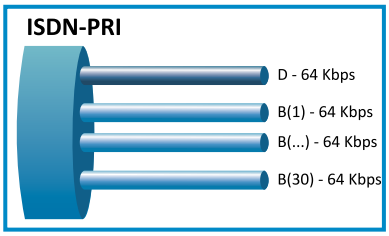


Figura 7: Exemplo de ISDN PRI
Fonte: Infowester ([200?b]).

Frame Relay

É uma tecnologia padronizada internacionalmente pela ITU-T (*International Telecommunication Union – Telecommunication Standards Section*) e pela ANSI (*American National Standards Institute*).

> Uma das principais características do *Frame Relay* é a inexistência de intermediários entre origem e destino, o que torna esta tecnologia uma solução de alto custo, podendo variar de acordo com a velocidade do link.

O caminho traçado entre origem e destino é feito logicamente e esse caminho denomina-se circuito virtual (VC-*Virtual Circuits*). Na grande maioria dos casos, uma rede *Frame Relay* é utilizada para interligar duas LANs (*Local Area Network*) que se encontram distantes umas das outras como, por exemplo, a interconexão entre uma filial no Brasil e sua matriz nos Estados Unidos.

Veja a seguir, um exemplo de uma comunicação em *Frame Relay*.

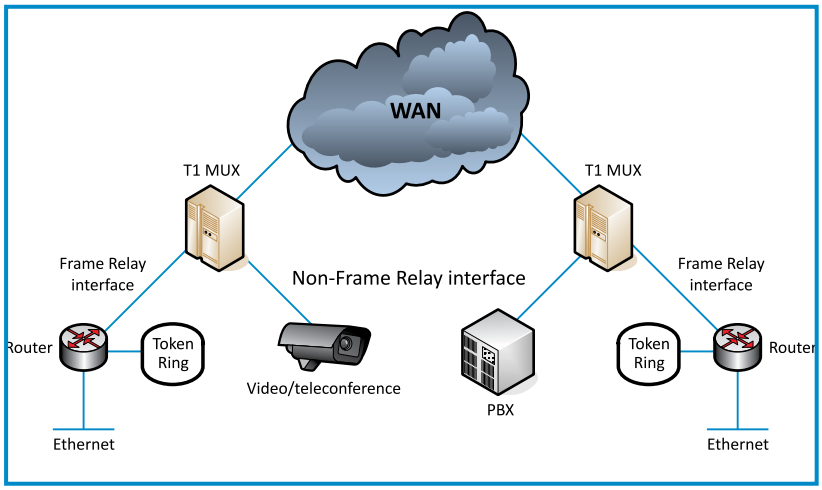


Figura 8: Exemplo de uma comunicação *Frame Relay*
Fonte: CISCO (2011).

Na figura anterior, a rede *Frame Relay* foi composta por uma série de elementos. Veja, a seguir, o que cada um deles representa.

- **Link de acesso:** é uma linha alugada de uma prestadora de serviços. Sua localização está entre o roteador (DTE) e o *Switch Frame Relay* (DCE).
- **Taxa de acesso:** é a velocidade definida, logicamente, de acordo com a necessidade de transferência de informações de cada cliente.
- ***Switch Frame Relay*:** é um computador de pacotes localizado dentro da empresa prestadora de serviços.

Está claro até agora? Podemos seguir com novas tecnologias? Vamos lá!

HDLC

É um protocolo proprietário da CISCO utilizado como padrão quando você não configura nada nas interfaces seriais do roteador. Porém, mesmo o HDLC sendo um protocolo aberto, roteadores de diferentes fabricantes podem não se comunicar de forma correta. Então, fique atento!

Isso acontece porque o HDLC é um protocolo que permite personalização de informações por parte do fabricante, tornando-o incompatível com outras plataformas.

Além das especificações físicas de cabos e conectores, temos que utilizar uma tecnologia de enlace. Isso significa escolher uma placa de rede adequada às necessidades. E, para isso, precisamos principalmente considerar a largura de banda e o meio físico a ser utilizado. Por exemplo, se dois equipamentos estiverem 500 metros distantes um do outro, pode ser necessário considerar o uso de fibra óptica ou radiofrequência. Nesse caso, a placa de rede a ser escolhida deve suportar o uso desse meio físico.

Você lembra da IEEE?

A IEEE define as características de como as placas de rede acessam cada tipo de meio físico. O uso mais comum é o da família de protocolos IEEE 802.3. Essa família de protocolos especifica o funcionamento das placas de rede para cabos metálicos e de fibra óptica.

O padrão *Ethernet* mais utilizado para conectar estações de trabalho às redes é o IEEE 802.3u. Mas é necessário considerar que deverá ser utilizado par trançado ou fibra óptica e que a distância máxima do cabo dependerá do meio físico utilizado. No caso do uso do par trançado, o limite é de 100 metros. Esse protocolo permite uma largura de banda máxima nominal de 100 Mbps. Observe que essa tecnologia é compatível com as anteriores, permitindo que a placa de rede também opere a 10 Mbps (802.3i). Esse padrão é conhecido também como *Fast Ethernet*.

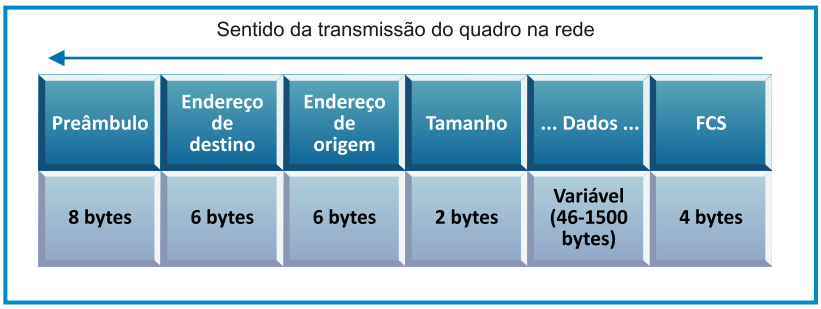
Ao definir o padrão a ser utilizado, observamos também que existem diferenças na escolha do tipo de cabo. No caso de par trançado, poderemos optar por diferentes implementações de cabeamento:

- 100BASET2;
- 100BASE-T4;
- 100BASE-TX, sendo este último o mais recente e utilizado com cabos de categoria 5 ou 5e.

DICA

Você poderá obter informações adicionais sobre os padrões IEEE 802 no site http://www.ieee802.org/. Vale a pena conferir!

Observe também que uma característica importante da camada de enlace é a definição do formato dos quadros. Um quadro Ethernet possui, entre outras informações, o endereço MAC do dispositivo de origem e do dispositivo de destino. Um exemplo de um quadro *Ethernet* 802.3 você verá a seguir. Acompanhe!



Quadro 1: Ethernet

As informações que são processadas pela camada de rede (pacote) são recebidas pelos protocolos da camada de enlace e colocadas no campo de dados do quadro. Esse processo é denominado de encapsulamento ou enquadramento. Além disso, a camada de enlace também é responsável por realizar a verificação de erros, utilizando para isso o campo "FCS *(Frame Check Sequence)*". Note que a verificação de erros pode indicar que o quadro foi corrompido durante a transmissão na rede. Por isso, ao receber um quadro, a interface de rede analisa esse campo antes de utilizar as informações do campo de dados.

Agora você é convidado a conhecer cabeamento, tema da próxima seção. Prepare-se para mais essa etapa.

SEÇÃO 3
Cabeamento

Você já ouviu falar nos meios físicos de comunicação, não é mesmo? Meios físicos de comunicação surgiram para um único fim, o do estabelecimento de comunicação entre dois ou mais equipamentos em uma rede. Existem alguns meios físicos para estabelecer essa comunicação como: cabos de par trançado, cabo coaxial, fibra óptica ou até mesmo pela rede elétrica, denominada PLC *(Power Line Communication)*.

Nessa etapa você conhecerá um pouco mais sobre cada um desses meios e dos protocolos das camadas físicas e de enlace do modelo OSI. Vamos lá?

Cabeamento par trançado

Atualmente esse é o meio físico mais utilizado para estabelecer a comunicação entre computadores. O nome "par trançado" deve-se ao fato de que os condutores são agrupados em pares e enrolados entre si. O enrolamento (trançado) dos pares é de suma importância para um bom desempenho da comunicação. Isso porque o trançado dos pares elimina a atenuação, evitando assim que um cabo interfira magneticamente no cabo ao lado. Vamos ao exemplo!

Figura 8: Exemplo de cabo par trançado
Fonte: Batista (2011)

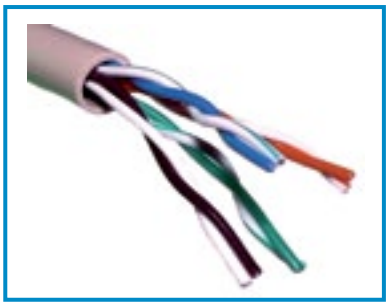


Figura 9: Exemplo de trançado dos pares
Fonte: Wikipédia (2010)

Existem três tipos de cabos de par trançado. Você sabe quais são eles?

1. UTP.
2. STP.
3. ScTP.

Unshielded Twisted Pair (UTP) ou par trançado sem blindagem são os mais utilizados em aplicações residenciais e empresariais. Isso porque esse tipo de cabo é de fácil implementação e permite uma transmissão de até 100 Mbps, podendo ter um lance máximo de até 100 metros para aplicação. Se houver necessidade de um maior lance de cabos é aconselhável o uso de fibra óptica.

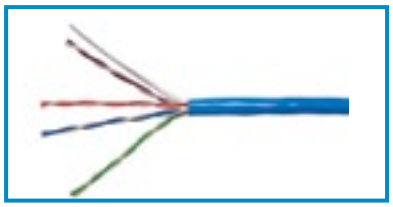


Figura 10: Exemplo de cabo trançado sem blindagem (UTP)
Fonte: Jobstown Networking (2010)

Screened Twisted Pair (ScTP) segue a mesma ideia dos cabos STP, porém, a malha metálica protege cada par separadamente, ao contrário do STP (onde uma única malha protege todos os quatro pares), e, com isso, conseguem ter uma melhor proteção contra interferências eletromagnéticas.

Figura 11: Exemplo de cabo trançado blindado (STP)
Fonte: Jobstown Networking (2010)

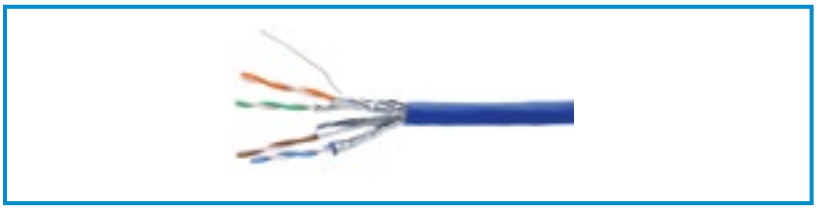


Figura 12: Exemplo cabo trançado blindado com malha metálica (ScTP)
Fonte: Cabo... (2010)

Cabeamento coaxial

Esse meio já foi muito utilizado em redes de computadores, mas atualmente caiu em desuso em função da criação de novas tecnologias, como o cabeamento de par trançado e a fibra ótica. Atualmente, você pode encontrar cabos coaxiais em TV a cabo, sistema de sonorização etc. A figura a seguir mostra as partes que compõe um cabo coaxial. Acompanhe com atenção!

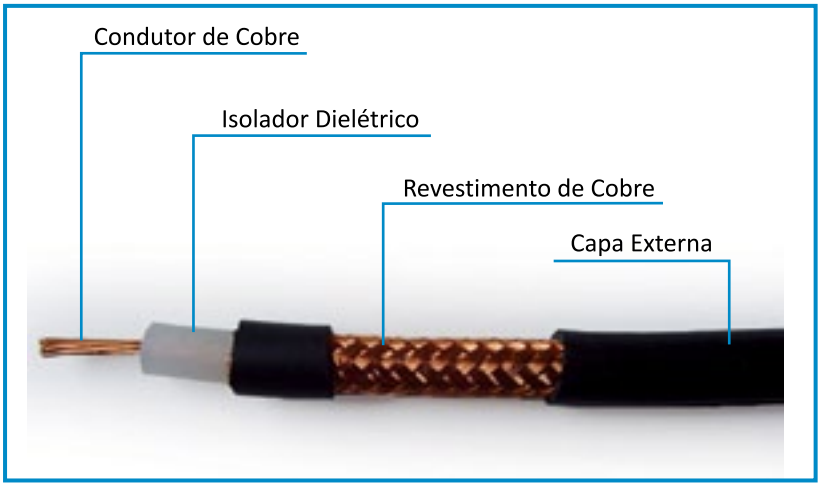


Figura 13: Partes de um cabo coaxial
Fonte: Wikipédia (2005)

Conheça agora as vantagens e desvantagens desse cabeamento.

Vantagens

- Baixo custo.
- Possui um bom sistema de isolamento contra interferências eletromagnéticas.

Desvantagens

- Problemas com mau contato.
- Difícil manipulação.

Cabeamento óptico

Diferentemente dos meios físicos citados anteriormente, o cabeamento óptico não utiliza o cobre para transmitir informações, mas sim a luz. Essa luz pode ser emitida tanto por um LED (*Light Emissor Diode*) como por um laser.

Esse é o mais utilizado, devido à sua potência e à sua menor largura espectral, onde o circuito da placa de rede é responsável por transformar o sinal elétrico em luz em uma das extremidades do cabo.

Essa luz desloca-se por dentro do núcleo, refletindo nas paredes internas. Esse deslocamento é feito normalmente à base de sílica ou plástico, até chegar ao receptor, onde faz o processo inverso, transformando o sinal de luz em pulsos elétricos e realizando, assim, a transferência de informações.

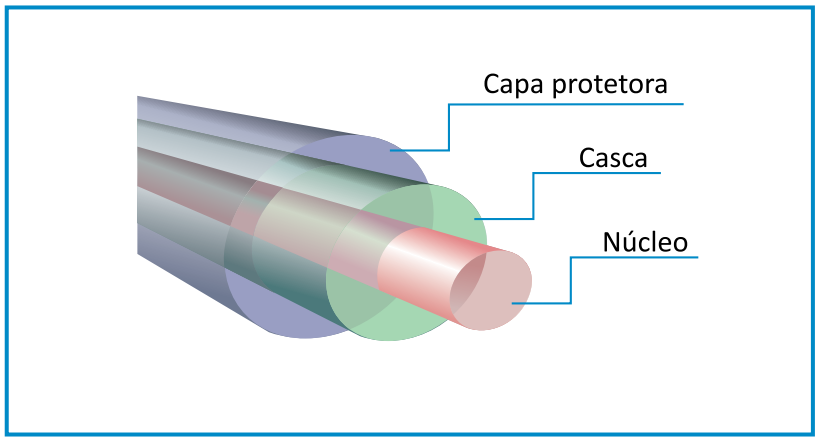


Figura 14: Cabeamento óptico

Ficou mais claro com os exemplos? Você deve ter muito desses cabos em sua casa. E agora, conhecerá seu funcionamento.

Vamos lá!

O cabeamento óptico possui um alto poder de taxa de transmissão de dados e, a cada dia que passa, novos estudos estão sendo feitos em cima dessa tecnologia. Em um futuro próximo, você poderá encontrar redes inteiras construídas com cabeamento óptico, pois muitos são os benefícios trazidos por esse meio. Além de suportar altas taxas de transmissão de dados, a fibra, por utilizar a luz como meio de transmissão, também é imune a interferências eletromagnéticas e automaticamente não gera interferência eletromagnética. Existem três tipos de fibra.

Você sabe quais são eles? Não? Então não se preocupe, é hora de conhecer.

- Multímodo degrau.
- Multímodo gradual.
- Monomodo.

Vamos descobrir o que são cada um deles? Em frente!

Fibras multímodo degrau são as mais utilizadas. Foram as primeiras a serem produzidas e sua principal característica é a reflexão total no núcleo da fibra. "[...] O termo degrau vem da existência de uma descontinuidade na mudança de índice de refração na fronteira entre o núcleo e a casca da fibra [...]" (SOARES; SOUZA FILHO; COLCHER, 1995, p. 99).

Já o termo multímodo refere-se ao fato de que vários feixes de luz podem ser projetados na fibra em diferentes ângulos. Confira o exemplo!

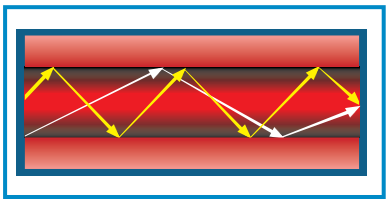


Figura 15: Fibra multímodo índice degrau

Já a fibra multímodo com índice gradual, ao contrário do índice degrau, possui um ângulo de reflexão mais suave. Com isso, à medida que a luz reflete no núcleo da fibra, gradativamente os ângulos atingirão o ângulo crítico. Isso diminuirá a refração, tendo uma maior velocidade na propagação, percorrendo distâncias maiores.

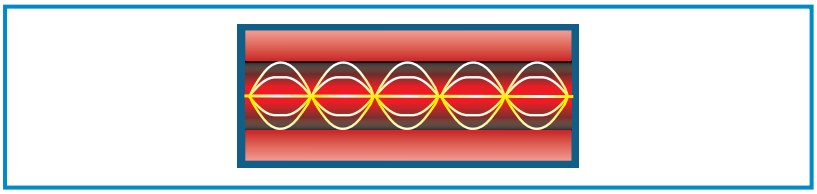


Figura 16: Fibra multímodo índice gradual

E a fibra monomodo, você sabe como funciona?

Como o próprio nome sugere nesse tipo de fibra a luz se propaga no meio de uma única forma, possibilitando que a fibra tenha um núcleo com um diâmetro bastante reduzido. Observe!

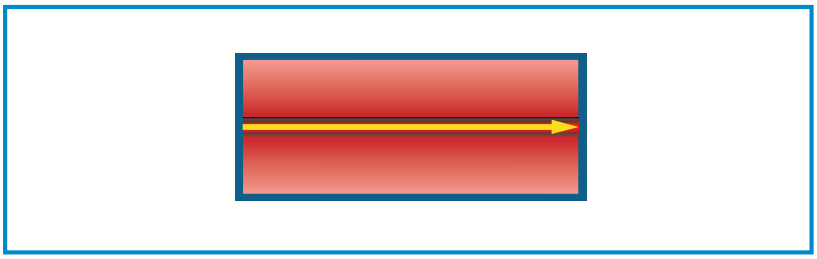


Figura 17: Exemplo de fibra monomodo

Cabeamento PLC

PLC (*Power Line Communication*) é uma nova tecnologia e, como o próprio diz, usa a maior rede existente para transmitir informações, a rede elétrica.

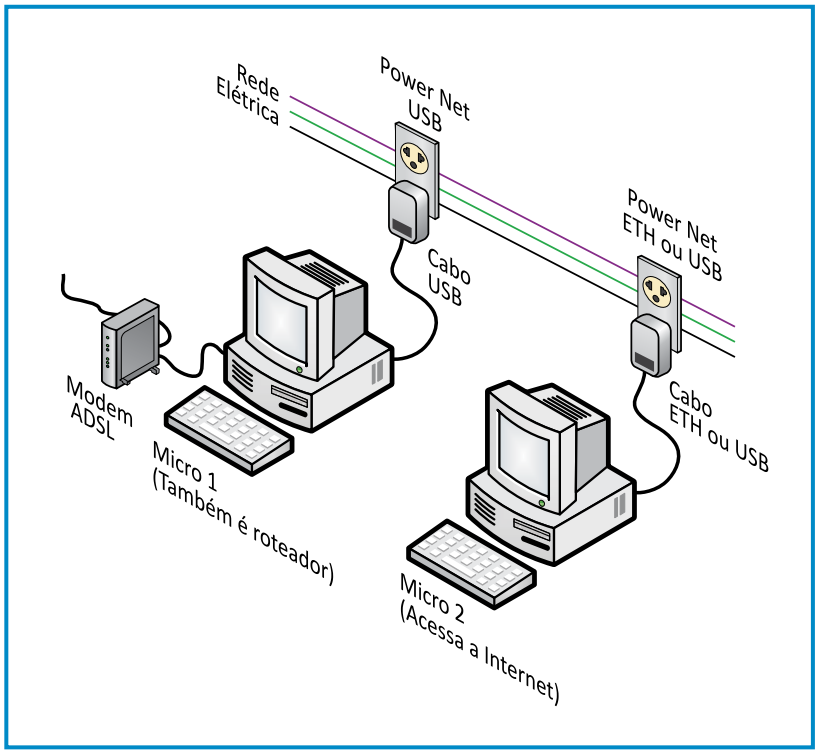


Figura 18: Exemplo de aplicação PLC

Os estudos sobre esta tecnologia são recentes, apesar de a energia elétrica ser usada desde 1920. Mas foi em 1991 que o Dr. Paul Brown, da *Norweb*, deu início a alguns testes com comunicação digital de alta velocidade através da rede elétrica da cidade de Manchester, na Inglaterra.

Vamos saber como essa tecnologia funciona?

Funcionamento

Existem dois tipos de redes PLC:

- Indoor;
- outdoor.

As redes *indoor* utilizam a rede elétrica interna de residências e apartamentos para a comunicação. Já as *outdoor* utilizam as rede públicas para esse mesmo fim.

As redes PLC trabalham com uma frequência em MHz na faixa de 1 a 30 MHz, sendo que a rede elétrica que utilizamos para ligar nossos equipamentos eletrônicos trabalha na faixa de frequência de 50 a 60 Hz. Com isso, as duas frequências podem existir em um mesmo meio, sendo que a ausência ou presença de uma não irá interferir na outra.

Quer saber as vantagens e desvantagens dessa rede? Veja!

Vantagens

A principal vantagem das redes PLC é a mobilidade, pois cada tomada existente em um ambiente pode se tornar uma ponte de rede. Outro fator positivo é sua velocidade, que pode chegar a 200 Mbps.

Desvantagens

A principal desvantagem das redes PLC é que cada ponto de energia se torna uma fonte de interferência. Assim, interferem principalmente no funcionamento de aparelhos que utilizam rádio frequência como: rádio, televisão, telefones sem-fio etc.

Nesta unidade de estudo você conheceu as camadas de transmissão de dados e quais os cabeamentos utilizados para redes de computadores. Este assunto é muito para o seu currículo profissional. Por isso, motivação, interesse e autonomia são fatores essenciais para que sua aprendizagem aconteça de forma efetiva e significativa.

Unidade de estudo 3

Seções de estudo

Seção 1 - Camada de rede
Seção 2 - Camada de transporte
Seção 3 - Endereçamento IP
Seção 4 - Configuração

Tecnologia para Internet e Transporte

SEÇÃO 1
Camada de rede

Por meio dos estudos sobre as camadas do modelo OSI e acompanhando o processo de encapsulamento dos dados, depois de receber os dados da camada de transporte o *host* encaminha-os ao protocolo da camada de rede, passando a ter a dominação de pacote. O processo de encapsulamento considera uma transmissão de dados de um *host* a outro.

No cabeçalho, o pacote recebe uma informação muito importante, o endereço lógico, proporcionando uma identificação única na rede e dessa forma permitindo a transferência dos dados do *host* de origem até o *host* de destino. Essa é uma das suas principais funções, o endereçamento de rede.

Para permitir a comunicação entre dois *hosts* na rede, ou seja, os pacotes de um *host* de origem serem entregues ao *host* de destino, a camada de rede fornece o mecanismo de endereçamento lógico. Cada pacote receberá um endereço lógico de origem e o endereço lógico de destino. Em uma rede IPv4, o endereço de origem/destino possui o tamanho de 32 *bits*, e uma vez atribuído a um dispositivo, ele passa a ser chamado de *host*.

Outra função muito importante da camada de rede é o roteamento entre os pacotes na rede. Nem sempre os *hosts* de origem estão conectados na mesma rede, podendo às vezes, o pacote viajar por meio de muitas redes.

Mover estes dados através de uma série de redes interconectadas é provavelmente uma das principais funções e o maior desafio da camada de rede.

Os dispositivos que conectam redes são chamados de roteadores, onde a principal função é selecionar o melhor caminho e direcionar os pacotes aos seus destinos corretos.

Cada vez que o pacote atravessa uma rede (ou passa por um roteador), diz-se que o pacote deu um salto. Conforme o pacote é movido entre as redes, o conteúdo do cabeçalho pode até ser alterado, mas os dados permanecerão intactos.

Durante o processo de encapsulamento, a camada 3 (OSI) recebe a PDU da camada 4 (OSI) (segmento), acrescenta um rótulo (cabeçalho) para criar a PDU da camada 3, que é chamada de pacote. Uma vez que o pacote foi formatado, ele está pronto para ser encapsulado pelas camadas mais baixas e enviado pelos meios físicos da rede.

O protocolo IP foi definido pela IETF, por meio do documento RFC 791 (em setembro de 1981), e foi a primeira versão utilizada globalmente nas redes de computadores.

A versão 6 do IP (IPv6), foi desenvolvida e está sendo implementada em algumas áreas, sendo adotado gradativamente e poderá no futuro substituir permanentemente a versão 4.

Segundo o documento RCF 791 "o Protocolo da Internet (IP), foi projetado para ser utilizado em sistemas interconectados de redes de computadores orientados a comutação de pacotes" (IETF, 2011). Ele foi elaborado como um protocolo com baixo *overhead*. Cada pacote é tratado como uma entidade independente, em relação aos demais. Com isso não há conexão ou circuitos lógicos. Como a camada de transporte é responsável pela conexão dos dados, o IP é um protocolo sem conexão, ou seja, nenhuma conexão é estabelecida antes do envio de dados. Por isso às vezes, o IP é referenciado como Datagrama IP.

O IP é considerado um protocolo não confiável, pois ele não possui a capacidade de gerenciar e recuperar pacotes perdidos durante a transmissão dos dados. Isso fica a cargo das camadas superiores.

O Protocolo IP implementa duas funções básicas:

- endereçamento;
- fragmentação.

Ele utiliza os endereços no cabeçalho para transmitir datagramas até o destino. A seleção dos caminhos para a transmissão é chamada de roteamento.

Cabeçalho do pacote IPv4

O cabeçalho IP possui uma parte fixa de 20 *bytes* e uma parte opcional de tamanho variável. O formato do cabeçalho você pode observar na figura a seguir.

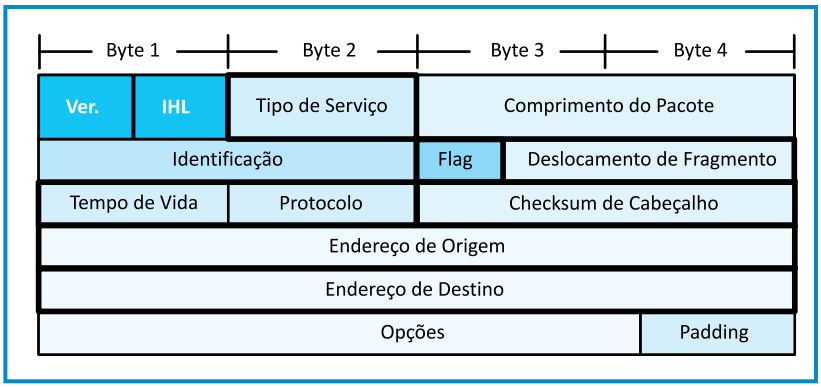


Figura 19: Cabeçalho IP

O campo versão especifica a versão do IP número 4 para IPv4 e 6 para IPv6.

O próximo campo (IHL) informa o tamanho do cabeçalho, em palavras de 32 *bits*. O valor mínimo é 5.

Já o campo Tipo de Serviço (TOS) é utilizado para mecanismos de QoS (Qualidade de Serviço), sendo possível assim identificar pacotes de dados por classes para um tratamento diferenciado. Como o pacote pode ter um tamanho variável (cabeçalho mais dados), o campo comprimento do pacote deverá especificar o tamanho desse pacote, em *bytes*.

Às vezes os dados podem não se "encaixar" dentro de um quadro da camada de enlace, então é de responsabilidade da camada de rede dividir ou fragmentar essa informação.

- O campo Identificação, identificará individualmente esses pacotes a fim de ser possível sua remontagem no *host* de destino.
- No campo *Flags*, um *bit* especial estará ligado nesse caso.

É possível também ligar um *bit* especial, DF, especificando assim que roteadores no meio do caminho não devem fragmentar a informação.

Tempo de Vida (TTL), é um valor binário de 8 *bits* que indica o tempo de vida do pacote, mas não é medido em escala de tempo e sim em saltos. Cada vez que o pacote passa por um roteador, esse campo é reduzido um valor, até chegar o valor zero, onde o pacote deverá ser descartado. No caso de ocorrer *loop* de roteamento, isso previne que a rede fique congestionada.

O campo Protocolo informa a que processo de transporte o pacote deve ser entregue. É a ligação com a camada superior. Alguns exemplos são:

- 01 para ICMP;
- 06 para TCP;
- 17 para UDP.

O *Checksum* do cabeçalho apenas confere o cabeçalho. A soma de verificação é útil para a detecção de erros.

Por fim, os campos Endereços de Origem e Endereço de Destino contêm um valor binário de 32 *bits* que representam o endereço do *host* de origem e destino respectivamente. Ainda nesta unidade de estudo você estudará o formato e a organização do endereçamento IPv4. A seguir você conhecerá camada de transporte. Vamos ver juntos esse assunto? Lembre-se, sua dedicação é fundamental para o sucesso da aprendizagem.

SEÇÃO 2
Camada de transporte

A camada de transporte é de vital importância para a comunicação entre aplicações pela rede. Ela será responsável pela segmentação, ou seja, pela divisão dos dados da camada de aplicação em pedaços menores, e também pelo empacotamento dessa informação, agregando um rótulo aos dados, que a partir desse momento é chamado de segmentos.

É importante lembrar o nome da Unidade de Dados de Protocolo (PDU – *Protocol Data Unit*) de cada camada em estudo, nesse caso a PDU da camada 4 é chamada de segmentos.

A camada de transporte proporciona a segmentação dos dados no *host* de origem, ou seja, vai dividir em pedaços pequenos o fluxo de dados da aplicação e adicionar um cabeçalho, que consiste numa sequência de *bits* que serão vistos como campos, a fim de controlar o envio e recebimento desses dados. No *host* de destino, a camada de transporte irá reagrupar os segmentos antes de repassar para a camada de aplicação.

Uma vez que os dados foram segmentados, ou seja, divididos em pequenos pedaços, será mais fácil o transporte da informação, pois caso ocorrer perda de dados durante a transmissão, apenas os segmentos que não chegaram serão retransmitidos.

Além de facilitar o transporte da informação, com o que mais a segmentação pode contribuir?

Além de facilitar o transporte da informação, com a segmentação é possível intercalar os segmentos de diferentes aplicações, permitindo assim que o tráfego de diferentes aplicativos atravesse à rede, nos dando a impressão de várias conversas simultâneas.

> Essa técnica de intercalar os pacotes é chamada de multiplexação, ou conversas simultâneas.

Protocolos da camada de transporte podem ser orientados à conexão (com confiabilidade), ou sem serviço de conexão (não confiável).

> Segundo Tanebaum (2003, p. 389) "O principal objetivo da camada de transporte é oferecer um serviço confiável, eficiente e econômico a seus usuários que, em geral, são processos presentes na camada de aplicação".

Confiabilidade e conexão

Para uma entrega confiável, um protocolo orientado a conexão deve primeiramente estabelecer uma sessão entre as aplicações dos *hosts*. Você verá adiante, que essa sessão é chamada de *handshake* de três vias.

Ao estabelecer uma sessão, o aplicativo estará pronto para receber os dados. Mas devido a alguns motivos, como por exemplo, ruídos na camada física ou congestionamento, poderá haver perda de dados. Um protocolo da camada de transporte confiável deve assegurar a entrega confiável, através de mecanismos presentes no cabeçalho do segmento como, número de sequência e número de reconhecimento e detectar se um segmento não foi entregue ao seu destino. Nesse caso, o *host* de origem deverá retransmitir o segmento e aguardar a confirmação de recebimento.

Em redes congestionadas, outro grande problema é a chegada dos segmentos fora de ordem. Como os pacotes podem pegar caminhos alternativos durante sua viagem da origem ao destino, uma informação que foi enviada em um segundo, poderá chegar antes do que a informação que foi enviada por primeiro. Nesse caso, durante o reagrupamento dos segmentos, a camada de transporte com protocolo orientado a conexão deverá recolocar em ordem correta.

E como isso acontece?

Para isso, o *host* de destino utiliza um *buffer* ou uma memória de fila de segmentos, que garantirá a sequência correta dos dados para as camadas superiores.

Como você pode notar um protocolo orientado a conexão também possui desvantagem, e nesse caso é justamente a sobrecarga adicional, ou *overhead*, que o protocolo adiciona a rede. Como se faz necessário que o *host* que está enviando tenha certeza que os segmentos chegaram ao destino, ele precisa parar por um instante a transmissão de dados e aguardar um segmento de reconhecimento chegar, confirmando que os dados enviados chegaram ao seu destino.

E no caso da informação não chegar?

Caso não chegar, após um tempo determinado os dados serão reenviados. Tudo isso gera uma grande sobrecarga ao protocolo, e algumas aplicações podem não tolerar essa "espera", tais como: programas de fluxo de *streaming*, voz sobre IP e multimídia.

Nesses casos, haveria algum problema?

Nesses casos, não haveria tanto problema se alguns segmentos fossem perdidos, pois a informação ainda seria compreendida, diferente, por exemplo, de uma transferência de arquivo, que no caso de perder um segmento, o arquivo final estaria corrompido ao ser remontado.

Está compreendendo o assunto? Que tal compartilhar ideias com o professor e colegas? Assim você tem a oportunidade de tirar suas dúvidas.

Endereçamento de portas

A fim de permitir que aplicações utilizem o meio de rede simultaneamente, utiliza-se a técnica de multiplexação, como você viu anteriormente. Para identificar esses fluxos de informações às corretas aplicações, utilizam-se endereços de portas rotuladas no cabeçalho de cada segmento. O campo portas então é utilizado para identificar as diferentes aplicações e repassar o fluxo de dados para as aplicações apropriadas, permitindo assim identificar a aplicação a qual pertence o fluxo de dados.

Cada aplicação terá um número de porta associado.

- No *host* de origem, será chamado de porta de origem e o número da porta será gerado aleatoriamente, e utilizado desde que nenhuma outra aplicação já esteja utilizando o mesmo número de porta.
- O *host* de destino deverá ter também uma porta de destino associado a uma aplicação ou serviço, já previamente aberta.

Por exemplo, imagine a solicitação de uma página *Web*, através do protocolo HTTP. O cliente utilizando a aplicação de navegador *Web* solicita uma página ao servidor *Web* 192.168.1.1, que possui uma porta associada ao serviço (porta 80), que será utilizada como porta de destino. O *host* que está solicitando, que possui o IP 192.168.1.20 irá selecionar dinamicamente uma porta, por exemplo, 49155, e utilizará como porta de origem. Ao retornar a informação, a combinação IP-porta de origem/destino será trocado, sendo o *socket* 192.168.1.1 / 80 como IP/porta de origem e 192.168.1.20/49155 como IP/porta de destino.

O IANA (*Internet Assigned Numbers Authority*), que é responsável pela designação de vários padrões de endereçamento, também é responsável pela designação do número de porta.

Conheça a seguir os três tipos utilizados.

- **Portas conhecidas** (0 a 1023) – são números reservados para aplicações e serviços, como o servidor *Web* (HTTP) e servidor de *email* (POP3/SMTP).
- **Portas Registradas** (1024 a 49151) – são número de portas designados para processos ou aplicações de usuários. Quando não utilizadas por alguma aplicação, podem ser utilizadas também como portas dinâmicas.
- **Portas Dinâmicas** (49152 a 65535) – geralmente designadas dinamicamente a aplicações de cliente quando se inicia uma conexão.

Por meio da definição e padronização de portas, não é necessário, por exemplo, colocar o número da porta do serviço HTTP (porta 80), no final de uma URL no navegador *Web*.

Protocolos TCP e UDP

Os principais protocolos da camada de transporte são o Protocolo TCP e o Protocolo UDP.

Consta na RFC 793 (IETF) que o TCP é um protocolo orientado à conexão, utilizado como um protocolo de entrega altamente confiável entre *hosts* fim-a-fim.

O TCP provê uma comunicação confiável entre os processos da aplicação do *host* de origem com a aplicação do *host* de destino, em computadores conectados às distintas redes de comunicações.

Para essa entrega confiável e segura, o TCP possui algumas funções adicionais:

- confiabilidade;
- entrega ordenada;
- controle de fluxo.

Ao estudar os campos do cabeçalho TCP, você verá onde cada função será executada.

A confiabilidade é garantida pelo número de sequência que cada segmento recebe no momento da segmentação. Depois de estabelecida uma conexão entre os dois *hosts*, o emissor enviará os segmentos e deverá aguardar a confirmação de recebimento. Somente quando ele receber a confirmação poderá enviar mais dados.

O número de sequência é o número relativo de *bytes* que foram transmitidos nessa sessão mais 1 (que é o número do primeiro *byte* de dado no segmento corrente). O TCP usa o número de confirmação em segmentos enviados de volta à origem para indicar o próximo *byte* que o receptor espera receber nessa sessão. Isto é chamado de confirmação esperada.

O *host* que enviou os dados ficará aguardando a confirmação, através do campo número de reconhecimento, que indicará o próximo segmento a ser enviado.

Lembre-se, caso ocorrer à perda de um segmento, o número de reconhecimento irá conter o número do segmento que está faltando.

Como são estabelecidas as conexões TCP?

Confira este assunto a seguir.

Estabelecimento de conexões TCP

Antes de dois *hosts* trocarem informações pelo TCP, é necessário estabelecer uma conexão entre os dois computadores. Depois que este processo inicial, chamado *handshake* triplo ou aperto de mão, for concluído com sucesso, um canal virtual é criado entre os dois *hosts*, e a troca de informações será possível. Cada conexão representa dois fluxos de comunicação, ou sessões, pois a troca de informações ocorrerá em duas vias (*download*/*upload*).

O *handshake* triplo estabelece que o dispositivo remoto esteja presente durante a comunicação, verifica que o serviço remoto está ativo e aceitando solicitações.

Nas conexões TCP, o *host* que inicia a conexão TCP será chamado de cliente. Os três passos para iniciar a conexão são.

1. O cliente envia um segmento ao *host* que deseja se conectar, contendo um valor sequencial inicial.
2. O servidor responde com um segmento contendo um valor de confirmação igual ao recebido mais 1, mais o seu próprio valor sequencial inicial, pois o servidor também deverá abrir uma conexão com o *host* que solicitou uma conexão.
3. O cliente que iniciou a conexão recebe a confirmação do servidor, juntamente com o pedido de conexão, e responde com o valor sequencial recebido mais um. Isso completa o processo de estabelecimento da conexão.

Para o controle de quando uma conexão deverá ser iniciada, serão utilizados *bits* ou *flags* adicionais no cabeçalho TCP. Você verá adiante, o significado de cada *bit* do campo *flags*.

O cabeçalho TCP

O cabeçalho TCP possui um tamanho fixo de 20 *bytes*, conforme figura a seguir, mas pode aumentar caso houver opções adicionais (cada campo opções deve ter 32 *bits* de tamanho). Pode ocorrer de trafegarem segmentos sem quaisquer dados válidos, que neste caso serão utilizados como confirmações de recebimento ou mensagens de controle.

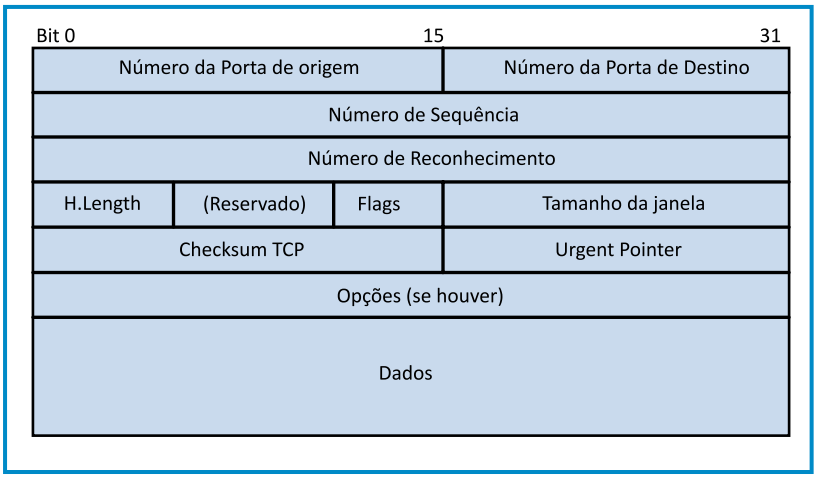


Figura 20: Cabeçalho TCP

Analisando o cabeçalho TCP, os dois primeiros campos são Porta de Origem e Porta de Destino. Como você viu anteriormente nessa seção, as portas são definidas pelo IANA. O conjunto endereço lógico (Endereço IP) mais número da porta forma um valor de 48 *bits,* conhecido como *socket*, que identifica um processo sendo executado no dispositivo de rede.

Como o cabeçalho TCP pode conter um tamanho variável, ou seja, pode-se anexar opções ao cabeçalho, o campo Tamanho do Cabeçalho deverá informar o tamanho de todo o cabeçalho IP. Caso não contenha opções, o valor será sempre o tamanho fixo, que é 20 *bytes*.

Em seguida, existe um campo reservado de 6 *bits* que não é utilizado, e reservado para provável utilização futura. O campo *Flags* merece uma atenção em especial, e é composto por 6 *bits* que representam as funções:

URG, ACK, PSH, RST, SYN e FIN

Quando o valor 1 é atribuído ao *bit* URG (Ponteiro Urgente), permite que o transmissor envie um sinal ao receptor sem envolver o serviço TCP no motivo da interrupção. O *bit* ACK (*Acknowledgement*) indica que o valor do campo Número de Conhecimento é válido, ou seja, deve-se enviar o próximo segmento conforme está solicitado no campo do reconhecimento.

O *bit* PSH (*Push*) definido para o valor 1, o receptor deverá entregar os dados diretamente à camada de aplicação, sem armazená-lo em *buffer*, evitando assim atrasos. Já o *bit* RST (*Reset*), é utilizado para reinicializar uma conexão, que pode ter ficado confusa devido a falhas em alguns dos *hosts*.

Quando o *bit* SYN estiver definido com o valor 1, significa que uma nova conexão deve ser iniciada, ou seja, no processo inicial de *handshake*, o envio da solicitação de conexão terá sempre o *bit* SYN definido como um. Visto que é uma comunicação bi-direcional, a resposta além de o *bit* SYN estar ativo, uma nova conversa agora do *host* que recebeu anteriormente o pedido deverá ser aberta com o *host* que originou o pedido da conexão. Dessa forma, a resposta também será um pedido de conexão, com o campo SYN definido com o valor 1. Por último para finalizar a conexão TCP, o *bit* FIN será utilizado.

Outra função muito importante do TCP é o controle de fluxo. Através de janelas deslizantes, o controle de fluxo ajuda na confiabilidade de transmissões TCP pelo ajuste da taxa de fluxo efetiva entre os dois serviços dos *hosts* que estão se comunicando. Para isso, o campo Tamanho da Janela irá especificar a quantidade de dados que podem ser transmitidos antes de receber uma solicitação de confirmação do *host* remoto para quem está enviando.

O tamanho da janela inicial é determinado durante a inicialização da sessão, pelo *handshake* triplo.

O protocolo UDP é um protocolo simples, não é orientado à conexão e possui baixo *overhead*. Como não é orientando à conexão, ele não fornece mecanismos de retransmissão, sequenciamento e controle de fluxos sofisticados. Isso não significa que todos esses controles estarão ausentes durante a transferência dos dados, mas será necessário ser implementado em outro lugar, como na própria aplicação.

Diferente de várias aplicações que não podem tolerar falhas ou perdas de dados, existe algumas aplicações que podem lidar com algumas perdas de segmentos, como por exemplo, jogos *on-line*, *streaming* de vídeo ou voz sobre IP. No caso da VoIP, um dos requisitos é ter uma baixa latência na rede, ou seja, o protocolo de transporte não deve adicionar uma sobrecarga muito alta. Para esse caso, não é viável a utilização do TCP, e sim do UDP, mesmo abrindo mão do controle de erros.

O cabeçalho UDP possui apenas 8 *bytes*, como visto na figura anterior. As duas portas servem para identificar as aplicações nos *hosts* distintos. Quando um datagrama UDP chega, sua carga útil é entregue ao processo associado à porta de destino.

Vale ressaltar que o UDP não realiza controle de fluxo, controle de erros ou retransmissão após receber um segmento incorreto.

Uma área na qual o UDP é utilizado é na situação cliente/servidor. Neste caso, o cliente envia uma pequena solicitação ao servidor e espera uma pequena resposta de volta. Um exemplo de protocolo utilizando o UDP como transferência de dados nesse modelo cliente/servidor é o *Trivial File Transfer Protocol* (TFTP), assim como o DNS também utiliza o UDP para pesquisas e resolução de nomes de domínio. Puxa! Quanta informação sobre camada de transporte não é mesmo? Mas não se preocupe. Dúvidas? Retorne ao conteúdo. Reflexões? Discuta com o professor e colegas. Na sequência você tem endereçamento. Siga em frente.

SEÇÃO 3
Endereçamento IP

O Protocolo IP possui um endereçamento hierárquico, que identifica cada IP de maneira única em toda a rede. O IPv4 é formado por duas partes:

1. identifica a rede;
2. identifica um *host* nessa rede.

Para melhor entender um endereço IPv4, a sua representação foi dividida em 4 grupos com 8 *bits* cada (octeto). Cada octeto é convertido em seu valor decimal, sendo eles separados por pontos. Exemplo: 192.168.1.50

O tamanho da porção de rede é designado pela máscara de rede, que tem por objetivo definir o tamanho de uma rede (tamanho da porção de *hosts*). A máscara padrão do Endereço IP 192.168.1.50 é representada em formato decimal pontuada: 255.255.255.0 ou simplesmente /24 no formato de prefixo.

Formato de prefixo significa a quantidade de *bits* 1 (uns) presentes na máscara de rede, convertendo o valor de decimal para binário.

Neste exemplo o primeiro octeto é 255 em decimal, que em binário será representado por 11111111. Quando o *bit* na máscara de rede tiver o valor de 1 significa que aquela posição do endereço IP fará parte da porção de rede e quando o valor for 0 significa que fará parte da porção de *hosts*. Você entenderá melhor sobre como definir e planejar o endereçamento de redes a seguir.

Nos sistemas de informação, todas as informações são armazenadas, transmitidas e organizadas com base no sistema binário. No entanto, os usuários precisam dessas informações de modo legível e utilizando linguagens naturais.

Para determinar e entender como funciona o sistema de endereçamento nas redes de computadores é importante que você conheça um pouco mais o sistema binário.

Como você já estudou, para endereçar um computador em uma rede, o protocolo IP (versão 4) utiliza 32 *bits*. Cada *host* de uma rede deve possuir um endereço único. Portanto, parte do endereço IP corresponde ao endereço da rede a qual ele pertence, e a outra parte, corresponde ao endereço do próprio *host* nessa rede. No entanto, podemos criar redes ou sub-redes diferentes, distinguindo os endereços modificando a máscara de rede.

Quando especificamos uma máscara, estamos definindo a quantidade de *bits* do endereço IP que será utilizada para endereçar a rede e a quantidade de *bits* que deve ser usada para endereçar os *hosts* dessa rede.

Planejamento de endereços

O que você deve levar em consideração ao instalar uma rede de computadores?

Quando planejamos a instalação de uma rede de computadores devemos levar diversos aspectos em consideração. Em relação ao endereçamento, é importante considerar o número de equipamentos que a rede deve suportar. Neste caso, dependendo da configuração dos equipamentos da rede, considere também o número de redes você deverá utilizar. Entre as diversas combinações, vamos apresentar algumas delas.

Ao utilizar a máscara padrão, significa que estamos adotando a máscara definida de acordo com as classes de endereços IP.

As classes utilizadas na definição de endereços IP para *hosts* são A, B e C. As classes D e E são utilizadas com outras finalidades.

Vamos analisar as classes existentes e a utilização dos *bits* do endereço para cada uma delas.

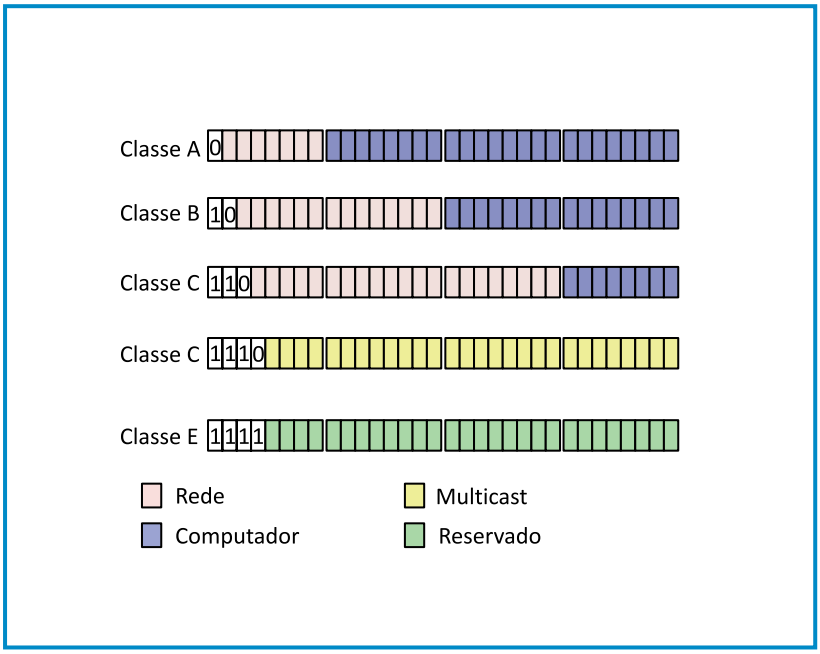


Figura 21: Classes de endereços IP

No exemplo a seguir, utilizamos o endereço 192.168.1.50 para endereçar um *host* da rede 192.168.1.0. A máscara padrão foi aplicada: 255.255.255.0. Esta definição permite o uso de 254 *hosts* nessa rede. Observe que, utilizando um endereço de classe A, você poderá possuir um número de equipamentos muito maior em sua rede.

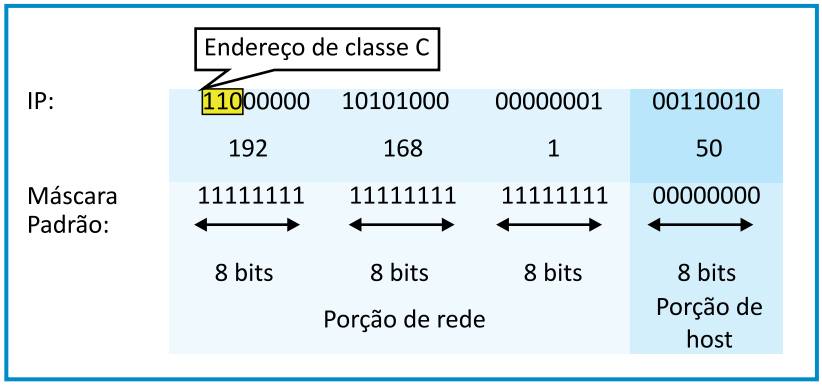


Figura 22: Exemplo de endereço IP e máscara de rede

A RFC 1918 (IETF) determina que somente alguns endereços de classe A, B e C podem ser utilizados para redes privadas, ou seja, são exclusivos para os equipamentos que compartilham o mesmo endereço IP para acessar a Internet. Hoje, seria impossível que cada equipamento conectado à Internet possuísse um endereço IP exclusivo. Pois os 32 *bits* não são suficientes. Para resolver esta situação, uma rede empresarial utiliza um endereço IP válido para a Internet (denominado também como endereço IP público) e compartilha esta conexão entre todos os demais *host*s de sua rede. Escolas, empresas, instituições de ensino e órgãos governamentais utilizam esta estratégia para acessar a Internet. No quadro a seguir você pode identificar a faixa de endereços IP privados definidos pela IETF. Todos os demais são considerados endereços IP públicos.

Início	Fim	Prefixo
10 .0 .0 .0	10 .255.255.255	(10/8)
172.16 .0 .0	172.31 .255.255	(172.16/12)
192.168.0 .0	192.168.255.255	(192.168/16)

Quadro 3: Endereços IP públicos

Além destas definições, você poderá criar sub-redes, pois nem sempre sua rede privada irá se adequar a uma destas três classes. Em uma situação em que você precise criar 10 sub-redes, e que cada uma delas possa comportar, no mínimo, 1000 *hosts*.

Como poderíamos resolver este problema?

Acompanhe o tópico a seguir para obter a resposta.

Determinação dos Endereços

No caso a seguir, vamos considerar que você deverá usar endereços de classe A. Desta forma, sabemos que o número 1000 precisa ser representado com, no mínimo, 10 *bits*. Isto significa que devemos emprestar dois *bits* do octeto vizinho. Emprestando esses dois *bits*, ainda nos restam 14 *bits* a serem utilizados para endereçar diversas outras sub-redes.

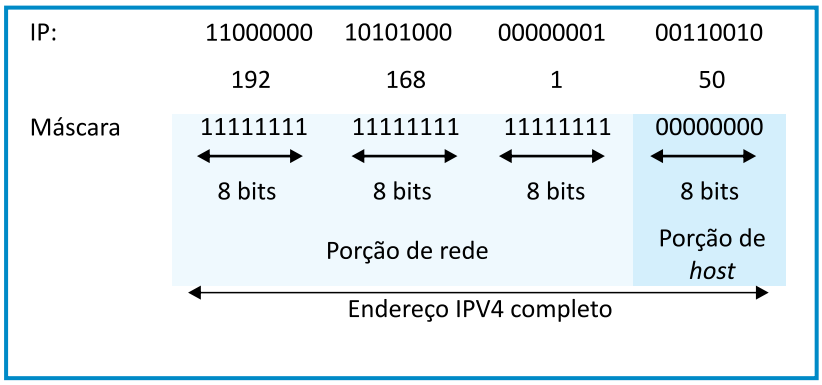


Figura 23: Exemplo de sub-rede

Podemos concluir que a máscara a ser aplicada a esta situação deverá ser 255.255.252.0 e que um *host* qualquer da sub-rede 10.0.0.4.0, neste exemplo, poderá ser endereçado com o endereço 10.0.4.51.

A melhor forma de descobrir os valores de máscara e endereço IP é convertê-los em binário. Pois assim, você poderá observar melhor o uso de cada *bit* do endereço.

Podemos aplicar máscaras de sub-rede a qualquer endereço IP, sejam eles públicos ou privados, e de qualquer classe. A necessidade de definir a quantidade de *host*s e sub-redes depende da infraestrutura física disponível, conforme já mencionamos. Lembre-se também que todo endereço IP precisa ser acompanhado de uma máscara. Sem isso, é impossível determinar qual é a parte do endereço que representa a rede, a sub-rede e os *host*s.

Ainda assim, poderíamos ter escolhido um endereço de classe B para resolver este caso, sem a necessidade de aplicar uma máscara de sub-rede. No entanto, precisamos considerar que ao escolher utilizar a máscara padrão da classe, estamos desperdiçando um número considerável de endereços de *host* ou sub-redes. No futuro, talvez seja necessário rever o esquema de endereçamento de sua rede devido às mudanças e ao aumento do número de *hosts*. Como estratégia para a definição de sub-redes, vamos analisar mais um exemplo, considerando um método muito utilizado. O método consiste de três etapas.

1. Análise do endereço e sua máscara:
   Por exemplo, IP: 10.0.3.1 e máscara: 255.255.255.248
   Se o endereço é de classe A, isto significa que apenas o primeiro octeto indica o endereço da rede (10).
   Verificando os *bits* 1 contidos na máscara, supomos que existem apenas três *bits* (no último octeto) para serem utilizados por endereços de *hosts*.

2. Verificação do número de *hosts* e redes.
   Para verificar o número de combinações possíveis na base binária (2), faz-se: 2^3, pois são 3 *bits* para *hosts*, isto perfaz um total de 8 combinações, sendo elas:
   ...000 - não pode ser utilizado para endereçar *hosts*, pois representa o endereço desta sub-rede (10.0.3.0)
   ...001
   ...010
   ...011
   ...100
   ...101
   ...110
   ...111 - não pode ser utilizado para endereçar *hosts,* pois é o endereço de *broadcast* desta sub-rede (10.0.3.7).
   Restando então, 6 endereços válidos nessa sub-rede (.1 ; .2 ; .3 ; .4 ; .5 ; .6).

3. Analisar os endereços das sub-redes:
   Quantos *bits* fazem parte do endereço da sub-rede?
   XXXXXXXX. YYYYYYYY. YYYYYYYY.YYYYY000 , onde X é rede; Y é sub-rede; e 0 são *bits* para *hosts*.

Qual é o padrão formado pelos endereços de sub-rede?

Neste caso, de 8 em 8 números decimais. Por exemplo: Sub-rede zero é: 10.0.0.0. Primeira sub-rede: 10.0.0.8. Segunda sub-rede: 10.0.0.16. Terceira sub-rede: 10.0.0.24... E assim, sucessivamente. Ou seja, o padrão para encontrar a décima sub-rede é 10 x 8 = 80 - > 10.0.0.80 (essa é a décima sub-rede e os *host*s dela são: 10.0.0.81, 10.0.0.82, 10.0.0.83, 10.0.0.84, 10.0.0.85 e 10.0.0.86, pois 10.0.0.87 é o endereço de broadcast desta sub-rede e 10.0.0.88 é o endereço da décima primeira sub-rede.

Você certamente já percebeu que por meio de exemplo, é bem mais fácil compreender um assunto como este que você acabou de estudar. E a partir de agora? O será que você irá estudar? Siga adiante e descubra você mesmo.

SEÇÃO 4
Configuração

A configuração dos *hosts* com os endereços corretos e a administração desses endereços IP também é uma atividade de um administrador de redes. No entanto, se você é responsável pela configuração de centenas de equipamentos de uma empresa, a tarefa de configurar um a um pode se tornar inviável. Para isso, existem diferentes formas de aplicar as configurações aos dispositivos de rede dos equipamentos.

Existem basicamente dois tipos de atribuição:

- **estática** - é realizada manualmente por um técnico responsável, em cada equipamento;
- **dinâmica**- feita através de um serviço de rede denominado DHCP.

No DHCP, você pode definir as faixas de endereços e as configurações necessárias para prover o acesso dos equipamentos aos recursos disponíveis na rede. Desta forma, automaticamente, ao iniciar o sistema operacional, cada *host* da sua rede irá procurar pelo serviço e receber as configurações definidas no servidor.

Dentro de uma rede ou sub-rede, os dispositivos se comunicam sem a necessidade de equipamentos intermediários (roteadores). Caso o *host* de destino esteja em outra rede, o pacote deverá ser entregue ao roteador da sua rede local, que possui o papel de *gateway* da rede local para alcançar outros *hosts* de redes remotas.

Como não é possível saber a rota para todas as redes, principalmente na Internet, utiliza-se um *gateway* padrão para encaminhar um pacote para fora da sua rede local. Esse roteador verificará em sua tabela de roteamento se possui uma entrada para o endereço de destino do pacote, ou então uma rota padrão e encaminhar o pacote para outro roteador.

Uma vez que a porção de rede do endereço de destino for diferente da porção de rede do endereço de origem, significa que o pacote deverá ser encaminhado para outra rede (pois não faz parte da rede local), através do *gateway* padrão. O *gateway* padrão deverá ser configurado nas conexões de rede, conforme você pode conferir na figura a seguir.

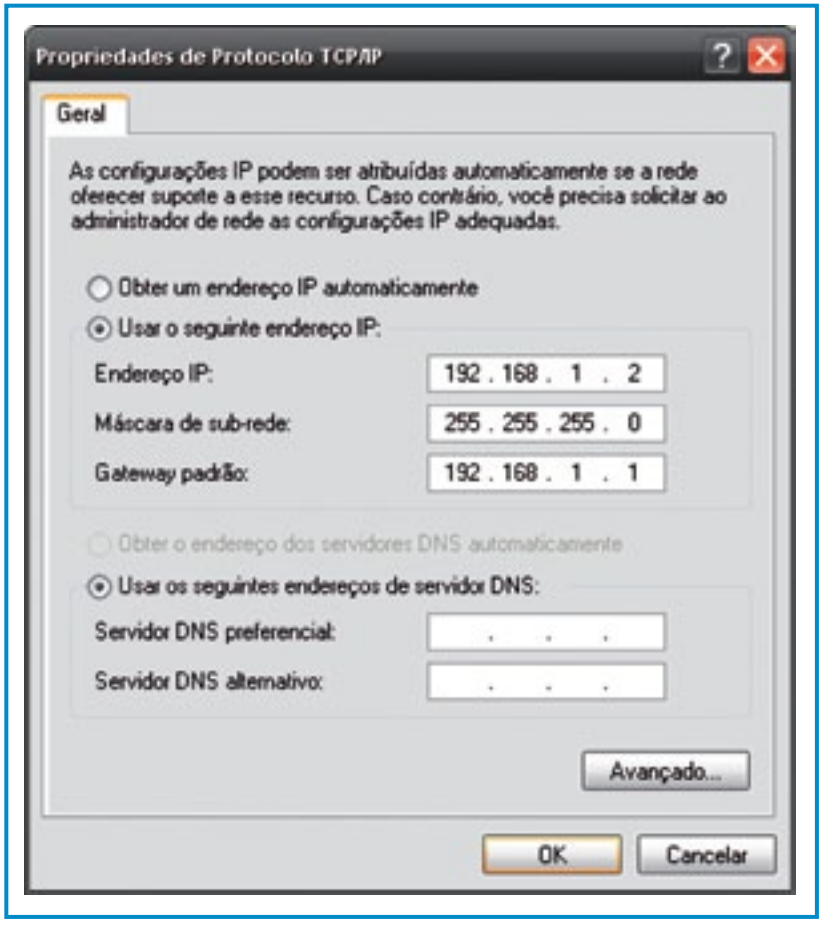


Figura 24: Configuração de conexão de rede.

As configurações de rede podem ser visualizadas no *Prompt* de comando do *Windows*, através do comando: ipconfig, ou ainda: ipconfig */all* para visualizar todos os parâmetros de rede.

Além das configurações de endereço IP, máscara de rede e *gateway,* é importante que o *host* tenha acesso a um servidor DNS. Caso o usuário necessite acessar páginas *Web,* ele não poderá utilizar apenas os endereços IP. Por isso, quando um usuário digitar um nome de domínio como: www.sc.senai.br, o servidor DNS poderá fornecer o endereço IP para que o processo de transferência de dados da página possa ocorrer.

Você chegou ao final de mais uma unidade de estudo. Certamente este conhecimento irá contribuir no seu desenvolvimento profissional, favorecendo uma prática consolidada, cujo resultado você mesmo reconhecerá com satisfação.

Unidade de estudo 4

Seções de estudo

Seção 1 - Camadas de sessão e apresentação
Seção 2 - Camada de aplicação
Seção 3 - Aplicações

Tecnologia de Aplicação

SEÇÃO 1
Camadas de sessão e apresentação

A camada de sessão é responsável por criar, manter e finalizar sessões na rede. Ela mantém diálogos entre os aplicativos dos *hosts* de origem e de destino.

Um exemplo de utilização dessa camada é a abertura de várias abas ou janelas no navegador, para diferentes *sites Web*. Você pode navegar em um *site* numa aba, abrir outro na segunda aba e assim por adiante, sem que uma sessão interfira na outra.

Figura 25: Abas de um navegador *Web*

E a camada apresentação?

A camada de apresentação é responsável pela codificação e conversão dos dados da camada de aplicação, assunto da próxima seção.

São exemplos dessa camada o texto puro ASCII, as imagens JPEG ou os formatos de arquivos de música MP3. Essa camada também é responsável pela compressão e descompressão dos dados (quando chegar ao *host* de destino), além da criptografia, quando aplicável como, por exemplo, o protocolo seguro HTTPS.

Figura 26: Site da internet utilizando o protocolo seguro HTTPS

Vamos agora ver a camada aplicação. Continue atento!

SEÇÃO 2
Camada de aplicação

Utilizando o modelo de referência OSI temos uma representação abstrata de camadas criada como diretriz para o *design* de protocolos da rede.

Representação abstrata?

Entenda melhor. A camada de aplicação faz a interface entre o protocolo de comunicação e o aplicativo que pediu ou que receberá a informação da rede.

Por exemplo: ao solicitar uma página *Web*, o seu navegador (aplicativo) irá solicitar seu pedido para a camada de aplicação.

Percebeu como é fácil?

Mesmo que o modelo TCP/IP tenha sido desenvolvido antes do modelo OSI, a camada de aplicação do TCP/IP se ajusta às três primeiras camadas do modelo OSI: aplicação, apresentação e sessão. Com isso, ao estudar a camada de aplicação, você inclui também informações sobre as camadas de apresentação e de sessão, entendendo como funciona a camada de aplicação do modelo TCP/IP.

Está claro até aqui? Que tal vermos agora alguns exemplos de protocolos utilizados na camada de aplicação do TCP/IP? Acompanhe.

- Protocolo de Serviço de Nome de Domínio (DNS) – utilizado para resolver nomes a endereços IP.
- Protocolo de Transferência de Hipertexto (HTTP) – utilizado para transferir arquivos que compõem as páginas *Web* da *World Wide Web* (WWW).
- Protocolo de Transferência de *E-mails* (SMTP) – utilizado para transferência de mensagens e anexos de *e-mail*.
- *Telnet* – protocolo de simulação de terminal, utilizado para fornecer acesso remoto a servidores e dispositivos de rede.
- Protocolo de Transferência de Arquivos (FTP) – utilizado para transferência interativa de arquivos entre sistemas.

Na seção a seguir, você conhecerá mais detalhadamente estes protocolos. Pronto para percorrer novos caminhos?

SEÇÃO 3
Aplicações

Nessa seção, veja exemplos de protocolos que trabalham na camada de aplicação, para que você possa compreender melhor na prática como isso tudo funciona.

HTTP

Segundo Tittel (2002, p. 205)

> O Protocolo de Transferência de Hipertexto (HTTP – *HyperText Transfer Protocol*) especifica as regras para a comunicação entre navegadores e servidores da *Web*. As solicitações HTTP são enviadas como texto ASCII, e existem várias palavras-chave que permitem diferentes tipos de ações.

Quando você acessa um *site* na internet, passa por diversos procedimentos que ficam ocultos ao usuário. A partir da requisição feita por um cliente (normalmente um navegador *Web*), o servidor responde com os dados e, no recebimento, o navegador interpreta as informações e as apresenta ao usuário.

> O navegador *Web* é a aplicação utilizada pelos computadores para acessar a *World Wide Web* e utilizar os recursos armazenados em um servidor *Web*.

Digitando o endereço *Web* (ou URL), seu computador estabelece uma conexão com o serviço *Web* que está sendo executado no servidor, utilizando o protocolo HTTP (*Hyper Text Transfer Protocol*).

Nessa fase, o navegador interpreta o endereço *Web* (http://www.sc.senai.br/index.html) que você requisitou e o divide em três partes:

1. http (protocolo);
2. www.sc.senai.br (nome do servidor);
3. index.html (nome do arquivo específico solicitado).

Após a realização desta interpretação, o navegador consulta um servidor de nomes (DNS) para converter www.sc.senai.br em um endereço numérico, que será utilizado para se conectar ao servidor.

Fazendo uso da estrutura do protocolo HTTP, o navegador envia uma solicitação do arquivo index.html ao servidor, que por sua vez, envia o código HTML contido no arquivo. Para finalizar, o navegador decifra o código HTML e formata a página para ser exibida na janela do navegador.

Percebeu quantos procedimentos estão envolvidos quando você acessa um site da internet?

O protocolo HTTP, utilizado na transferência dos dados, é um dos protocolos mais utilizados na camada de aplicação. Seu contexto se baseia em solicitação e resposta. Basicamente, quando o cliente envia uma solicitação, o protocolo HTTP define os tipos de mensagens da comunicação com o servidor e também as características da resposta.

Mas, atenção! Embora o protocolo HTTP seja considerado flexível, não é seguro. As mensagens transferidas entre cliente e servidor são facilmente interceptadas e lidas, muito pelo fato de não serem criptografadas. Para realizar uma comunicação segura, utiliza-se o protocolo HTTP Seguro (HTTPS). Com ele, podem ser utilizadas autenticação e criptografia para proteger os dados que trafegam entre o cliente e o servidor.

Figura 28: Navegador *Web*

Quer saber o que são os Protocolos de Transferência de Arquivos? Confira os FTPs!

FTP

O Protocolo de Transferência de Arquivos (FTP) possibilita transferências de arquivos entre um cliente e um servidor, pela internet. Ele executa um serviço (*daemon*) no servidor, aceitando solicitações FTP. Nesse caso, o cliente utilizará uma aplicação cliente-FTP.

Segundo Tittel (2002, p. 181):

> O Protocolo de Transferência de Arquivo (FTP – *File Transfer Protocol*) é um dos protocolos IP mais antigos em uso. É o protocolo mais popular usado na internet para transferência de arquivos entre sistemas diferentes.

Para transferir arquivos, o FTP precisa de duas conexões FTP. A primeira é utilizada para controle de tráfego, comandos e respostas do servidor na porta 21/TCP. No momento da transferência dos arquivos, o cliente estabelece uma segunda conexão, na porta 20/TCP, permitindo assim a real transferência do arquivo.

Vale lembrar que a transferência de arquivos pode acontecer em ambas às direções, ou seja, *download* ou *upload*.

E-mail

Você já tentou imaginar-se sem *e-mail* nos dias de hoje?

Esse poderoso protocolo revolucionou a forma como as pessoas interagem e trocam informações. Envio de textos, mensagens, fotos e imagens podem ser rapidamente realizados por *e-mail*. É importante também saber que os dois principais protocolos utilizados são o SMTP e o POP3. Vamos aos conceitos de cada um deles!

O *Simple Mail Transfer Protocol* (SMTP) é responsável pelo envio de mensagens da aplicação cliente – também conhecida como *Mail User Agent* (MUA) –, até o servidor que estará executando o serviço e escutando na porta 25/TCP.

O servidor de *e-mail* opera em dois processos separados.

- *Mail Transfer Agent* (MTA).
- *Mail Delivery Agent* (MDA).

Processo MTA e MDA?

Isso mesmo! O processo MTA é utilizado para encaminhar *e-mail*, ou seja, enviar uma mensagem para outro servidor de *e-mail* ou entregar localmente para o MDA. Já o MDA é responsável por entregar a mensagem de *e-mail* para a caixa local do usuário, fazendo assim a entrega real. Ficou mais claro agora, não é mesmo?

Já o POP3 (*Post Office Protocol*, versão 3) é um protocolo de entrega de correspondência de entrada, típico cliente-servidor. Portanto, o cliente, aplicando o *e-mail* (MUA), solicita ao servidor a listagem de mensagens em sua caixa postal. Quando a conexão é estabelecida, o servidor responde à requisição e ao *download* das mensagens para o cliente de *e-mail*, apagando as mensagens do servidor em seguida.

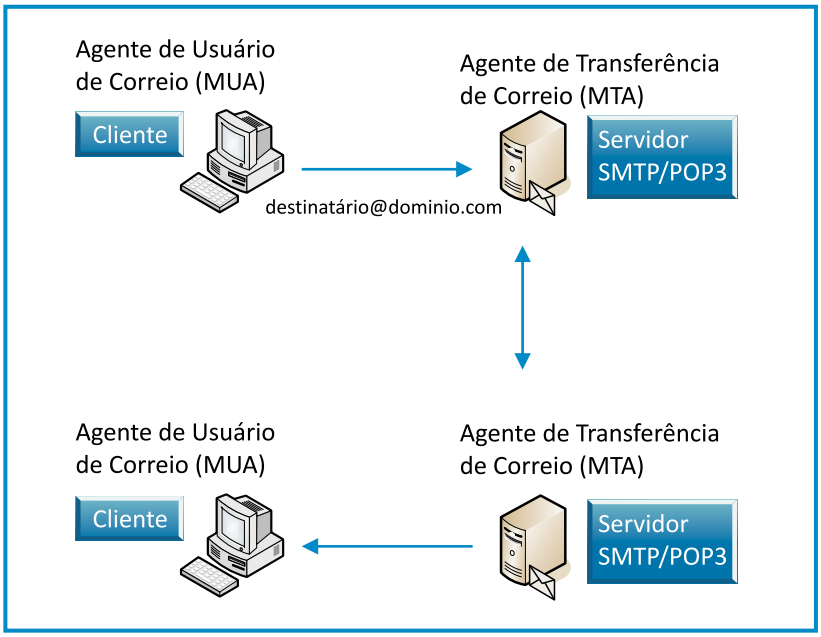


Figura 29: Transferência de *e-mails* entre MUA e MTA

DNS

Você estudará em detalhes, que em redes TCP/IP cada pacote é rotulado com o endereço lógico de origem e de destino, conhecido como endereço IP. Em uma pequena rede local, lembrar do endereço de algumas máquinas poderá até ser fácil. Mas, com a inclusão de novos computadores, ou até mesmo com endereços IPs de servidores de outras redes, torna-se praticamente impossível lembrar-se de tudo.

Imagine o seguinte endereço de *e-mail*: aluno@192.168.196.35. Seria muito difícil memorizá-lo. Podemos ainda pensar em outra situação: o endereço IP do servidor precisou ser alterado e o novo endereço de *email* deve ser informado a todos. Isso seria totalmente impraticável sem um nome de domínio, como é utilizado hoje. Você concorda?

Nomes como www.senai.br são mais fáceis de lembrar-se do que endereços IP. É aí que entra o Servidor de Nomes de Domínio – DNS (*Domain Name Server*), que foi criado para resolver o nome de domínio em endereço IP.

Lembre-se de que, no pacote IP, só é aceitável o endereço IP como endereço de destino ou origem.

Segundo Tittel (2002, p. 189):

> Quando dispositivos diferentes se comunicam um com o outro, são usados endereços IP e endereços físicos (MAC) para transferir as informações entre os transmissores e receptores. É muito mais fácil as pessoas se lembrarem de uma sequência de palavras ou caracteres do que uma sequência de números. Portanto, para que os sistemas sejam convenientes ao usuário, e possam se comunicar há a necessidade da existência de um mecanismo que traduz esses nomes amigáveis para os endereços IP correspondentes. O DNS é um dos serviços e mecanismos disponíveis no conjunto de protocolos IP que fornece esse tipo de serviço.

Isso significa que, ao solicitarmos uma URL, por exemplo, o cliente DNS local no computador irá solicitar um pedido para o servidor DNS que está definido na configuração do adaptador de rede local do *host*. Um utilitário muito importante para verificar se o DNS está respondendo a requisições é o *nslookup*, utilizado no *prompt* de comando. Vamos entender o que é o servidor DNS e para que ele serve? O servidor DNS armazena cada domínio como um conjunto de registros. Esses registros contêm o nome, endereço e tipo de registro.

E quais são os tipos de registros?

Veja a seguir.

- A – endereço do dispositivo final.
- NS – servidor de nome confiável.
- CNAME – nome canônico (ou Nome de Domínio Completo) para um codinome. Utilizado quando vários serviços têm um único endereço de rede, mas cada serviço tem sua própria entrada no DNS.
- MX – registro de troca de correspondência. Mapeia um nome de domínio para uma lista de servidores de troca de e-mail para tal domínio.

Por falar em Sistema de Nome de Domínio, você sabia que ele se utiliza de um sistema hierárquico para criar um banco de dados de nomes para fornecer resolução do nome? Isso mesmo. A hierarquia se parece com uma árvore invertida, com a raiz no topo e os galhos embaixo.

A resolução de um domínio acontece sempre de trás para frente, começando em buscas no servidor DNS raiz, que mantém registros sobre como chegar aos servidores de domínio de nível superior como, por exemplo, "br". É importante observar que esses servidores representam o tipo de organização ou país de origem. Logo abaixo deles estão os domínios de segundo nível ou secundários, que irão responder, por exemplo, a "empresa.com. br". A figura seguinte mostra uma visão geral da hierarquia DNS. Acompanhe!

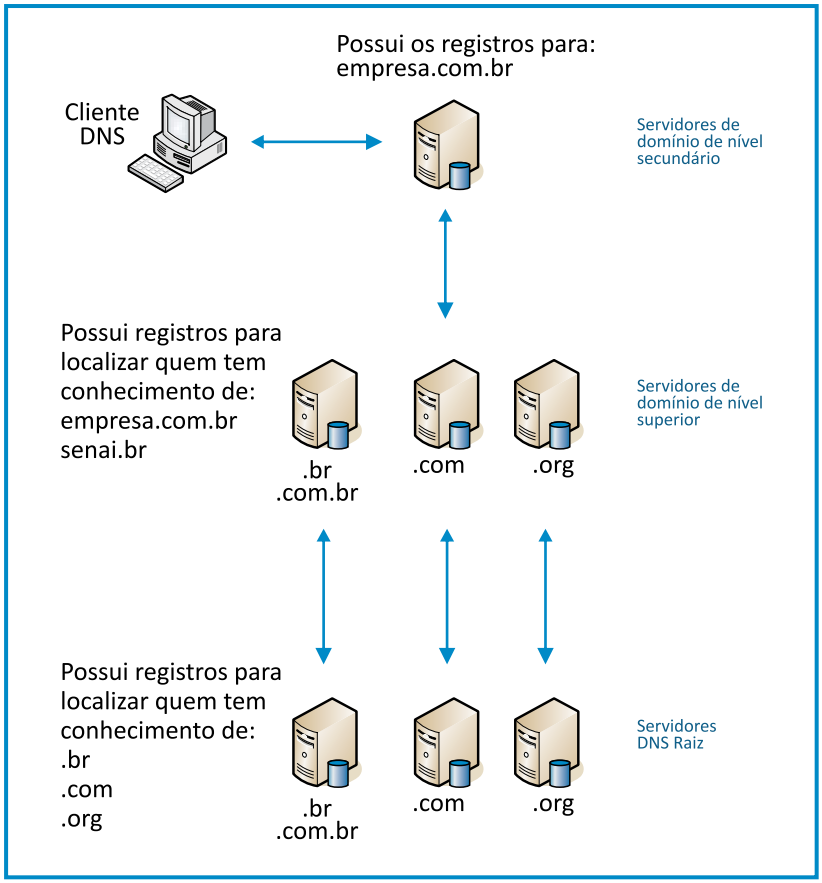


Figura 27: Hierarquia DNS

DHCP

Você já ouviu falar em DHCP?

A sigla em inglês corresponde ao serviço Protocolo de Configuração Dinâmica de *Host* e permite que toda a configuração de rede seja feita de forma automática, sem a intervenção do usuário. O DHCP permite ainda que um *host* obtenha um endereço IP quando se conecta a rede. O servidor DHCP é contatado e um endereço é solicitado. Sendo assim, esse servidor escolhe um endereço de uma lista configurada de endereços chamada *pool* e o atribui (aluga) ao *host* por um período determinado.

Como funciona o DHCP?

Você verá que o computador cliente, que possui a configuração automática de rede, torna-se o cliente DHCP. Ele enviará uma mensagem *broadcast* pela rede, solicitando a resposta de um servidor DHCP. Assim, o primeiro servidor DHCP que estiver na rede e ouvir o pedido, responderá, oferecendo-se como servidor DHCP para fornecer a configuração da rede.

Caso o cliente aceite, retornará uma mensagem para o servidor e este reservará um endereço IP e atribuir ao cliente. Além de enviar o endereço IP, enviará a máscara de rede, endereço *gateway*, servidores DNS, domínios DNS e tempos de concessão da locação, como poderá ser visualizado na figura seguinte.

Figura 28: Troca de mensagens DHCP

Precisamos lembrar também que o servidor DHCP mantém um *pool* (grupo) de endereços IP e aluga um endereço a qualquer cliente habilitado por DHCP quando o cliente é ativado. Como os endereços IP são dinâmicos (alugados) em vez de estáticos (atribuídos permanentemente), os endereços em desuso são automaticamente retornados ao *pool* para realocação. Agora que estudamos o servidor DHCP, vamos ao *Telnet*/SSH. Confira!

Telnet/SSH

Muitas vezes não é possível estar na frente do computador ou do dispositivo de rede para efetuar a sua configuração. Portanto, é interessante ter um protocolo que permita que a porta console do dispositivo seja enviada pela rede, permitindo a interação com o administrador da rede, como se ele estivesse na frente do dispositivo.

Com esse objetivo, foi criado o *Telnet*.

Vamos descobrir sua função?

O *Telnet* é um protocolo que nasceu nos anos 70, sendo uns dos mais antigos no conjunto TCP/IP. Cada conexão *Telnet* é chamada de terminal virtual ou VTY.

Para oferecer conexões *Telnet*, o servidor precisa executar um serviço *Telnet*, que ficará escutando solicitações na porta 23/TCP. Atualmente, todos os sistemas operacionais oferecem clientes *Telnet* junto ao sistema.

Mas temos aqui um problema, a segurança. Com o Protocolo *Telnet*, o usuário e a senha são enviados em formato de texto puro pela rede, o que permite que outros usuários, utilizando uma ferramenta de analisador de pacotes (*sniffer*), possam capturar os dados e ler os dados trafegados. Isso é muito perigoso!

Já o SSH (*Shell* Seguro) oferece um método seguro para acesso ao servidor. Acontece que, antes de enviar qualquer informação pela rede, um túnel totalmente seguro será criado através de criptografia assimétrica, onde a chave utilizada para cifrar (criptografar) não será a mesma que será utilizada para decifrar.

Percebeu a diferença no que se refere à segurança? Então, vamos seguir!

Aplicações P2P

Existem inúmeras formas de conseguir aquela música, vídeo, foto ou arquivo que você procura. Usando SMB, FTP ou HTTP para realizar esta tarefa, pode até parecer que não há outras formas de obter arquivos. No entanto, vamos olhar agora para outro protocolo, o *Gnutella*. Ele permite aos usuários compartilharem arquivos entre si, usando aplicações P2P, já estudadas anteriormente. Se você é de uma geração que se preocupava em procurar letras de música em revistas e gravar fitas cassete para escutar, deve lembrar facilmente de um *site* chamado *Napster*. Esse *site* ficou mundialmente famoso por apresentar músicas gratuitamente, que pudessem ser baixadas de uma gigante base de dados. Sim, você não precisava mais ir a uma loja de CD para comprar um álbum novo de sua banda favorita. E havia muita música para buscar, ao alcance do *mouse* (e da largura de banda disponível, claro).

Atualmente, um *software* P2P serve para conectar outras aplicações que usem o mesmo protocolo para *download* de arquivos. Na prática, o que o *Napster* fazia e que de certa forma ainda pode ser feito por meio de aplicações como *Azureus*, *LimeWire, Morpheus* e o *Torrent* (veja na figura seguinte), é praticamente o mais leve cliente P2P existente para o MS *Windows*.

Existem vários programas P2P. O Protocolo *Gnutella* é mantido pela *Gnutella Developer Forum*, mas esses clientes que você estudou anteriormente e outros que você talvez conheça e utilize por algum motivo, são desenvolvidos frequentemente como extensões para obter melhor funcionamento em algum caso específico. Um exemplo é o *Torrent*, que foi desenvolvido para não precisar de muitos recursos.

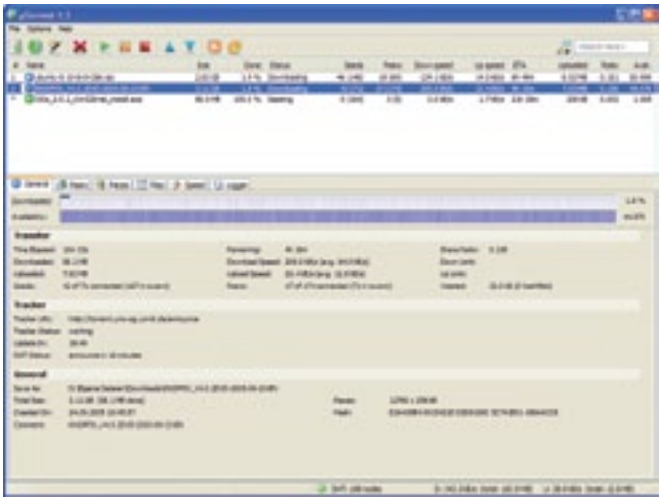


Figura 29: Cliente *Torrent*

Note! Normalmente não há um banco de dados central responsável por registrar todos os pares (*peers*) na rede. Ao contrário, cada computador na rede é capaz de conversar com os outros, inclusive para localizar outros recursos. Confira a imagem a seguir para compreender melhor.

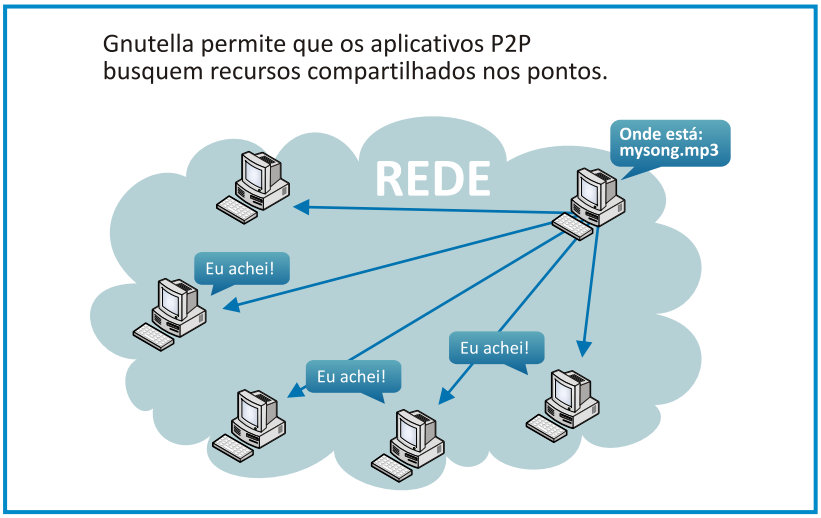


Figura 30: Funcionamento P2P

Ficou mais claro agora? Observe que, quando você usa um programa que trabalha com o Protocolo *Gnutella* (ou outro derivado), sua aplicação procura outras aplicações, formando nós, sobre o mesmo protocolo que estiver na rede. Esses nós trabalham para procurar respostas ao arquivo que você procurou e que serão transportados por serviços HTTP.

No protocolo *Gnutella*, existem cinco tipos de pacotes, cada qual com sua funcionalidade. Os pacotes poderão descobrir arquivos (*ping*), receber respostas de *ping* (*pong*), procurar ou consultar por arquivos (*query*), buscar resposta para uma consulta (*query hit*), ou ainda pedir para baixar o arquivo (*push*).

Com as informações que esta unidade de estudo disponibilizou, é interessante você trocar ideias com o professor e colegas. Caso sentir necessidade, releia o conteúdo. A seguir você terá mais uma etapa, cujo tema, ativos de redes será apresentado a você. Explore todo o conteúdo.

Unidade de estudo 5

Seções de estudo

Seção 1 - *Switch*
Seção 2 - Redes sem-fio
Seção 3 - Roteamento

Ativos de Rede

SEÇÃO 1
Switch

Nesta unidade curricular, os equipamentos ativos de rede que você estudará operam na camada 2 do modelo OSI ou na camada 1 do modelo TCP/IP. São eles que realizam as operações necessárias para a entrega dos dados entre *hosts* de uma mesma rede local.

Primeiramente, precisamos saber que os ativos de redes locais devem considerar o formato do quadro de acordo com o protocolo que está sendo utilizado. Por exemplo, um ativo de rede que opera com o protocolo *Ethernet* 802.3 deve analisar os quadros considerando as informações que o mesmo carrega. Observe!

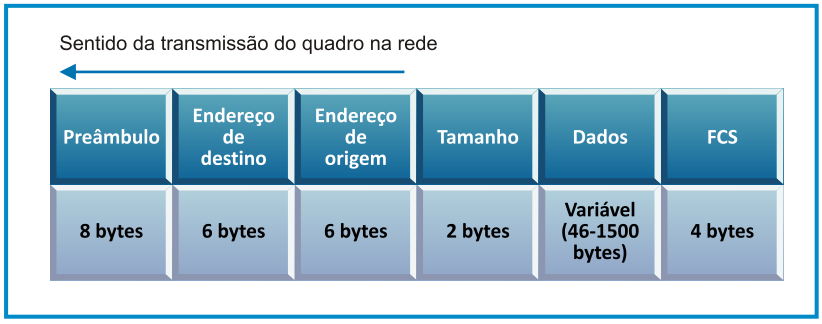


Figura 31: Modelo de quadro *Ethernet* 802

Após o recebimento de um quadro *Ethernet* 802.3, o *host* de destino deve entregar as informações do campo "Dados" para o seu protocolo de camada 2 (TCP/IP). No entanto, nosso estudo neste momento se restringirá às operações realizadas antes desta etapa.

Portanto, quando um *host* precisa encaminhar um quadro para outro *host* da rede local, o mesmo possui apenas a informação de endereço IP. Nesse momento, o protocolo ARP (*Address Resolution Protocol*) entra em operação no *host* de origem. Ele encaminha um quadro *broadcast* ao concentrador de rede que deverá ser recebido por todos os outros *hosts* no mesmo segmento de rede.

E você sabe qual é a função do protocolo ARP?

Esse protocolo é responsável por identificar o endereço MAC (Media Access Control) do *host* de destino, pois até o momento de enviar as informações, o *host* de origem não o conhece. Após receber a mensagem ARP, o *host* de destino identifica-se para o de origem, que poderá incluir o endereço de destino no quadro que precisa encaminhar.

Mas todo esse processo ocorre milhares de vezes nas redes locais. Os quadros *broadcast* são endereçados com FF:FF:FF:FF:FF:FF.

E apenas os *hosts* que fazem parte do mesmo domínio de *broadcast* recebem essa solicitação. Um domínio de colisão é criado por um *switch* quando dois *hosts* se comunicam em uma rede.

Você sabe o que isto significa?

Quando utilizamos um *hub* para conectar diversos *hosts*, todos fazem parte do mesmo domínio de colisão. Observe, no entanto, que os *hub*s não são capazes de identificar as informações dos quadros.

> E o mais importante: não podem segmentar domínios de colisão.

Portanto, todos os *hosts* que estão conectados a um *hub* devem compartilhar o mesmo canal de comunicação. Esta forma de operação é menos eficiente, uma vez que a largura de banda deve ser dividida entre os *hosts* que trocam dados pela rede.

Ficou claro até aqui? Vamos seguir!

Para aumentar o desempenho das redes, as tecnologias de *switch*ing introduziram inúmeros conceitos e protocolos. Um *switch Ethernet* é capaz de aprender o endereço MAC de cada *host* e associá-lo a cada uma de suas portas. Ou seja, quando utilizamos o *switch*, segmentamos o domínio de colisão fazendo com que os *hosts* possam utilizar um canal exclusivo de comunicação.

Um conceito importante neste estudo é o de comutação. Pense em comutação como sendo um mecanismo que permite aos *hosts* realizarem um revezamento no uso dos canais de comunicação disponíveis pelo ativo de rede

Para realizar a comutação, um *switch* utiliza a tabela CAM (Content Addressable Memory). O objetivo desta memória é armazenar uma relação entre os endereços MAC dos *hosts* da rede com as portas nas quais eles podem ser encontrados.

Desta forma, quando um dos *hosts* encaminha um quadro ao *switch*, irá identificá-lo e armazenar seu endereço nesta memória. No exemplo seguinte, apresentamos uma ideia de como funciona a tabela CAM. Consideramos que os *hosts* A, B e C estão associados às portas 2, 4 e 6 de um *switch* qualquer. Observe.

Tabela 1: Exemplo de tabela CAM

MAC	Porta
AA:AA:AA:AA:AA:AA	2
BB:BB:BB:BB:BB:BB	4
CC:CC:CC:CC:CC:CC	6

Neste caso, sempre que o *switch* receber um quadro com endereço MAC de destino AA:AA:AA:AA:AA:AA, ele deverá encaminhá-lo para a porta 2. Mas, quando desligamos o *switch*, ele perde todos os endereços e deverá aprender novamente ao ser ligado. A mesma coisa acontece quando trocamos fisicamente os cabos que conectam os equipamentos ao *switch*.

Então fique atento!

Agora que você aprendeu alguns conceitos básicos, vamos ao próximo assunto?

Modelo de rede hierárquico

Um modelo de rede hierárquico deve considerar três grupos de equipamentos com funções diferentes:

- núcleo;
- distribuição;
- acesso.

Diversos autores descrevem as funções desses três grupos, também denominados de camadas. Vamos ver cada uma delas?

A camada de núcleo deve ser o *backbone* de alta velocidade. Ela será responsável por interconectar redes distintas e encaminhar um grande volume de dados.

E a camada de distribuição? Qual será sua função?

Para distribuir os dados entre o núcleo e os diversos setores de uma infraestrutura de redes, é necessário definir regras sobre as políticas de acesso entre os *hosts*. Em uma empresa, cada *host* deve possuir acesso apenas às informações estritamente necessárias. Esse é o papel da camada de distribuição.

Já no controle de acesso dos *hosts* aos outros canais de comunicação da rede está a camada de acesso.

Essa camada é responsável por conectar cada *host* ao seu segmento de colisão e *broadcast*. A camada de acesso também poderá determinar regras de acordo com as políticas de acesso dos *hosts* aos demais equipamentos da rede. Observe que esses conceitos devem ser considerados no momento do planejamento da infraestrutura de rede.

Como inúmeros recursos estão disponíveis nos ativos de rede, eles permitem melhorar o desempenho, aumentar a disponibilidade de acesso aos serviços e definir adequadamente as ferramentas de segurança a serem implementadas.

Ficou mais claro agora? Podemos prosseguir?

Modos de comutação

Quando um *switch* analisa o quadro que recebeu, ele deverá descobrir o endereço MAC do *host* de destino para decidir a qual porta ele poderá encaminhar.

Decidir a qual porta poderá encaminhar?

Isso mesmo! Caso o *switch* não tenha o endereço MAC em sua memória, ele deverá encaminhar o quadro a todas as portas do mesmo domínio de *broadcast* (VLAN).

Mas preste atenção! Se o quadro estiver corrompido, o switch pode decidir por descartá-lo, quando utiliza o método *store-and-forward* (armazenar e encaminhar). No entanto, esse método é lento, pois o *switch* somente poderá encaminhar o quadro para o *host* de destino após recebê-lo e verificar a integridade através do campo "FCS (*Frame Check Sequence*)".

É importante saber que o modo de comutação mais rápido é pelo método *cut-through*, pois esse método não verifica a integridade dos quadros. Apenas o campo de endereço MAC de destino é verificado. Esta estratégia melhora a eficiência do *switch*, mas ainda permite que quadros que tenham problemas com colisões, ocasionando defeitos em outros campos, sejam encaminhados aos *hosts* de destino.

O terceiro modo de comutação é denominado *fragment-free*.

Sabe o que representa?

O termo significa "livre de fragmentos" e a sua operação é semelhante ao método cut-through. No entanto, esse modo faz com que o *switch* receba os primeiros 64 *bytes* do quadro.

Esse recebimento garante que os quadros incompletos não fiquem trafegando na rede e não sejam entregues aos *hosts*. Além disso, faz com que quadros que tenham endereço de origem ou tamanho inválido também possam ser descartados.

Que tal conhecermos agora sobre a utilização de cabeamentos? Confira no próximo tópico!

Cabeamento

No projeto e construção das redes de computadores, a instalação dos ativos de rede deve prever a utilização do cabeamento correto para cada situação. Isso é muito importante! O estudo sobre cabeamento estruturado está relacionado à camada física do modelo OSI e abrange uma série de padrões e normas que deve ser observada.

Para o correto funcionamento dos ativos de rede, devemos assegurar que os *hosts* serão conectados aos concentradores de rede utilizando um padrão definido pela EIA/TIA. Nesse caso, denominado de cabo direto. No entanto, para interconectar dispositivos que trabalham na mesma camada do modelo OSI, devemos inverter os pares de fios que transmitem e recebem os sinais elétricos. Isso significa, na prática, que devemos utilizar um cabo denominado cruzado ou *crossover*.

E como funciona o cabo cruzado? Descubra a seguir!

Um cabo cruzado tem em uma das pontas a conectorização T568-A e, na outra, T568-B. Ao conectar dois PCs sem a utilização de um concentrador de rede (*hub* ou *switch*), por exemplo, será necessário um cabo cruzado. Podemos citar ainda alguns exemplos, como conectar uma porta de um *switch* a outra porta de outro *switch*, ou uma interface *Ethernet* de um roteador a outra interface *Ethernet*. Essa regra é válida até a camada de rede (camada 3 do modelo OSI).

Que outros tipos de cabos podem ser usados?

Outro tipo de cabo comumente utilizado é o rollover, ou também denominado cabo console. Esse cabo é necessário para a realização da configuração dos ativos de rede. É por ele que acessamos o console de configuração do dispositivo, o que permite ao técnico realizar alterações no modo como o ativo deverá funcionar. Além disso, através do console do equipamento é possível visualizar os registros sobre o seu funcionamento, identificando possíveis problemas de operação ou configuração.

A construção dos cabos rollover normalmente é realizada pelo fabricante.

No entanto, o mais comum é a inversão dos fios nas duas pontas do cabo, utilizando em uma ponta 1-2-3-4-5-6-7-8 e, na outra, 8-7-6-5-4-3-2-1. Observe na figura a seguir.

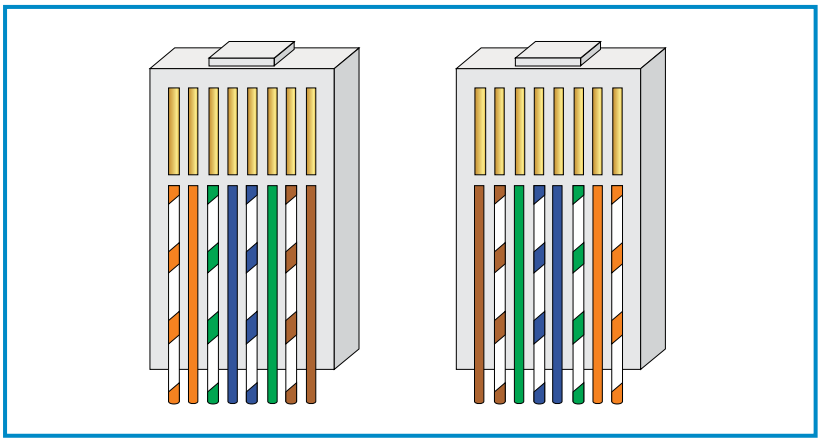


Figura 32: Conectorização cabo rollover

Fonte: Stafford (2011).

Vamos conhecer agora as redes locais virtuais.

Redes Locais Virtuais (VLAN)

Você sabe o que são as VLANs?

São redes locais virtuais, sendo que em uma única infraestrutura física podemos ter várias redes locais logicamente separadas, utilizando *switch*es que tenham suporte a esta tecnologia.

Segundo Moraes (2008) "são redes locais organizadas logicamente que podem ser construídas a partir de um único *switch* ou por vários". Observe a figura a seguir, que representa a topologia de uma rede local segmentada por duas VLANs.

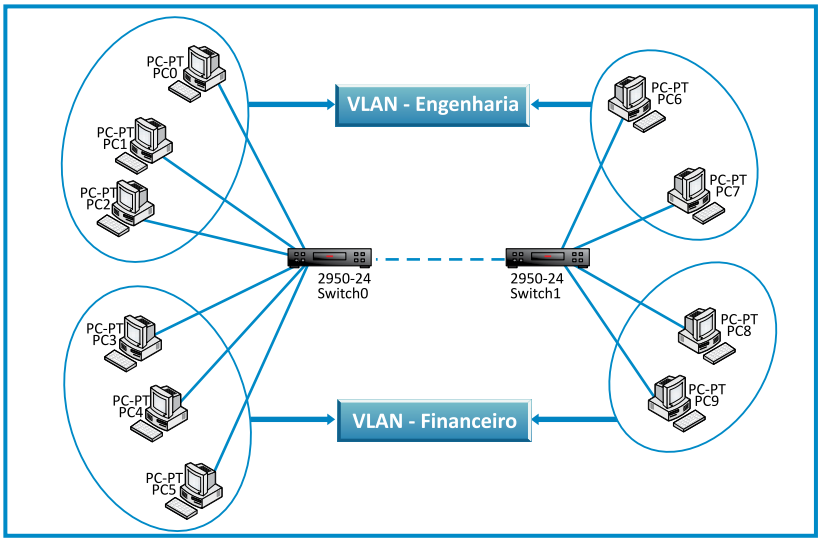


Figura 33: Exemplo de aplicação prática de VLAN

A utilização de VLANs pode representar a solução de vários problemas, dentre os quais podemos destacar a segmentação dos domínios de *broadcast*. Vale lembrar que uma rede local pode ter um tráfego bastante grande de mensagens de *broadcast*, gerados principalmente por protocolos da camada 2 e 3 como, por exemplo, o ARP e o *Spanning Tree*.

Assim, quanto maior for a rede local, maior será o volume de tráfego de mensagens de *broadcast*. Anteriormente, este problema era resolvido somente com a utilização de roteadores dentro da rede local, fazendo a segmentação da mesma em duas ou mais sub-redes. Como os roteadores não encaminham mensagens *broadcast*, o problema era resolvido.

Com a tecnologia das VLANs sendo implementada, nos *switch*es atuais esse problema ficou cada vez mais fácil de ser resolvido.

Como cada VLAN é uma rede distinta e não se comunica com a outra, a não ser com a utilização de dispositivos da camada 3, é um roteador que, como dito anteriormente, não encaminhará as mensagens de *broadcast*.

Ficou mais claro após a explicação? Outra grande utilidade das VLANs é a questão da segurança da informação dentro da rede local. Com a divisão das sub-redes, poderão controlar o acesso das informações entre cada uma delas. Caso o compartilhamento de informação de um servidor específico seja necessário, deve-se programar o rote amento entre as sub-redes, bem como utilizar um *firewall* responsável em definir o que pode e o que não pode passar de uma rede para outra.

Existem *switches* de camada 3 que, além da comutação dos quadros, fazem roteamento. Por isso, como no exemplo visualizado anteriormente, a figura do *hardware* do roteador poderia ser substituída.

Vamos acompanhar os comandos necessários para a criação e a vinculação de uma interface a uma VLAN em um *Switch* Cisco Catalyst 2950?

```
Switch>enable
Switch#configure terminal
Switch(config)#vlan 10
Switch(config-vlan)#name Engenharia      // Criando a vlan com ID 10 e nome Engenharia.
Switch(config)#vlan 20
Switch(config-vlan)#name Financeiro      // Criando a vlan com ID 20 e nome Financeiro.
Switch(config-vlan)#exit
Switch(config)#interface fastEthernet 0/2
Switch(config-if)#switchport mode access    //colocando a porta 2 em modo de acesso
Switch(config-if)#switchport access vlan 10  // colocando a porta 2 do switch na vlan Engenharia ID 10
```

Figura 34: Exemplo dos comandos de configuração

TIPOS DE VLAN

A utilização de VLANs em uma estrutura de rede local de médio e grande porte é extremamente importante para o seu desempenho. Existem alguns métodos utilizados na criação das VLANs. No entanto, a utilização desses métodos depende da marca e do modelo do *switch*. Portanto, quando se define um projeto de rede local utilizando VLANs, é necessário especificar de maneira correta o *switch* que deverá atender às tecnologias de VLANs definidas. Conheça cada um dos tipos de VLAN.

Acompanhe!

- **VLAN baseada em porta:** é o tipo mais comum, onde cada porta do *switch* é vinculada a uma determinada VLAN. Os exemplos de comandos apresentados acima atendem a esse tipo de configuração.
- **VLAN baseada em endereço MAC:** nem todos os *switches* suportam esse tipo de VLAN. Este método associa o endereço MAC de uma interface de rede a uma VLAN específica. Assim, quando o *host* é ativado, passa a ser vinculado a sua VLAN, independentemente da porta do *switch* a que está fisicamente conectado.
- **VLAN baseada em endereço IP:** obrigatoriamente, deverá ser utilizado um *switch* de camada 3, que tem capacidade de verificar qual o endereço IP de origem do *host* que está conectado a ele. Após essa identificação, fará a ligação do *host* a sua respectiva VLAN. Da mesma maneira que o tipo de VLAN anterior vai possibilitar que um determinado *host* possa conectar-se fisicamente a qualquer *switch* da rede e, independentemente da porta a que foi conectado o *host*, terá acesso à VLAN configurada anteriormente.
- **VLAN baseada em autenticação:** é o tipo de associação de VLAN mais dinâmico. É feito a partir da autenticação do usuário, utilizando, por exemplo, o protocolo IEEE 802.1x em um servidor RADIUS, onde na base de dados desse servidor cada usuário teria vínculo a uma determinada VLAN. Dessa maneira, independentemente do *host* que o usuário está utilizando e do local físico que ele está na rede local, o mesmo terá à disposição sua rede de trabalho.

Depois de conhecer os tipos de VLAN, chegou o momento de estudar as redes sem- fio. Prepare-se para muitas descobertas.

SEÇÃO 2
Redes sem-fio

Com a evolução humana, é cada vez maior a necessidade de ter acesso à informação de forma rápida, segura em qualquer hora e lugar. Para isso, algumas tecnologias têm evoluído com mais intensidade, como é o caso das redes sem-fio, que proporcionam algo muito procurado por todos os usuários, a mobilidade.

As redes sem-fio estão presentes em nossas vidas há muitos anos. Atualmente, essa tecnologia vem se expandindo com mais intensidade e você pode encontrar uma gama muito grande de equipamentos que se comunicam utilizando rede sem-fio, desde o controle remoto de sua televisão, até avançados sistemas utilizados na área cirúrgica.

Cada dispositivo utiliza um determinado tipo de tecnologia sem-fio para se comunicar. Eles podem ser infravermelho, *Bluetooth* e outros. É importante lembrar que cada um tem suas características próprias.

E você sabe quais as tecnologias de redes sem-fio mais utilizadas nos dias de hoje?

As redes sem-fio (*wireless*) são divididas em dois grupos:

- redes *indoor*;
- redes *outdoor*.

As redes *indoor* encontram-se na parte interna de prédios e residências. Ao contrário desta, as *outdoor* são redes externas que podem interligar cidades, estados e até países com rede sem-fio. As redes *outdoor* também são largamente utilizadas para interligação de empresas entre matriz e filiais.

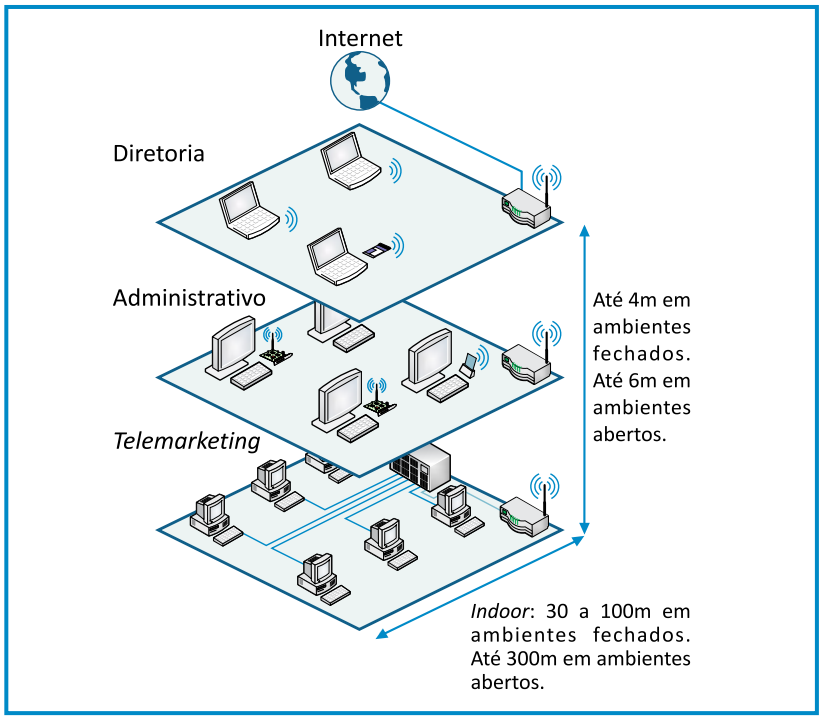


Figura 35: Exemplo de rede *indoor*

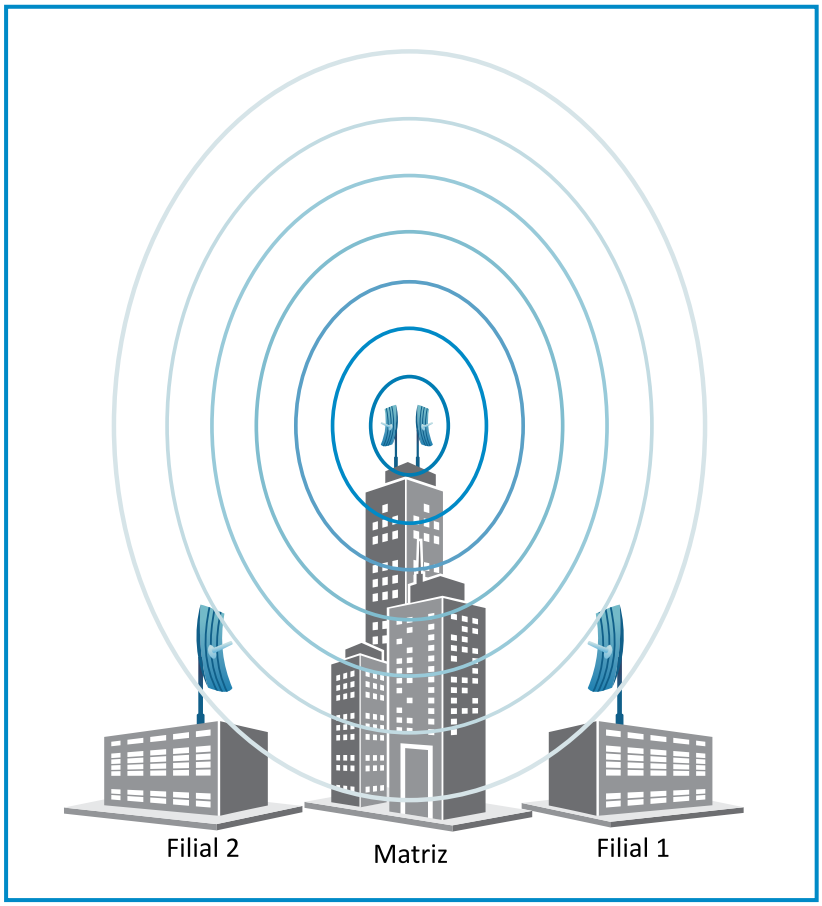


Figura 36: Exemplo de rede *outdoor*
Fonte: Nick Network (2011)

Mas, dependendo do tipo de ambiente (*indoor* ou *outdoor*), um dos tipos de tecnologia é recomendado. Para isso, é importante que você conheça as tecnologias e os protocolos existentes em redes sem- fio. Vamos lá?

Tecnologias

Bluetooth

Esta, sem dúvida, é a tecnologia mais utilizada em ambientes *indoor*.

Você sabe por quê? Isso acontece em função do seu método de comunicação ser baseado em espalhamento espectral, onde todos os dispositivos que estiverem no seu raio de propagação poderão se comunicar entre si.

O *bluetooth* trabalha na frequência de 2.4 GHz e utiliza saltos de frequência em sua comunicação, podendo trocar de frequência até 1.600 vezes por segundo. Confira!

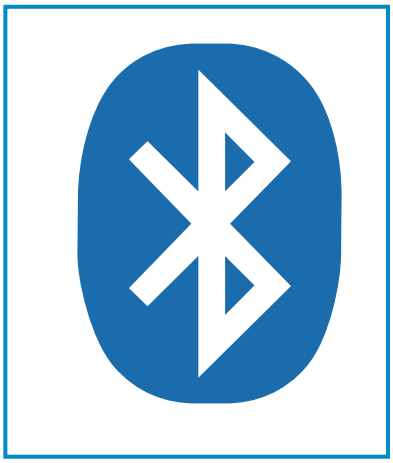


Figura 37: Logotipo *Bluetooth*

O raio do espalhamento espectral do *bluetooth* pode chegar a 11 metros. A princípio, parece ser uma distância curta, mas essa tecnologia sempre teve como objetivo o baixo consumo de energia, tornando maior a duração de baterias de dispositivos móveis como celulares e *handhelds*. Quanto à velocidade de transmissão, o *bluetooth* pode chegar a até 721Kbps.

Os dispositivos *bluetooth* se comunicam por meio de uma piconet ou picorede, podendo conter, no máximo, até oito dispositivos. O primeiro dispositivo a iniciar a conexão será o master (mestre) e os demais serão os slaves (escravos). O mestre terá a função de controlar a comunicação entre os dispositivos e estabelecer o sincronismo. Caso você precise de uma rede com mais dispositivos, poderá sobrepor as piconets.

Este esquema é denominado *scatternet*.

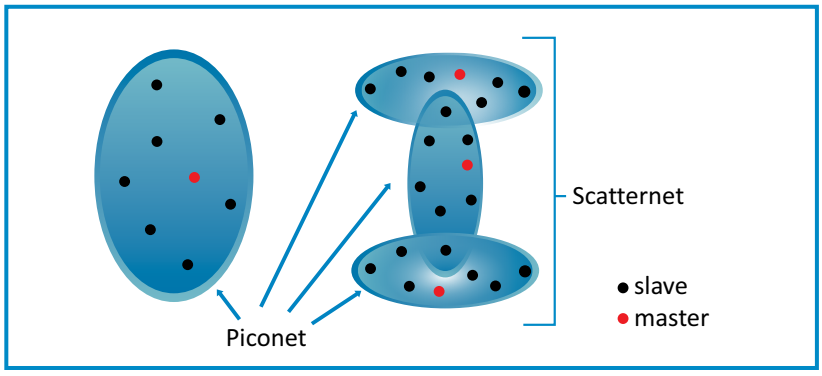


Figura 38: Exemplo de piconet e *scatternet*
Fonte: Infowester (2010)

Infravermelho

As comunicações com infravermelho atualmente são padronizados pelo IrDA (*Infrared Data Association)*. Essa tecnologia é muito utilizada em controles remotos e em aplicações que precisam de curta distância e não precisem de mobilidade, pois ao contrário do *bluetooth*, precisa que o emissor e o receptor de sinal estejam alinhados e sem nenhuma obstrução entre si.

Percebeu a importância destas tecnologias? Então acompanhe o próximo tópico!

Protocolos

Assim como tudo em redes de computadores, as redes sem-fio também seguem protocolos de funcionamento e configuração.

Você lembra o que são protocolos?

Um protocolo é basicamente um conjunto de regras que são seguidas em especial na busca pela homogeneidade dos sistemas. Em redes sem-fio existem três padrões largamente difundidos que pertencem à família 802.11, criada pelo IEEE (*Institute of Electrical and Electronics Engineers*). Esses padrões são compostos por uma série de especificações para redes locais. E com base nessas especificações, foram criados os padrões.

- 802.11b.
- 802.11g.
- 802.11a.

Atenção! Conhecer os padrões de redes sem-fio e suas características é de suma importância para que sua rede sem-fio tenha um bom funcionamento, pois cada padrão tem suas características próprias, que devem ser aplicadas de acordo com a necessidade de cada ambiente.

Pronto para ver cada um dos padrões?

802.11b

Esse foi o primeiro padrão de redes sem-fio utilizado em grande escala. Trabalha com uma velocidade máxima de transmissão de 11 Mbps na frequência de 2.4 GHz e suporta até 32 dispositivos conectados a uma estação emissora de sinal. A principal desvantagem do padrão 802.11b é justamente em função de trabalhar na freqüência de 2.4 GHz, a mesma utilizada por outros aparelhos como os telefones sem-fio, fornos de micro-ondas e aparelhos com suporte a *bluetooth*. Em contrapartida, há os pontos positivos desse padrão, dos quais podemos destacar dois:

baixo custo de dispositivos com suporte à tecnologia 802.11b;

sua larga difusão no mundo todo, o que facilita a mobilidade.

802.11g

Padrão apresentado em 2003 pelo IEEE, assim como o padrão 802.11b atua na faixa de 2.4 GHz, com uma velocidade máxima de transmissão de 54 Mbps. O 802.11g é compatível com o 802.11b e trabalha na mesma frequência de canalização.

802.11a

Esse padrão foi proposto em 1999 e opera na frequência de 5 GHz, podendo chegar a uma velocidade máxima de 54 Mbps com suporte de até 64 usuários conectados a um mesmo ponto de acesso. Esse padrão conta com disponibilidade de 12 canais: oito voltados para redes sem-fio *indoor* e quatro para rede ponto a ponto *outdoor*.

O que são as redes sem-fio *indoor* e *outdoor*?

Redes sem-fio *indoor* são as redes presentes na parte interna dos ambientes como, salas e escritórios.

Redes *outdoor* são utilizadas na parte externa dos ambientes como, por exemplo, para criar um *link* entre a matriz e as filiais de uma empresa.

Está mais claro agora? Você entenderá melhor depois do exemplo a seguir. Observe.

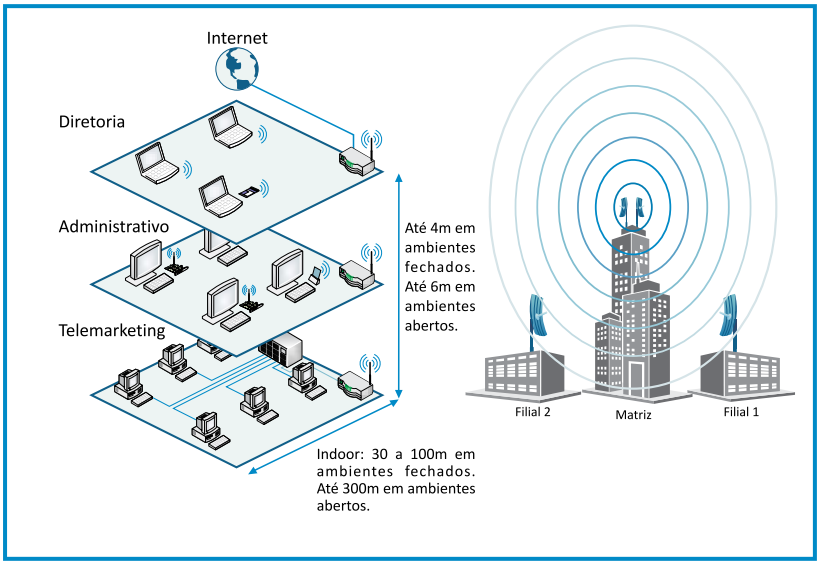


Figura 39: Exemplos de redes sem-fio *indoor* e *outdoor*

Este padrão conta com dois importantes aspectos positivos, que são sua velocidade e a ausência de interferência por atuar com frequência de 5 GHz. Em contrapartida, possui a desvantagem de ser incompatível com *Access Point* do padrão 802.11b e 802.11g. Porém, é compatível com clientes 802.11b e 802.11g.

Assim como nas redes cabeadas, as redes sem-fio funcionam na velocidade do dispositivo com menor desempenho.

Com base nessas informações sobre os protocolos de comunicação em redes sem- fio, a seguinte tabela pode ser formulada. Acompanhe!

Tabela 2: Características técnicas dos padrões de redes sem-fio

Padrão	Frequência	Velocidade	Compatibilidade com 802.11b
802.11b	2,4 GHz	11 Mbps	Sim
802.11g	2,4 GHz	54 Mbps	Sim
802.11ª	5 GHz	54 Mbps	Não

Vamos conhecer o próximo tópico, infraestrutura das redes sem-fio!

Infraestrutura

Entre os principais componentes de uma rede sem-fio existem dois básicos que são os emissores de sinal e os receptores, que podem ser dos mais variados modelos.

> Lembre-se: deve ser feito um estudo cuidadoso dos dispositivos que farão parte de sua rede sem-fio, pois esse tipo de rede conta com uma gama muito grande de fabricantes.

O principal aspecto que deve ser observado ao se projetar uma rede sem-fio é a relação custo-benefício, sem perder o foco na qualidade da rede.

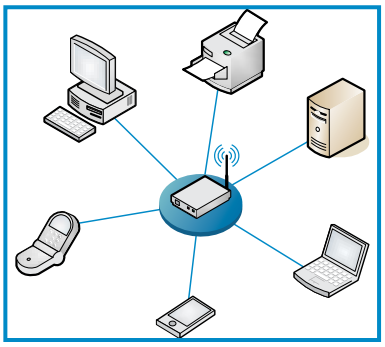


Figura 40: Exemplo de rede sem-fio
Fonte: Baixaki (2011).

Access Point (Ponto de Acesso)

É o ponto central de uma rede sem-fio. Aqui você poderá definir diferentes tarefas, de acordo com a necessidade da rede. A parte mais importante de um AP (Access Point) é o seu transceptor sem-fio, que é responsável pela emissão e recepção das informações.

O que é esse transceptor?

Trata-se de uma antena que recebe o sinal sem-fio e o converte em pulso elétrico.

Para transmitir, faz o processo inverso, tornando possível a comunicação entre os dispositivos que fazem parte da rede sem-fio.

Receptores

Com o mercado de redes sem-fio crescendo rapidamente, várias tecnologias foram criadas para fazer parte desse disputado mundo. Hoje encontramos vários dispositivos atuando com suporte a redes sem-fio como: mouse, teclado, impressoras, celulares e outros.

O funcionamento desses receptores é igual, em que o sinal, ao ser recebido, é interpretado. Com base nas informações, atitudes são tomadas em relação ao dispositivo.

E quais as vantagens das redes sem-fio?

Quando se fala em redes sem-fio, logo se pensa em mobilidade, uma das principais vantagens. Mas não é a única, pois esse é um tipo de rede fácil de ser implementada, considerada uma tecnologia barata e seu uso é cada vez mais seguro devido a seus métodos de criptografia a autenticação, que serão explicados mais adiante.

Existe alguma desvantagem nas redes sem-fio?

Sim, o grande problema das redes sem-fio sempre foi e continua sendo a interferência que ocorre no sinal, desde a emissão até a recepção. Essas interferências podem ocorrer de várias maneiras. Em redes *outdoor*, as principais são as árvores e os espelhos d'água gerados por lagos, rios etc.

Já nas redes *indoor*, o problema é maior quando, além de plantas e aquários, pessoas e móveis geram interferências no sinal. Devido a tais situações, é altamente aconselhável que o AP seja posicionado em pontos altos. Assim como o receptor, isso facilita a linha de visada entre o emissor e o receptor.

Ao se projetar uma rede sem-fio, tanto *indoor* como *outdoor*, alguns fatores devem ser observados. Veja!

Cuidados ao se implementar uma rede sem-fio

- **Antena em lugares baixos:** Em muitos manuais de Access Point, o usuário é orientado a colocá-lo em um lugar alto. Isso ajudará na linha de visada entre o emissor e os receptores presentes na rede.
- **Telefone sem-fio:** Conforme abordado anteriormente, alguns padrões de rede trabalham na frequência de 2.4 GHz, frequência que também é utilizada por outros aparelhos eletrônicos, como telefones sem-fio, por exemplo. Recomenda-se a troca do padrão da rede sem-fio ou que o dispositivo que esteja gerando interferência seja retirado do ambiente.
- **Concreto e trepadeiras:** Esses dois itens podem atrapalhar e muito o sinal da rede, pois ambos evitam que o sinal avance para uma distância maior ou podem causar uma grande interferência no sinal.
- **Micro-ondas:** Assim como o telefone sem-fio, os fornos de micro-ondas usam a frequência de 2,4 GHz. O ideal é que fiquem isolados do ambiente onde está a rede.

- **Receptor de sinal no chão:** Como mencionado sobre o posicionamento dos *Access Points*, quanto mais alto ele for, melhor será a frequência. Isso também é válido para os receptores, pois ajudará na recepção de sinal.
- **Água no ambiente:** Recipientes com água, como aquário e bebedouro, podem ser considerados como uma barreira para a propagação do sinal.
- **Vidros e árvores:** Vidros e árvores prejudicam a qualidade do sinal, causando reflexão e dispersão do sinal.

Percebeu a importância desses cuidados para ter uma boa qualidade no sinal de sua rede? Adiante!

Planejando uma rede sem-fio

Antes de você comprar antenas, *modems,* placas de rede sem-fio etc., é necessário fazer um projeto/planejamento da rede, que mostrará como os dispositivos da rede ficarão dispostos. É aconselhável fazer um diagrama, pois com o projeto em mãos tudo ficará mais claro na hora da compra dos equipamentos, mostrando possíveis equívocos.

Depois das análises sobre o diagrama da rede, poderemos dar início à compra dos equipamentos. Procure comprar tudo de um mesmo padrão, como 802.11b ou 802.11g, por exemplo. Recomenda-se, também, que todos os equipamentos sejam de um mesmo fabricante, para evitar problemas com incompatibilidade e tornar sua rede mais homogênea.

A figura a seguir mostra um exemplo simples de projeto de rede sem-fio, mas deixa claras as características da rede. Os equipamentos podem ser comprados com base nessas características.

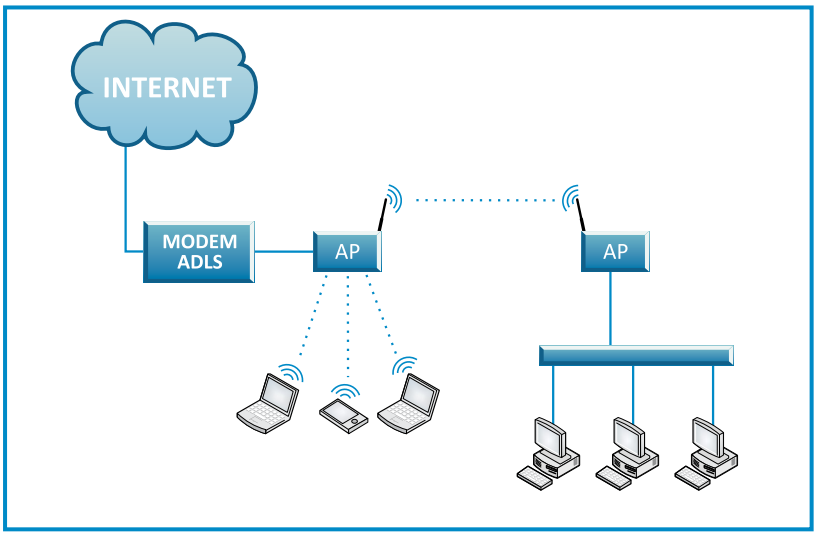


Figura 41: Exemplo de projeto de rede sem-fio

Você pode observar que, na rede apresentada, um AP distribui seu sinal para vários tipos de receptores. Entre eles está outro AP, que recebe o sinal e o distribui pela rede cabeada.

O tópico a seguir é segurança!

Segurança

A segurança é algo que sempre preocupou e preocupa usuários e desenvolvedores de tecnologias voltadas para redes sem-fio. Conheça os principais mecanismos de segurança utilizados nessas redes e como implementá-los.

As telas que serão apresentadas na sequência foram obtidas do *firmware* da AP *Router*, que está disponível no endereço eletrônico www.aprouter.com.br.

Prossiga!

SSID

O SSID (*Service Set Identifier*) também é conhecido como o ID da rede, ou seja, o endereço da rede. Trata-se de uma combinação de caracteres que são agrupados de acordo com a necessidade de cada rede sem-fio (por exemplo: "SENAI", "XYF Contabilidade" etc.).

Quando um *Access Point* é construído/configurado pelos fabricantes, eles deixam um valor padrão de SSID. O conselho é que você altere esse nome. Outra configuração que também é deixada como padrão pelos fabricantes é a opção "*broadcast* SSID" ativa.

Quando essa opção está ativa, o SSID da rede é enviado periodicamente, permitindo que todos os usuários próximos se conectem à sua rede, sem precisar saber o código. Isso é muito utilizado onde a rede sem-fio é tomada como rede pública, como em aeroportos, hotéis, cafés etc.

Porém, esse tipo de aplicação é completamente inviável em uma rede corporativa por onde trafegam dados relativos à empresa. Nesses ambientes é aconselhável que você desative a opção "*broadcast* SSID", pois essa é uma pequena prática de segurança que deve ser tomada. Ao propagar o endereço da rede, qualquer dispositivo que tiver suporte à rede sem-fio saberá o nome dela e poderá passar a monitorá-la. Fique atento!

Um dos primeiros passos para invadir uma rede sem-fio é justamente saber o SSID da rede.

Figura 42: Ativando/Desativando o SSID

Fonte: AP Router (2011).

É importante observar que, hoje em dia, são frequentes os casos em que redes sem- fio são vítimas de duas práticas de invasão de rede, o *warchalking* e o *wardriving*.

Você sabe o que significa cada uma delas? Acompanhe!

Os praticantes do *warchalking* literalmente passeiam, em geral no centro das cidades, com dispositivos receptores de redes sem-fio como *notebooks,* celulares etc. em busca de redes desprotegidas ou com uma proteção fraca. Ao encontrá-las, os indivíduos fazem desenhos em objetos próximos a redes vulneráveis. Assim, os praticantes do *warchalking* poderão utilizar os recursos da rede sem custo algum. Em muitos casos essa técnica pode trazer grandes prejuízos às empresas, pois é difícil saber quem foi o responsável sem um sistema de proteção.

Ao contrário de uma rede física, que está presente somente na parte interna de uma empresa, as redes sem-fio podem ir além dos limites geográficos da empresa. Assim, qualquer um que passar por perto poderá fazer uso dela. Isto é muito importante!

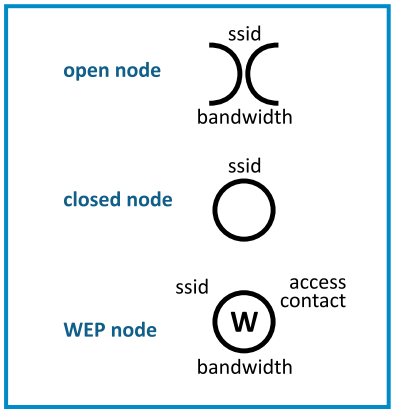


Figura 43: Exemplo de símbolos utilizados na prática do *warchalking*
Fonte: Wikipedia ([200?]).

A prática do *wardriving* é semelhante à do *warchalking*. Sua principal característica é a utilização de um veículo para ajudar na captura de sinal. O indivíduo instala um receptor de sinal em seu carro e o liga em um *notebook*. Em alguns casos, a própria antena do *notebook* é utilizada como receptor de sinal e, quanto melhor for a antena, melhor será a recepção de sinal.

Ao encontrar uma rede, ela fica sujeita a uma verificação para quebrar sua senha (caso exista uma senha). Essa análise de rede e quebra de senha é feita com a ajuda de *softwares* facilmente encontrados na internet.

Ao mostrar as duas técnicas de invasão de redes, queremos fazer com que você fique atento à segurança quando for projetar uma rede sem-fio. A seguir você conhecerá alguns métodos de criptografia criados para ajudar na segurança das redes sem-fio.

Está pronto para seguir em frente? Vamos relembrar o que é criptografia?

Criptografia

Criptografia é uma palavra de origem grega: kriptós quer dizer "escondido", e gráphein, "escrita". Logo, criptografia é uma técnica em que a escrita (informações) é escondida. Quanto ao seu funcionamento, trata-se de um embaralhamento que é feito com as informações e só o emissor e o receptor sabem como desembaralhar tais informações. Assim, qualquer intruso que venha a interceptar essas informações não saberá o que existe em seu conteúdo.

Esse embaralhamento e desembalharamento é conhecidos como encriptação e decriptação de dados, respectivamente.

Encriptação e decriptação de dados? Isso mesmo!

É importante observar que na área de redes sem-fio existem alguns métodos de criptografia para proteger sua rede. Os principais e mais utilizados são WEP e WPA.

Confira em detalhes cada um deles.

WEP

É um método de criptografia muito utilizado na atualidade.

A WEP foi projetada para agir meramente como uma porta trancada, impedindo que os invasores penetrem no tráfego da rede sem-fio; outras medidas destinam-se a sustentar essa linha inicial de defesa. "A WEP basicamente criptografa todos os dados que fluem por uma rede sem-fio, impedindo que os invasores espionem o tráfego da rede" (Engst, 2005, p. 274).

A WEP possui alguns problemas que foram se agravando ao longo dos anos. Um deles é com relação à configuração, em que uma chave WEP deve ser configurada no emissor, e em todos os receptores que tiverem acesso à rede deve ser criada uma conexão contendo a chave de criptografia configurada no seu emissor. Isso tornou o processo de configuração do WEP um tanto quanto maçante para a equipe de tecnologia da informação (TI).

Imagine você ter de configurar o WEP em 200 *notebooks* e dispositivos móveis em uma empresa. Essa tarefa com certeza não seria fácil, não é mesmo?

Outro problema do WEP, que é o mais grave, refere-se ao seu próprio método de criptografia. Com relação à geração de chaves, que são únicas e combinadas com um número de 24 *bits*, conhecido como um vetor de inicialização no qual a chave pode ser retirada com certa facilidade, a integridade WEP está exposta devido a cálculos matemáticos feitos pelo próprio WEP para checar se os dados não foram alterados. Durante a transmissão, esses mesmos cálculos são feitos de modo simples por *softwares* gratuitos encontrados facilmente na internet.

DICA

Aprenda agora como ativar a criptografia WEP para ajudá-lo a proteger sua rede. Para essa demonstração, será utilizado o *firmware* da empresa AP *Router*, que está disponível para *download*/acesso em www.aprouter.com.br.

Para configurar a criptografia do tipo WEP, é necessário que você crie uma senha de acesso de 64 *bits*, composta por cinco caracteres, ou de 128 *bits*, de 13 caracteres. Também é configurada uma numeração para essa chave como "chave 1", por exemplo. Observe um exemplo dessas configurações a seguir.

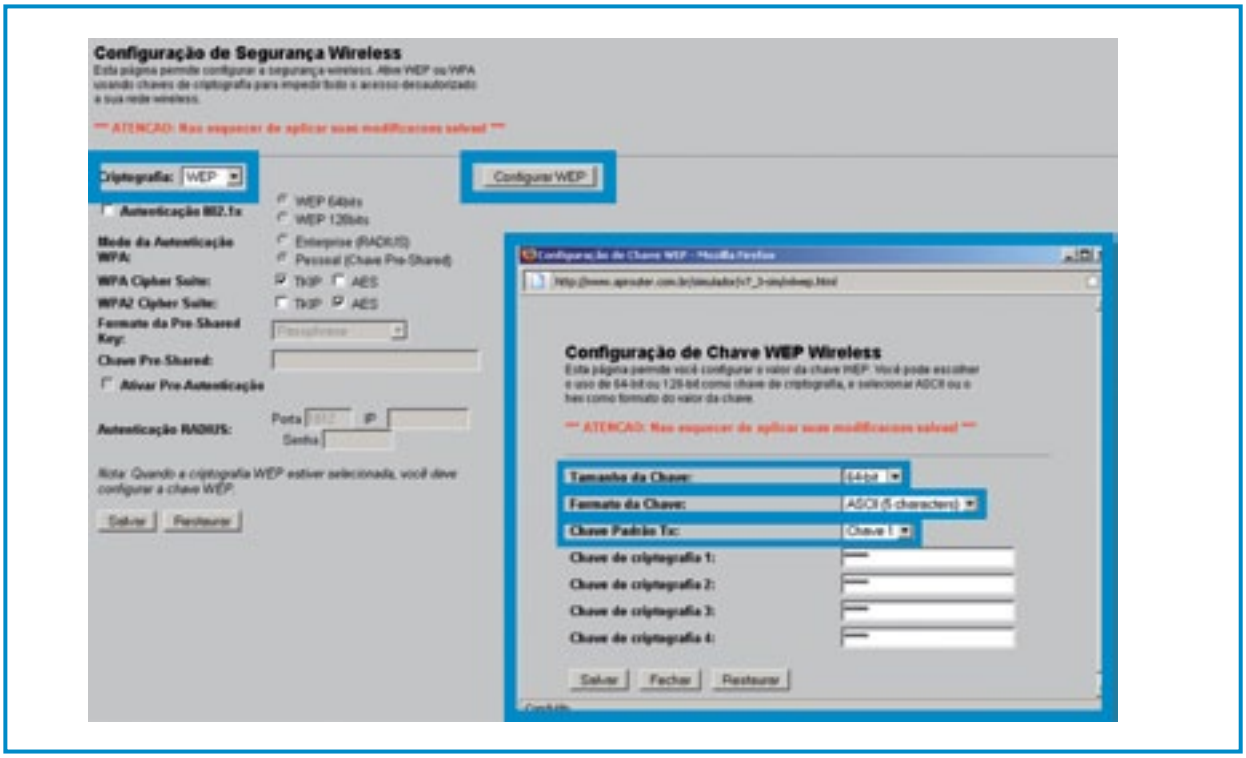


Figura 44: Ativando a criptografia WEP
Fonte: AP Router (2011)

É importante observar que o *firmware* utilizado nas demonstrações é da AP Router e as opções podem variar sua localização de fabricante para fabricante. No entanto, de modo geral a configuração sobre WEP possui as mesmas características.

Depois de criada a rede sem-fio, você terá de configurar as estações que terão acesso a essa rede. Aqui é necessário configurar a rede com a senha e o SSID configurados no *Access Point*.

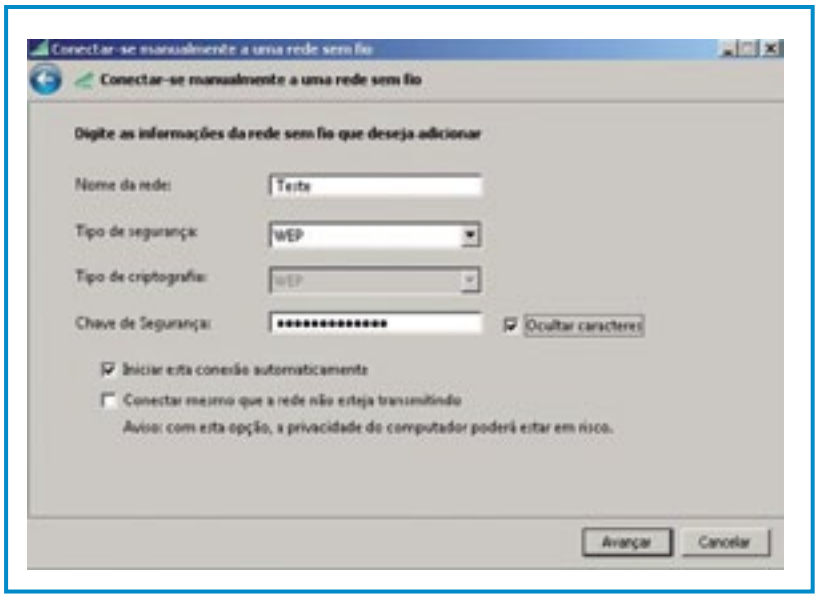


Figura 45: Exemplo de configuração no cliente WEP

Veja agora o método WPA

WPA

Uma das principais diferenças da criptografia WEP para a WPA está na maneira como as chaves são compartilhadas. Segundo Engst (2005, p. 277) "O segredo pré-compartilhado não é realmente a própria chave de criptografia, em vez disso, a chave é matematicamente derivada dessa senha".

Naturalmente, se alguém obtém o segredo pré-compartilhado, ele ainda pode acessar a sua rede, mas os *crackers* não podem extrair essa senha dos dados da rede, como era possível com a WEP.

Nesse padrão foram feitas melhorias com relação ao vetor de inicialização em que foi inserida uma nova tecnologia chamada TKIP (*Temporal Key Integrity Protocol*). Com essa tecnologia, o vetor de inicialização passou para 48 *bits*, aumentando a qualidade na criptografia e dificultando ou quase impossibilitando que a senha seja quebrada.

Além de seu alto nível de segurança, a sua configuração também é mais simples que o WEP. Ao ativar o WPA com suporte ao TKIP, basta criar a senha que o WPA cuidará da segurança das informações, conforme você verá a seguir.

Figura 46: Configurando WPA

Fonte: AP Router (2011).

A segurança é algo que sempre vai preocupar a equipe de TI. Ao implementar um sistema de distribuição de rede sem-fio, é importante que você siga algumas regras básicas que podem dificultar o acesso à rede. Algumas delas são:

- desativar o *broadcast* do SSID;
- evitar colocar informações sobre a empresa na configuração de senha;
- criar políticas de alteração de senhas: por exemplo, uma vez por mês trocar a senha;
- optar por criptografia WPA.

Essas são pequenas e boas práticas que dificultam e em muitos dos casos impedem o acesso não permitido à sua rede. Fique atento!

No mercado atual existem vários *softwares* criados para detecção e análise em tráfego em rede sem-fio. Como exemplo, temos o *NetStumbler*.

Essa é uma ferramenta criada para a plataforma Windows que funciona como um scanner, podendo criar mapas das redes encontradas no nível de recepção de sinal de cada *Access Point*, gerando gráficos de cada rede.

Figura 47: Exemplo de tela do NetStumbler
Fonte: NetStumbler (2011).

Assim como o *NetStumbler*, várias outras ferramentas são encontradas com facilidade e gratuitamente para o mesmo fim. Portanto, esteja preocupado com a segurança de sua rede!

Configurações

O que precisamos para configurar uma rede sem-fio?

Isso vai depender da necessidade de cada rede, pois em cada situação os dispositivos que fazem parte dessa rede deverão passar por diferentes configurações. Mas as configurações terão de ser feitas nos dispositivos que fazem parte da rede.

> É importante que você tenha sempre em mãos o manual do AP, pois seu sistema varia de fabricante para fabricante.

Por exemplo, para acessar um AP do fabricante AP *Router*, é necessário digitar a IP padrão 192.168.2.1 em seu navegador. Para ter acesso em outros modelos, o endereço IP de acesso é diferente. Depois de digitado o endereço no navegador, um assistente aparecerá pedindo que você se autentique. Se você não souber a senha, consulte o manual ou entre no site do fabricante.

Após a autenticação, é chegada à hora de configurar o AP. Na grande maioria dos APs, existe um assistente que auxiliará na configuração. Esse assistente é chamado, na maioria dos casos, de "*Wizard*" ou "Assistente".

DICA

Utilize o assistente "*Wizard*" apenas em rede com estruturas básicas como, por exemplo, a rede que está sendo apresentada, pois o assistente não trata das configurações avançadas do AP.

Guarde bem essas informações! Elas farão a diferença na hora de utilizar o assistente. Vamos ao exemplo!

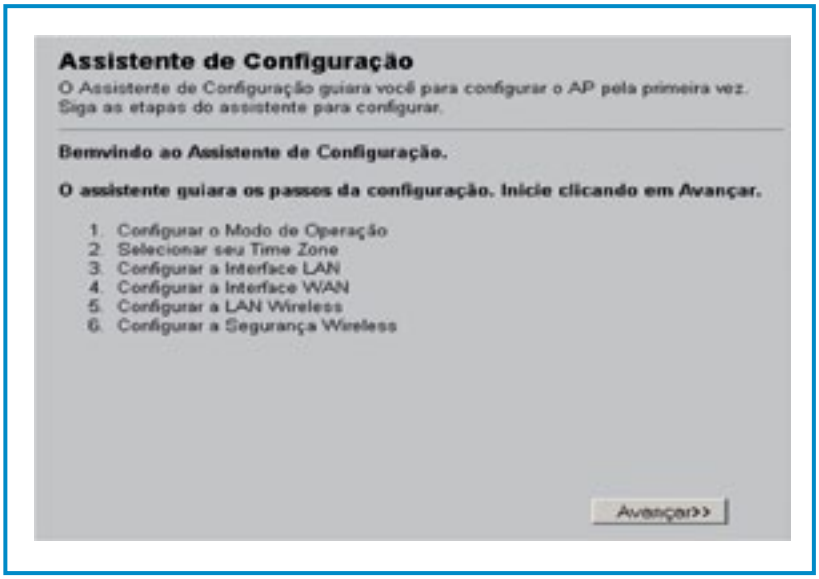


Figura 51: Exemplo de assistente de configuração
Fonte: AP Router (2011).

Algumas configurações não estão dispostas no assistente, como canal e frequência de transmissão, que devem ser configurados de acordo com os dispositivos que farão parte da rede. A seguir confira uma lista com as configurações que devem ser analisadas ao se configurar uma rede sem-fio. Vamos aos itens!

1. Configurar SSID.
2. Ativar/Desativar a opção "*broadcast* SSID".
3. Configurar um canal de comunicação.
4. Configurar a frequência do sinal.
5. Cliente ou não de um servidor DHCP.
6. Tipo de criptografia e sua respectiva autenticação (de preferência WPA).

Ao fazer e salvar essas configurações no AP, sua rede estará pronta. Agora basta configurar a autenticação nos dispositivos que terão acesso a essa rede.

A seção que você acabou de estudar, trouxe informações importantes para que você possa desempenhar sua função técnica com pleno conhecimento do assunto. Não fique com dúvidas, converse com seu professor, retorne ao conteúdo quando vezes achar necessário. Assim, você poderá acompanhar o próximo assunto com tranquilidade fazendo as devidas conexões entre as seções já estudadas.

SEÇÃO 3
Roteamento

Como você pôde ver na unidade de estudo 1, dentro de uma rede ou sub-rede, os dispositivos se comunicam se existir necessidade de equipamentos intermediários (roteadores). Caso o *host* de destino estiver em outra rede, o pacote deverá ser entregue ao roteador da sua rede local, que possui o papel de *gateway* da rede local para alcançar outros *hosts* de redes remotas.

Mas como não é possível saber a rota para todas as redes, principalmente na internet, utiliza-se um *gateway* padrão para encaminhar um pacote para fora da sua rede local. Esse roteador verificará em sua tabela de roteamento se há uma entrada para o endereço de destino do pacote ou uma rota padrão e encaminhar o pacote para outro roteador.

Uma vez que a porção de rede do endereço de destino for diferente da porção de rede do endereço de origem, significa que o pacote deverá ser encaminhado para outra rede (pois não faz parte da rede local), através do *gateway* padrão. Este deverá ser configurado nas conexões de rede, conforme figura seguinte.

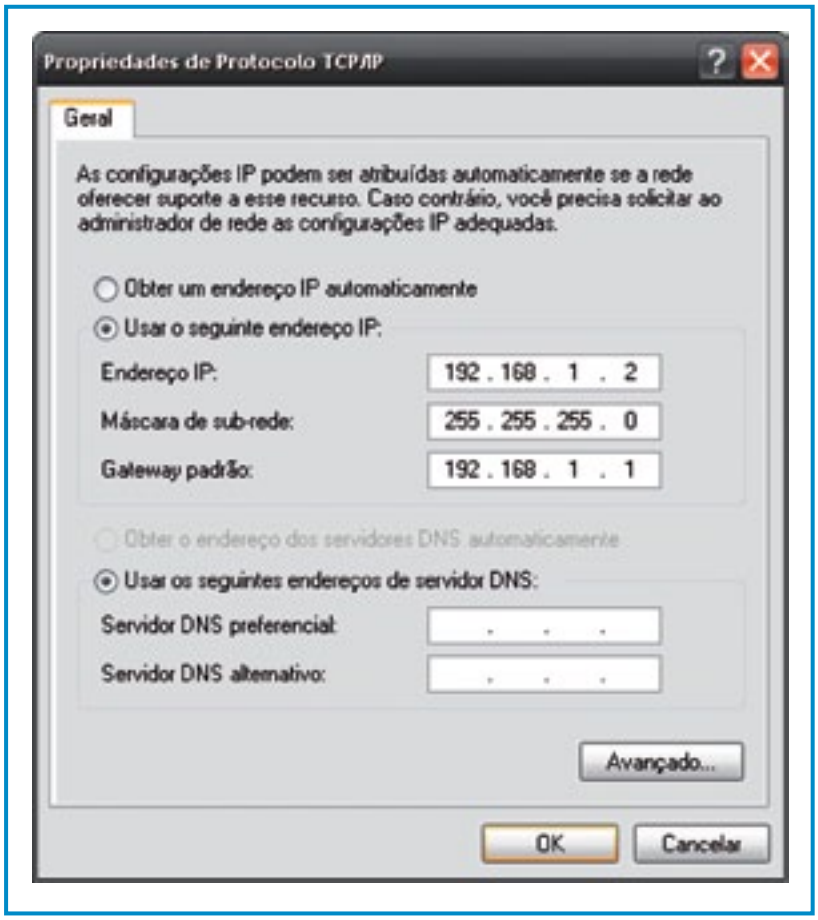


Figura 48: Configuração de conexão de rede

As configurações de rede podem ser visualizadas no Prompt de Comando do Windows, por meio do comando ipconfig, ou ainda, ipconfig /all, para visualizar todos os parâmetros de rede.

Observe que a cada salto as decisões de encaminhamento são baseadas nas informações do cabeçalho IP. Sendo assim, o roteador recebe o pacote, desencapsula até a camada 3, lê as informações do cabeçalho IP e baseado no endereço IP de destino, busca uma entrada na tabela de roteamento. Caso não encontre nenhuma entrada e nenhuma rota padrão (*gateway* para outro roteador), o pacote será descartado e um aviso de rede não alcançável será enviado. Mas, uma vez que existe uma rota e o caminho é selecionado, o pacote deverá ser novamente encapsulado. Nesse caso, o tempo TTL é diminuído, pois um novo valor Checksum do cabeçalho será calculado (pois houve alteração) e repassado à camada de enlace para, em seguida, ser entregue à camada física e transformado em *bits*.

Por que o roteador é tão importante?

O que faz do roteador um dispositivo importante na estrutura de redes e consequentemente, na internet, é a sua capacidade de tomar decisões para onde deve encaminhar um pacote. Essa decisão é realizada em cima da sua tabela de roteamento. Assim, como dispositivos finais, os roteadores também adicionam rotas para as redes conectadas à sua tabela de roteamento. Um roteador conectado a duas redes locais, por exemplo, terá duas entradas em sua tabela de roteamento, conhecendo assim o início e o término de cada rede conectada diretamente a ele.

Para outras redes (redes remotas), é necessário adicionar essas rotas. Elas podem ser aprendidas manualmente, quando um administrador configura manualmente as rotas no roteador, ou dinamicamente, quando são aprendidas automaticamente, utilizando-se de um protocolo de roteamento.

Perceba que uma rota para uma rede remota deve sempre apontar para a um próximo salto, ou seja, para o endereço IP do roteador ao qual está conectado diretamente.

No exemplo da próxima figura, o roteador local está conectado a outro roteador pela rede 192.168.1.0/24. Para alcançar as redes remotas 10.1.1.0/24 e 10.1.2.0/24, deve-se criar as rotas para essas redes apontando para o endereço do roteador remoto (192.168.1.2).

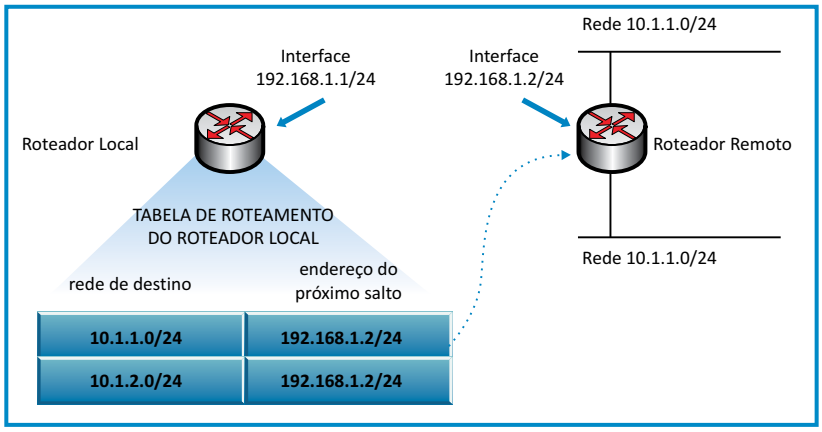


Figura 49: Tabela de roteamento

Uma tabela de roteamento estática não recebe muitas atualizações, diferentemente da tabela de roteamento dinâmica, que pode receber atualizações caso uma rede remota ou links deixem de estar disponíveis. Em redes com vários roteadores e redes, faz-se necessário a utilização de protocolos de roteamento dinâmico para manter sempre atualizadas as tabelas de roteamento de todos os roteadores com informações precisas.

Quais são os principais protocolos de roteamento? Qual sua função?

Veja!

Os principais protocolos de roteamento são:

- *Routing Information Protocol (RIP).*
- *Enhanced Interior Gateway Routing Protocol (EIGRP).*
- *Protocolo OSPF.*

Os protocolos de roteamento fornecem tabelas de roteamento atualizadas aos roteadores, acrescentando um custo adicional na rede. Primeiro, a troca de informações de rotas adiciona *overhead*, que consome a largura de banda da rede. Esse *overhead* pode ser um problema, especialmente para os *links* de baixa largura de banda entre os roteadores. Em segundo lugar, as informações de rotas que um roteador recebe são processadas intensivamente por protocolos como EIGRP e OSPF, para criar as entradas na tabela de roteamento. Isso significa que os roteadores que empregam esses protocolos precisam ter capacidade de processamento suficiente tanto para implementar os algoritmos dos protocolos como para realizar o roteamento e encaminhamento dos pacotes em tempo hábil.

Mas observe que é importante fazer um planejamento de toda a rede antes de optar ou escolher o modo de roteamento utilizado e, se caso for dinâmico, por qual protocolo escolher.

O roteamento estático não introduz sobrecarga adicional à rede, diferente do dinâmico, que é necessário para os protocolos interagirem entre os roteadores e trocarem informações sobre tabelas de roteamento. Em contrapartida, o roteamento dinâmico pode reagir rapidamente a mudanças na rede, sem a intervenção de um administrador.

Interface dos roteadores

Conforme você estudou nas seções anteriores, existem três tipos básicos de conexão em um roteador, que são:

- interfaces de redes de longa distância (WAN);
- interfaces de redes locais (LAN);
- interfaces de configuração (CONSOLE/AUX).

Veja na figura a seguir!

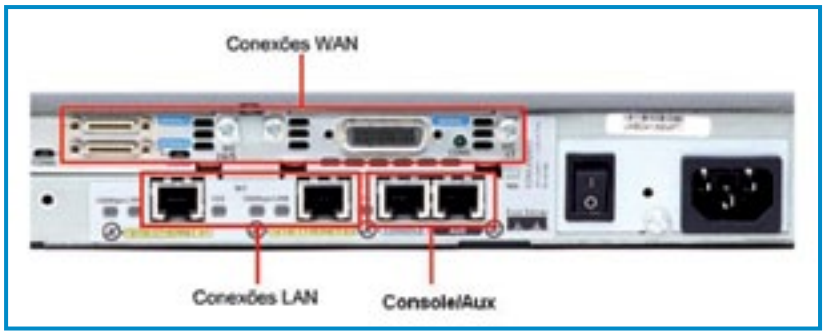


Figura 50: Interfaces de um roteador

Pronto para estudar cada uma delas?

As interfaces LAN: permitem que você conecte o roteador à rede local de trabalho. A tecnologia mais comumente utilizada nestes casos é a *Ethernet*.

As interfaces WAN: estabelecem conexão entre a interface do roteador e uma rede distante, passando por um provedor de serviços.

Interfaces de gerenciamento: possuem uma função diferente das demais, fornecendo uma conexão baseada em modo texto, que permitem que se configure ou resolva problemas no roteador. As portas utilizadas para este fim são as consoles e as auxiliares, onde pode ser conectado um cabo do roteador à porta COM (serial) do computador. Com a ajuda de um emulador de terminal, você poderá ter acesso às configurações do roteador.

Está claro até aqui? Agora, confira algumas configurações importantes que podem ser feitas em um roteador, por meio de um emulador de terminal.

Configuração de interfaces

Para colocar um roteador em rede, um dos primeiros passos é atribuir o endereço IP de cada interface de acordo com a necessidade de cada rede. Para exemplificar, acompanhe a seguir como endereçar as interfaces seriais de dois roteadores para que se comuniquem, conforme mostra a figura seguinte.

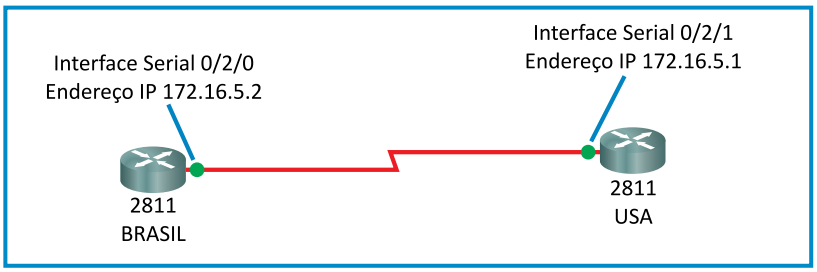


Figura 51: Topologia de exemplo

Como você pode perceber, os dois roteadores estão conectados pelas suas portas seriais, onde o roteador "BRASIL" está conectado na interface serial 0/2/0 e o roteador "USA", na serial 0/2/1.

> Para configurar o endereçamento IP, você precisa primeiro, saber em qual interface esse endereço será atribuído como interface *Fast-ethernet*, *Gigabit-ethernet* ou interface serial.

No exemplo da figura anterior os roteadores estão conectados pelas suas interfaces seriais.

Observe no quadro a seguir, como se configuraram os roteadores mostrados na figura anterior, para que estabeleçam uma comunicação.

Configuração do roteador "BRASIL"

```
BRASIL>enable
Password:
BRASIL#configure terminal
BRASIL(config)#interface serial 0/2/0
BRASIL(config-if)#ip address 172.16.5.2 255.255.255.0
BRASIL(config-if)#clock rate 56000
BRASIL(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/2/0, changed state to down
BRASIL(config-if)#
BRASIL#
```

Figura 52: Configurando endereço IP

Onde

- BRASIL>*enable* = comando utilizado para entrar com usuário privilegiado.
- *Password*: = solicitação de senha.
- BRASIL# = logado como usuário privilegiado.
- BRASIL#*configure terminal* = entrar no modo de configuração.
- BRASIL(config)#*interface serial* 0/2/0 = interface do roteador a ser configurada.
- BRASIL(config-if)#ip *address* 172.16.5.2 255.255.255.0 = atribuição de endereço IP.
- BRASIL(config-if)#*clock rate* 56000 = velocidade de comunicação no *link*.
- BRASIL(config-if)#*no shutdown* = comando para ativar a interface.
- %LINK-5-CHANGED: *Interface Serial*0/2/0, *changed state to down* = xxxx.
- BRASIL(config-if)# *exit* = sair da configuração de interface.
- BRASIL# = início.

Agora que você estudou as configurações no roteador "BRASIL", é hora de executar o comando show running-config. Esse comando mostra as configurações atuais do roteador.

Ao executar o comando show running-config, observe que, em algum ponto, as seguintes linhas estão descritas com as informações configuradas anteriormente. Agora, o endereço IP 172.16.5.2 está atribuído a interface serial 0/2/0.

```
...
interface FastEthernet0/0
ip address 172.16.5.1 255.255.255.0
...
```

Figura 53: Verificação de configuração

Configuração do roteador "USA"

Para configurar o endereço IP no roteador "USA" você deve seguir, exatamente, os mesmo passos que foram feitos para configurar o roteador "BRASIL". Porém, aqui, você deve ficar atento à interface e ao endereço IP de cada roteador, que são diferentes um do outro.

DICA

No roteador "USA" não deve ser definido o clock rate, pois esta configuração define o padrão da frequência a ser utilizada na comunicação. Quando os roteadores são conectados através de *modem*, ele é o responsável pela definição da velocidade de comunicação. Peça orientação ao instrutor sobre quais cabos você deve utilizar nestas conexões.

Ao executar o comando no shutdown no roteador "USA" aparecerá a seguinte mensagem: "*%LINK-5-CHANGED: Interface Serial* 0/2/1, *changed state to up*". Isto quer dizer que os dois roteadores estão se comunicando.

Para testar se realmente os dois roteadores estão configurados e se comunicando corretamente, basta executar o comando *ping* seguido do endereço IP do roteador remoto no caso "USA", conforme mostra a figura a seguir.

```
BRASIL#ping 172.16.5.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.5.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 19/28/32 ms

BRASIL#
```

Figura 54: Teste de comunicação entre os roteadores

Onde

BRASIL#*ping* 172.16.5.1 = comando utilizando para testar a comunicação.

Type escape sequence to abort.

Sending 5, 100-*byte* ICMP *Echos to* 172.16.5.1, *timeout is* 2 *seconds*:

!!!!! = "!" simboliza que os pacotes enviados foram recebidos com sucesso.

Success rate is 100 *percent* (5/5), *round-trip min/avg/max* = 19/28/32 ms

BRASIL#

A partir de agora, veja as configurações básicas de acesso ao roteador. Está pronto para mais esta etapa? Vamos lá!

Atribuição de nome ao roteador

Esta configuração serve para organizar sua rede e também, para que você se localize em sua rede e não venha a configurar um roteador achando que está configurando outro. Parece ser algo improvável, mas ao se montar uma rede você terá que configurar vários roteadores e nomeá-los. Esse procedimento pode auxiliar a evitar futuros transtornos.

Para isso, primeiramente, verifique se o roteador está conectado ao computador. Em seguida, abra um simulador de terminal, acesse o roteador e então, siga as configurações apresentadas na figura seguinte.

```
Router>enable

Router#configure terminal

Router(config)#hostname BRASIL

BRASIL(config)#exit

BRASIL#
```

Figura 55: Configurando nome no roteador

Onde

- *Router>enable* = comando utilizado para entrar com usuário privilegiado.
- *Router#configure terminal* = entrar no terminal de configuração do roteador.
- *Router(config)#hostname* BRASIL = comando utilizado para definir o nome do *host*.

OBS: Perceba que o nome do roteador mudou de *Router* para "BRASIL".

BRASIL(*config*)#*exit* = comando utilizada para retornar ao ponto anterior.

BRASIL# = ponto inicial.

Configuração de senha para acesso via *telnet*

Frequentemente você precisará acessar o roteador e não estará próximo do mesmo. Com isso, você terá de acessá-lo, remotamente, e uma das formas de se fazer isso é via *telnet*. E é claro que você não quer que qualquer pessoa tenha acesso ao seu roteador, pelo menos sem se autenticar no mesmo. Sendo assim, é necessário configurar uma senha para o acesso via *telnet*, como mostra a figura a seguir:

```
Router>enable

Router#configure terminal

Router(config)#line vty 0 4
Router(config-line)#password
Router(config-line)#login
```

Figura 56: Configurando senha em *line* vty

Onde

- *Router>enable* = comando utilizado para entrar com usuário privilegiado.
- *Router#configure terminal* = entrar no terminal de configuração do roteador.
- *Router(config)#line* vty 0 4 = acessando as linhas vty de 0 a 4.
- *Router(config-line)#password.*
- Teste123 = definição de senha para vty de 0 a 4.
- *Router(config-line)#login* = ativando senhas.

A partir de agora, ao tentar acessar o roteador através das linhas de 0 a 4, a senha teste123 terá de ser digitada para liberar o acesso. Percebeu como foi fácil?

Senha de ativação e segredo de ativação

São utilizados a fim de restringir a acesso ao modo privilegiado. A senha de ativação só é utilizada caso o segredo de ativação não esteja ativo. É altamente aconselhável que o segredo de ativação seja sempre utilizado, pois ele é criptografado, ao contrário da senha de ativação, que é em texto plano, ou seja, não faz uso da criptografia. O quadro a seguir mostra como ativar as senhas de ativação.

```
Router(config)#enable password
123456
Router(config)#enable secret
123456
```

Figura 57: Configurando senhas de ativação

Onde

- *Router(config)#enable password* 123456 = ativação de senha.
- *Router(config)#enable secret* 123456 = ativação de senha.

Para verificar as configurações de senha utilize o comando show runningconfig, no modo de execução privilegiado. Repare que, dentre as informações obtidas no resultado do comando show running-config, uma delas é, justamente, sobre as senhas recém-configuradas, como mostra o quadro a seguir:

```
!
!

enable secret 5 $1$mERr$H7
PDxl7VYMqaD3id4jJVK/

enable password 123456

!
!
```

Figura 58: Senhas ativadas

Observe que, na figura anterior, em uma das linhas, a senha está sendo mostrada em texto plano, ou seja, sem a utilização de nenhuma criptografia. Para resolver este problema, utilize o comando *service password* encryption, no modo de execução privilegiado. Em seguida, execute, novamente, o comando *show running-config* e observe que, agora, ambas as senhas estão criptografadas. .

```
!
!

enable secret 5 $1$mERr$H7PDxl7V
YMqaD3id4jJVK/

enable password 7
08701E1D5D4C53

!
!
```

Figura 59: Senhas ativadas e criptografadas

E o próximo passo?

O próximo passo é verificar se as configurações funcionaram. Para isso, em *Router#* digite o comando *exit* e você retornará para *Router>*. Agora digite o comando enable e, se tudo foi configurado corretamente, o sistema pedirá uma senha de autenticação e, ao digitá-la, corretamente, você se logará como usuário privilegiado.

```
Router >enable

Password:

Router #
```

Figura 60: Teste de autenticação no roteador

Onde

Router>enable = comando utilizado para entrar com usuário privilegiado.

Password: = solicitação de senha.

BRASIL# = logado como usuário privilegiado.

As demonstrações anteriores são apenas configurações básicas de um roteador. Para ter o domínio das configurações de um roteador é necessário muito estudo e dedicação.

Então, vamos seguir com as configurações de *banners* de *login*!

Configuração de *banners* de *login*

Esta configuração é utilizada a fim de deixar uma mensagem para todos os usuários que venham a ter acesso ao roteador. Na maioria das vezes, estas mensagens são de alertas, avisando sobre áreas restritas e suas penalidades como, por exemplo, "este sistema é particular e o acesso só é permitido perante autorização".

O quadro seguinte mostra como ativar um banner de login:

```
Router>enable

Password:

Router#configure terminal

Router(config)#banner motd # "Este
sistema e particular, o acesso so e
permitido perante autorização"#

Router(config)#

Router#
```

Figura 61: Ativando *banner* de *login*

Ao tentar logar novamente no roteador, verifique que a mensagem configurada anteriormente, aparecerá novamente.

Comando *show*

Você sabe o que é o comando *show*?

O comando *show*, seguido de uma especificação, serve para mostrar valores de determinadas configurações dos roteadores ou verificar o status do funcionamento do roteador. Este comando é recomendado caso você precise verificar se alguma configuração foi aplicada corretamente ou, até mesmo, para fazer consultas às configurações existentes no roteador. Acompanhe, a seguir, uma lista com alguns comandos *show* que podem ser utilizados.

- *Show clock:* mostra o horário definido no roteador.
- *Show hosts*: mostra uma lista, em cache, dos nomes e endereços dos *hosts*.
- *Show users*: exibe todos os usuários que estão conectados ao roteador.
- *Show history*: exibe um histórico dos comandos que foram inseridos.
- *Show flash*: exibe informações sobre a memória flash e quais arquivos do IOS estão armazenados nela.
- *Show version*: exibe informações sobre a versão do *software* carregado no momento, além de informações de *hardware* e dispositivo.
- *Show startup-config*: exibe o conteúdo da NVRAM, se presente e válido, ou exibe o arquivo de configuração apontado pela variável de ambiente CONFIG_FILE.
- *Show running-config*: exibe o conteúdo do arquivo de configuração em execução ou o arquivo de configuração para uma interface específica.

Esta unidade de estudo chega ao fim, e todo conteúdo estudado permite que você experimente toda esta teoria de forma prática agregando valor a sua experiência profissional.

Finalizando

O profissional que atua com montagem e manutenção de computadores deve identificar necessidades e propor soluções tecnológicas para garantir a conectividade de redes de computadores de pequeno, médio e grande porte. Neste sentido, buscamos apresentar neste livro um conjunto de conceitos e tecnologias que possam auxiliá-lo nesta jornada.

Entendemos que esta não deve ser a única fonte de consulta utilizada no desenvolvimento de suas atividades profissionais, embora a maioria dos equipamentos disponíveis no mercado tenha aplicações que utilizem os mesmos conceitos de funcionamento. Manuais técnicos, catálogos de fabricantes de componentes e equipamentos e livros didáticos são fontes de consulta muito importantes para o seu desenvolvimento profissional.

Gostaríamos também de ressaltar que a evolução tecnológica acontece rapidamente nesta área, com novos tipos de protocolos, equipamentos e soluções de *hardware* e *software*. Essa evolução exige atualização constante do profissional. Neste sentido, esteja disposto a buscar novos conhecimentos e aperfeiçoar suas habilidades continuamente, de acordo com os seus objetivos pessoais e profissionais e com as necessidades do mercado de trabalho.

Sucesso!

Referências

- AP ROUTER. **Ativando/Desativando o SSID.** 2010. Disponível em: <http://www.aprouter.com.br/simulador/v7_3-sim/home.html>. Acesso em: 10 abr. 2010.
- BAIXAKI. **Exemplo de Rede Sem Fio.** Disponível em: <http://www.baixaki.com.br/imagens/materias/rede_wireless_artigo_1.jpg>. Acesso em: 19 abr. 2011.
- BATISTA, L. G. **Cabo de rede**. 2009. Disponível em: <http://blogdoluguta.files.wordpress.com/2009/10/cabo20rede.jpg>. Acesso em: 23 fev. 2011.
- CISCO. **Exemplo de comunicação *Frame Relay*.** [200?] Disponível em: <http://www.cisco.com/en/US/i/Other/cpress_ill/CT_-_Mar_2002/IT841003.jpg>. Acesso em: 20 abr. 2011.
- DATACENTER CERN. Disponível em: <http://upload.wikimedia.org/wikipedia/commons/9/98/Cern_datacenter.jpg>. Acesso em: 25 abr. 2011.
- DIÓGENES, Y. **Certificação Cisco:** CCNA 4.0: guia de certificação para o exame 640-801.3. ed. Rio de Janeiro: Axcel Books, 2004. 408 p.
- ENGST, Adam C. **Kit do iniciante em redes sem fio:** o guia prático sobre redes Wi-Fi para Windows e Macintosh. 2. ed. São Paulo, SP: Pearson Education, Makron Books, 2005. xviii, 277 p.
- IETF. **Internet Protocol**. Disponível em: <http://www.ietf.org/rfc/rfc791.txt>. Acesso em: 20 abr. 2011.
- IMG47502A67.PNG. Disponível em: <http://img230.imageshack.us/img230/9778/img47502a67.png>. Acesso em: 10 fev. 2011.
- INFOWESTER. **Exemplo de ISDN BRI.** [200?a]. Disponível em: <http://www.infowester.com/img_art/isdn_bri.jpg>. Acesso em: 20 abr. 2011.
- _____. **Exemplo de ISDN PRI.** [200?b]. Disponível em: <http://www.infowester.com/img_art/isdn_pri.jpg>. Acesso em: 20 abr. 2011.
- NETSTUMBLER. **Exemplo de Tela do NetStumbler.** Disponível em: <http://invinceble.files.wordpress.com/2006/11/netstumbler_big.jpg>. Acesso em: 10 abr. 2011.
- NICK NETWORK. **Soluções corporativas**. Disponível em: <http://www.nicknetwork.com.br/imagens/i_solucoescorporativas.jpg>. Acesso em: 10 fev. 2011.
- SAMPAIO, Edson. **Exemplo de Criptografia Assimétrica**. 2004. Disponível em: <http://www.devmedia.com.br/articles/viewcomp.asp?comp=10717&hl= > Acesso em: 10 dez. 2009.
- SANCHES, Carlos Alberto. **Projetando redes WLAN**: conceitos e práticas. Rio de Janeiro: Érica, 2005. 342p.
- SKYPE. Disponível em: <http://info.abril.com.br/aberto/infonews/fotos/skype-20090414201439.png>. Acesso em: 25 abr. 2011.

- SOARES, Luiz Fernando G.; SOUZA FILHO, Guido Lemos de; COLCHER, Sérgio. **Redes de computadores**: das LANs, MANs e WANs às redes ATM. 2. ed. rev. e ampl. Rio de Janeiro, RJ:Campus, 1995. 705 p.

- STAFFORD, Edward. **Ether Rollover Cable**. Figura 2. Disponível em: <http://www.webstafford.com/NETWORK/ether_rollover_cable.htm>. Acesso em: 22 fev. 2011.

- TANENBAUM, Andrew S. **Redes de computadores.** Rio de Janeiro, RJ: Campus, Elsevier, c2003. xvi, 945 p.

- WIKIPÉDIA. **Exemplo de símbolos utilizados na prática do warchalking.** [200?] Disponível em: <http://pt.wikipedia.org/wiki/Ficheiro:Warchalking.svg>. Acesso em: 28 abr. 2010.

- _____. **Internet Protocol Suite**. Disponível em: <http://en.wikipedia.org/wiki/Internet_Protocol_Suite>. Acesso em: 25 abr. 2011.

Equipe de Desenvolvimento de Recursos Didáticos

Coordenação de Educação a Distância
Beth Schirmer

Coordenação Projetos EaD
Maristela de Lourdes Alves

Coordenação de Desenvolvimento de Recursos Didáticos
Gisele Umbelino

Projeto Educacional
Angela Maria Mendes
Israel Braglia

Projeto Gráfico
Daniela de Oliveira Costa
Jordana Paula Schulka
Juliana Vieira de Lima

Design Educacional
Rozangela Aparecida Valle

Capa, Ilustrações, Tratamento de Imagens
D'imitre Camargo Martins
Diego Fernandes
Luiz Eduardo Meneghel

Diagramação
Flávia Akemi Ito

Revisão e Fechamento de Arquivos
Daniela de Oliveira Costa
Juliana Vieira de Lima

Revisão Ortográfica e Normatização
SENAI/SC em Jaraguá do Sul