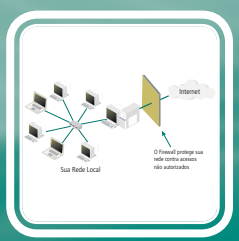
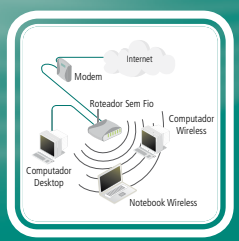
rede e-Tec Brasil

Protocolos e Serviços de Redes

Renan Osório Rios

Curso Técnico em Informática





INSTITUTO FEDERAL
ESPÍRITO SANTO

UNIVERSIDADE FEDERAL
DE SANTA CATARINA

Ministério da Educação

Protocolos e Serviços de Redes

Renan Osório Rios

Colatina - ES
2012

Presidência da República Federativa do Brasil

Ministério da Educação

Secretaria de Educação a Distância

Este Caderno foi elaborado em parceria entre o Instituto Federal de Educação, Ciência e Tecnologia do Espírito Santo e a Universidade Federal de Santa Catarina para a Rede Escola Técnica Aberta do Brasil – e-Tec Brasil.

Equipe de Elaboração
Instituto Federal de Educação, Ciência e Tecnologia do Espírito Santo – IFES

Coordenação Institucional
Guilherme Augusto de Morais Pinto/IFES
João Henrique Caminhas Ferreira/IFES

Coordenação do Curso
Allan Francisco Forzza Amaral/IFES

Professor-autor
Renan Osório Rios/IFES

Comissão de Acompanhamento e Validação
Universidade Federal de Santa Catarina – UFSC

Coordenação Institucional
Araci Hack Catapan/UFSC

Coordenação do Projeto
Silvia Modesto Nassar/UFSC

Coordenação de Design Instrucional
Beatriz Helena Dal Molin/UNIOESTE e UFSC

Coordenação de Design Gráfico
André Rodrigues/UFSC

Design Instrucional
Gustavo Pereira Mateus/UFSC

Web Master
Rafaela Lunardi Comarella/UFSC

Web Design
Beatriz Wilges/UFSC
Mônica Nassar Machuca/UFSC

Diagramação
Bárbara Zardo/UFSC
Juliana Tonietto/UFSC
Marília C. Hermoso/UFSC
Nathalia Takeuchi/UFSC

Revisão
Júlio César Ramos/UFSC

Projeto Gráfico
e-Tec/MEC

R586p Rios, Renan Osório

Protocolos e serviços de redes: curso técnico em informática / Renan Osório Rios. – Colatina: CEAD / Ifes, 2011.
87 p. : il.

ISBN: 978-85-62934-36-0

1. Redes de computação - Protocolos. 2. TCP/IP (Protocolo de rede de computação). 3. Sistemas de comunicação sem fio. 4. Material didático. I. Instituto Federal do Espírito Santo. II. Título.

CDD: 004.62

Apresentação e-Tec Brasil

Prezado estudante,

Bem-vindo ao e-Tec Brasil!

Você faz parte de uma rede nacional pública de ensino, a Escola Técnica Aberta do Brasil, instituída pelo Decreto nº 6.301, de 12 de dezembro 2007, com o objetivo de democratizar o acesso ao ensino técnico público, na modalidade a distância. O programa é resultado de uma parceria entre o Ministério da Educação, por meio das Secretarias de Educação a Distancia (SEED) e de Educação Profissional e Tecnológica (SETEC), as universidades e escolas técnicas estaduais e federais.

A educação a distância no nosso país, de dimensões continentais e grande diversidade regional e cultural, longe de distanciar, aproxima as pessoas ao garantir acesso à educação de qualidade, e promover o fortalecimento da formação de jovens moradores de regiões distantes, geograficamente ou economicamente, dos grandes centros.

O e-Tec Brasil leva os cursos técnicos a locais distantes das instituições de ensino e para a periferia das grandes cidades, incentivando os jovens a concluir o ensino médio. Os cursos são ofertados pelas instituições públicas de ensino e o atendimento ao estudante é realizado em escolas-polo integrantes das redes públicas municipais e estaduais.

O Ministério da Educação, as instituições públicas de ensino técnico, seus servidores técnicos e professores acreditam que uma educação profissional qualificada – integradora do ensino médio e educação técnica, – é capaz de promover o cidadão com capacidades para produzir, mas também com autonomia diante das diferentes dimensões da realidade: cultural, social, familiar, esportiva, política e ética.

Nós acreditamos em você!

Desejamos sucesso na sua formação profissional!

Ministério da Educação
Janeiro de 2010

Nosso contato
etecbrasil@mec.gov.br

Indicação de ícones

Os ícones são elementos gráficos utilizados para ampliar as formas de linguagem e facilitar a organização e a leitura hipertextual.

Atenção: indica pontos de maior relevância no texto.

Saiba mais: oferece novas informações que enriquecem o assunto ou "curiosidades" e notícias recentes relacionadas ao tema estudado.

Glossário: indica a definição de um termo, palavra ou expressão utilizada no texto.

Mídias integradas: sempre que se desejar que os estudantes desenvolvam atividades empregando diferentes mídias: vídeos, filmes, jornais, ambiente AVEA e outras.

Atividades de aprendizagem: apresenta atividades em diferentes níveis de aprendizagem para que o estudante possa realizá-las e conferir o seu domínio do tema estudado.

Sumário

Palavra do professor-autor

Olá, estudante!

Bem-vindo ao conteúdo da disciplina **Protocolos e Serviços de Redes**!

Para implantar soluções em redes de computadores é necessário estar sempre atualizado. Mas se você não tem experiência com redes de computadores, não se preocupe! O caminho do conhecimento exige tempo, persistência e disciplina. O seu maior aliado é você mesmo. Faço essa afirmação, pois quando entrei no curso superior de Informática, havia tido meu primeiro computador e, portanto, foi o meu primeiro contato com o mundo da informática. Posso resumir o dia a dia de um profissional de TI com a seguinte frase "a vida é um eterno *upgrade*", espero que você possa aprender o máximo e aproveitar esta grande oportunidade.

A diferença do estudante em um curso a distância e o presencial está na força de vontade de ambos, isso varia de um para outro. Não adianta estar presente na sala e não estudar. Você faz a diferença. Logo, faça a diferença e seja o melhor!

Um forte abraço!

Professor Renan Osório Rios

Apresentação da disciplina

A disciplina Protocolos e Serviços de Redes é indispensável para o profissional de redes. Portanto, ela é de fundamental importância para o curso. Nesta disciplina, o aluno aprenderá os principais protocolos e serviços de rede que estão sendo utilizados no mercado. Além disso, essa área não para de crescer e demandar um profissional cada vez mais capacitado.

Este curso oferecerá a você, estudante, material impresso e virtual de aprendizagem. Em ambos haverá teoria e variadas atividades para fixação do conhecimento.

Para sanar qualquer dúvida, você poderá acionar o tutor a distância e, sempre que necessário, poderá solicitar que ele entre em contato com o professor. Além disso, temos à nossa disposição um ambiente virtual cheio de recursos para nos auxiliar nesse processo.

Aprenda o máximo que o curso Técnico em Informática que o Instituto Federal de Educação, Ciência e Tecnologia do Espírito Santo (IFES) lhe oferece. O mercado de Tecnologia da Informação possui muitas áreas. Qual você seguirá?

Bons estudos e sucesso profissional!

Projeto instrucional

Disciplina: **Protocolos e Serviços de Redes (Carga Horária: 60hs).**
Ementa: Aplicações e serviços TCP/IP.

AULA	OBJETIVOS DE APRENDIZAGEM	MATERIAIS	CARGA HORÁRIA (horas)
1. Introdução a protocolos e serviços de redes	- Conhecer os conceitos básicos da disciplina Protocolos e Serviços de Rede. - Relacionar a evolução da internet ao número de computadores das últimas décadas. - Analisar o cenário amplo em que o profissional da área de redes pode atuar. - Conhecer a importância do compartilhamento de recursos em uma rede de computadores. - Conhecer os principais recursos que estão sendo utilizados na internet.	Vídeos do programa "Olhar Digital" com os temas: • Você fala inglês? • O que as empresas procuram no profissional de TI. • Profissões do futuro e computação nas nuvens.	10
2. Modelo de referência TCP/IP	- Conhecer o modelo que nasceu na internet e funciona nela. - Compreender as principais aplicações utilizadas nas redes de computadores. - Conhecer as portas de comunicação dos protocolos. - Compreender a importância da camada de transporte. Entender o funcionamento dos protocolos de transporte TCP e UDP. - Apresentar o protocolo IP. - Compreender o controle de *link* lógico e os principais dispositivos de rede do mercado.	Artigo do *site* "Clube do Hardware". Vídeo do programa "Olhar Digital" com o tema: Como a internet funciona. Vídeos do *site* "How Stuff Works" com o tema: Fibra óptica.	10
3. Serviços de redes para *web*	- Compreender o funcionamento dos protocolos de encaminhamento de dados IPv4 e as vantagens oferecidas pelo IPv6. - Conhecer o sistema de documentos hipermídia, WWW e http. - Compreender as funcionalidades e utilidades do protocolo FTP. - Compreender o funcionamento do DNS. - Compreender os protocolos de serviço de *e-mail* IMAP e SMTP. - Entender os protocolos de acesso remoto Telnet e SSH.	Vídeos do *site* "Antispam", do Comitê Gestor da Internet no Brasil com os temas: Navegar é preciso, Os invasores, *Spam*, Defesa e IPv6.	10

AULA	OBJETIVOS DE APRENDIZAGEM	MATERIAIS	CARGA HORÁRIA (horas)
4. Serviços de rede cliente- servidor	- Compreender a utilidade do *Gateway*. - Entender a dinâmica das funcionalidades do DHCP. - Compreender o funcionamento do *proxy*. - Compreender as utilidades e vantagens do *firewall.*	Vídeos do programa "Olhar Digital" com os temas: *firewall*e *proxy*.	10
5. Serviços de redes WAN	- Conhecer a tecnologia de rede de alta velocidade ATM. - Demonstrar como funciona a tecnologia de banda larga mais utilizada no Brasil, ADSL. - Compreender o que é roteamento e roteadores. - Apresentar o que são sistemas autônomos. - Conhecer as VPNs, uma tecnologia em ascensão no mercado de TI.		10
6. Segurança em redes *Wi-Fi*	- Apresentar as redes *Wi-Fi*, seus padrões e a importância de mantê-las seguras. - Demonstrar como identificar o endereço MAC das interfaces de rede e como esse endereço pode ser usado para adicionar mais segurança em ambiente *Wireless*. - Compreender as vulnerabilidades que possui o protocolo WEP. - Conhecer as chaves de criptografia seguras WPA e WPA2.	Vídeos do programa "Olhar Digital" com os temas: Você sabe como a *Wi-Fi* funciona, *Wireless*-n e segurança em redes *Wireless*.	10

Aula 1 – Introdução a protocolos e serviços de redes

Objetivos

Conhecer os conceitos básicos da disciplina Protocolos e Serviços de Rede.

Relacionar a evolução da internet ao número de computadores das últimas décadas.

Analisar o cenário amplo em que o profissional da área de redes pode atuar.

Conhecer a importância do compartilhamento de recursos em uma rede de computadores.

Conhecer os principais recursos que estão sendo utilizados na internet.

A Aula 1 apresenta o cenário que os profissionais da área da Tecnologia da Informação tem pela frente! É muito importante que o técnico de informática saiba os principais conceitos que estão sendo aplicados no mercado. Aula após aula, você estará viajando pelas redes de computadores. Boa leitura e bom estudo!

1.1 Conceitos básicos

Mas, o que são **protocolos**? Os protocolos são desenvolvidos por algoritmos, instruções bem definidas para executar uma tarefa. Os protocolos são utilizados em duas ou mais máquinas em rede, para se comunicarem. Existem vários protocolos no mundo inteiro, ao quais podem oferecer diversos serviços em uma comunicação de computadores.

A-Z

Protocolo
De acordo com Falbriard (2002, p. 63), "os protocolos utilizados em redes de comunicação definem conjuntos de regras que coordenam e asseguram o transporte das informações úteis entre dois ou mais dispositivos".

E o que são serviços de rede? São os serviços oferecidos em uma rede de computadores. Tais serviços podem ser oferecidos por diversos protocolos. Quando estamos fazendo um *download* de um arquivo pela internet, estamos utilizando um serviço de rede, normalmente proporcionado pelo protocolo *File Transfer Protocol*, que significa "Protocolo de Transferência de Arquivos", mais conhecido como FTP.

Agora que você já conheceu um pouco mais sobre protocolos e serviços de redes, responda às seguintes perguntas e comente no fórum 02 "Atividades da Aula 1".

1. O que são protocolos?

2. O que é um serviço de rede?

1.2 O crescimento das redes de computadores e a internet

Reportagem do programa "Olhar Digital", com o seguinte tema: "Mercado de TI: Você fala inglês?" http://olhardigital.uol.com.br/produtos/central_de_videos/ingles_/_mercado. É de suma importância ter noções da língua inglesa para trabalhar com informática, principalmente na área de redes. Comente este vídeo no Ambiente Virtual de Ensino-Aprendizagem no fórum 01 "Vídeos da Aula 1".

Com o advento da internet e a quantidade de usuários que a utilizam, o tráfego na rede aumentou; por isso, novos protocolos estão sendo propostos e muitos protocolos antigos estão sendo revisados para não deixarem de ser utilizados. São oferecidos diversos serviços em uma rede de computadores, entre os quais podemos perceber nos últimos anos um aumento significativo nos serviços de telefonia e vídeo.

O Quadro 1.1 resume a expansão da internet e demonstra o crescimento de componentes importantes do uso de computadores.

Quadro 1.1: Expansão da internet

	número de redes	número de computadores	número de usuários	número de gerentes
1980	10	10^2	10^2	10^0
1990	10^3	10^5	10^6	10^1
2000	10^5	10^7	10^8	10^2
2005	10^6	10^8	10^9	10^3

Fonte: Comer (2006, p. 7)

Faça o trabalho abaixo e comente no fórum 02 "Atividades da Aula 1".

1. Quais fatores influenciaram no aumento do número de:

a) Redes

b) Computadores

c) Usuários

d) Gerentes

1.3 O cenário do profissional da área de TI

A área de informática é muito dinâmica e, quando falamos em tecnologia da informação, temos que ficar atentos às novidades tecnológicas. O profissional de TI pode atuar em diversas áreas da informática, as quais podem compreender tecnologias relacionadas à rede, *software*, *hardware*, etc. Vale uma dica: atue na área que você tenha maior facilidade e se sinta bem em desenvolver seu trabalho.

O foco deste caderno são os serviços de rede que os protocolos podem nos oferecer. O profissional de TI que se especializar nesta área poderá atuar em: implantação de servidores com domínio intranet ou extranet, fornecimento de soluções em *backup*, segurança, acesso remoto, etc.

Para o profissional de TI se qualificar, é necessário estudar constantemente; para isso, é necessário escolher o melhor material didático disponível no mercado. Lembre-se, seu tempo é muito precioso.

O mercado brasileiro e mundial demanda profissionais capacitados e qualificados nesta área. O que o destaca dos demais é a sua proatividade. Hoje em dia, temos muitas informações publicadas em livro e espalhadas pela internet em forma de tutoriais, artigos, fóruns, etc.

Faça o trabalho abaixo e comente no fórum 02 "Atividades da Aula 1".

1. Qual a diferença entre intranet e extranet?

2. O que é *backup*? Cite exemplos.

3. Quais tipos de segurança poderiam ser implantados em uma rede de computadores?

Reportagem do programa "Olhar Digital", com o tema: Carreira digital: Saiba como atuar na área. http://www.youtube.com/user/programaolhardigital#p/search/1/5ZZhHC0VYyw . Essa reportagem apresenta informações importantes para atuar na área da Tecnologia da Informação. Comente este vídeo no Ambiente Virtual de Ensino-Aprendizagem no fórum 01 "Vídeos da Aula 1".

1.4 Compartilhamento de recursos na rede

Das redes locais até uma rede global, podemos compartilhar recursos entre nossas máquinas. Mesmo numa rede local que não tenha acesso à internet, podemos compartilhar pastas, arquivos, impressoras, etc.

Com a internet, as possibilidades de compartilhamento nas redes de computadores aumentam. É possível trocar informações com qualquer computador do mundo que esteja conectado.

Esses recursos são possíveis por meio de protocolos que proporcionam serviços que podem ser instalados e configurados pelo profissional de TI.

Faça o trabalho abaixo e comente no fórum 02 "Atividades da Aula 1".

1. Cite três exemplos de recursos utilizados em uma rede de computadores de uma empresa. Explique-os.

1.5 Compartilhamento de serviços na internet

O compartilhamento de serviços na rede mudou a maneira de o mundo se comunicar, desde conversas *on-line* até o envio de vídeo em tempo real. As pessoas estão resolvendo suas pendências do dia a dia na internet, realizando transações bancárias, compra e venda de mercadorias e serviços, estão utilizando as redes sociais para ficar mais perto de pessoas distantes.

Enfim, tudo isso é possível, porque os protocolos proporcionam diversos serviços nas redes de computadores. É importante entendê-los e compreender o funcionamento dos principais protocolos.

Reportagem do programa "Olhar Digital", com o tema: Carreira digital: o que as empresas procuram nos candidatos? http://olhardigital.uol.com.br/produtos/central_de_videos/carreira-digital-o-que-as-empresas-procuram-nos-candidatos. Essas dicas são essenciais para o profissional de TI. Comente esse vídeo no Ambiente Virtual de Ensino-Aprendizagem no fórum 01 "Vídeos da Aula 1".

Reportagem do programa "Olhar Digital", com o tema: As profissões do futuro no mercado de TI. http://olhardigital.uol.com.br/negocios/central_de_videos/profissoes_do_futuro. É sempre importante ficar "antenado" com as novas tecnologias. As maiores empresas do mundo estão sempre inovando. Comente esse vídeo no Ambiente Virtual de Ensino-Aprendizagem no fórum 01 "Vídeos da Aula 1".

Resumo

Nesta aula, você conheceu o incrível crescimento das redes de computadores nas últimas décadas, o cenário amplo do profissional de Tecnologia da Informação (TI) no mercado e a importância do compartilhamento de recursos e serviços em redes de computadores. Portanto, esta aula é apenas o início de muito conhecimento sobre protocolos e serviços de rede que você vai aprender!

Atividades de aprendizagem

Estamos chegando ao fim da primeira aula. Resolva os exercícios abaixo, e comente no fórum 02 "Atividades da Aula 1".

1. O que são algoritmos?

2. Por que os protocolos e serviços de redes andam juntos?

3. Como é possível o profissional de TI ficar atualizado?

4. O que o mercado de trabalho exige do profissional de TI?

5. Quais os maiores desafios encontrados pelo profissional de TI no mercado?

6. Explique o que é computação em nuvens.

7. Quais aplicativos em nuvens estão funcionando no mercado?

8. Sobre a computação em nuvens, explique as seguintes afirmações:

a) Com a computação em nuvem é possível compartilhar recursos pela internet.

b) Vários serviços de rede serão disponibilizados pela computação nas nuvens.

9. Cite três exemplos de serviços que você utiliza na internet. Explique-os.

Reportagem do programa de tv "Jornal da Globo", informando sobre o "Google e a computação nas nuvens". http://www.youtube.com/watch?v=j2n4Ubc40VM. Essa nova tecnologia está despertando uma grande corrida entre as empresas de informática. Quem sairá na frente? O programa "Olhar Digital" esclarece mais este tema com a reportagem "Cloud Computing: mais fácil e acessível do que você imagina". http://olhardigital.uol.com.br/produtos/central_de_videos/cloud-computing-mais-facil-e-acessivel-do-que-voce-imagina. Comente esse vídeo no Ambiente Virtual de Ensino-Aprendizagem no fórum 01 "Vídeos da Aula 1".

Aula 2 – Modelo de Referência TCP/ IP

Objetivos

Conhecer o modelo que nasceu na internet e funciona nela.

Conhecer as principais aplicações nas redes de computadores.

Informar ao aluno as portas de comunicação dos protocolos.

Conhecer a importância da camada de transporte.

Entender o funcionamento dos protocolos de transporte TCP e UDP.

Conhecer o protocolo IP.

Compreender o controle de *link* lógico e os principais dispositivos de rede do mercado.

Nesta aula, estudaremos o modelo de referência TCP/IP e suas principais características!

2.1 Modelo TCP/IP

O modelo de referência TCP/IP foi dividido em camadas bem definidas; cada camada realiza uma tarefa de comunicação. Para estudar uma tecnologia, é importante aprender a sua história. A Advanced Research and Projects Agency ou Agência de Pesquisas em Projetos Avançados, mais conhecida como ARPANET, é tida como a propulsora da internet atual. Ela foi uma rede de pesquisa criada pelo Departamento de Defesa dos Estados Unidos em 1969.

De acordo com Tanenbaum (2003, p. 44), pouco a pouco, centenas de universidades e repartições públicas foram conectadas, usando linhas telefônicas dedicadas.

Quando foram criadas as redes de rádio e satélite, começaram a surgir problemas com os protocolos existentes, o que forçou uma nova arquitetura de referência. Mais tarde, essa arquitetura ficou conhecida como modelo de referência TCP/IP, esse modelo foi definido pela primeira vez em 1974.

Segue, no *link* http://olhardigital.uol.com.br/produtos/central_de_videos/como-a-internet-funciona, uma reportagem demonstrando como funciona a internet. Comente este vídeo no Ambiente Virtual de Ensino-Aprendizagem no fórum 03 "Vídeos da Aula 2".

O nome TCP/IP vem dos nomes dos protocolos mais utilizados deste modelo de referência, sendo eles, o *Internet Protocol* ou Protocolo de Internet, mais conhecido como IP. E o *Transmission Control Protocol* ou Protocolo de Controle de Transmissão, usualmente chamado de TCP.

O modelo TCP/IP é dividido em camadas, os protocolos das várias camadas são denominados pilha de protocolos. Cada camada interage somente com as camadas acima e abaixo. Vejamos no Quadro 2.1 o modelo de referência TCP/IP.

Quadro 2.1: Modelo de referência TCP/IP

Modelo de Referência TCP/IP
Aplicação
Transporte
Inter-redes
Host/Rede

Fonte: Tanenbaum (2011, p. 28)

Alguns livros citam que o modelo TCI/IP possui cinco camadas; outros citam que existem quatro camadas. Essa diferença está relacionada à camada de *Host*/Rede; alguns autores as dividem em outras duas camadas, sendo elas, física e enlace. Foi adotado neste caderno o modelo de quatro camadas.

O modelo OSI possui sete camadas, três camadas a mais que o modelo TCP/IP. Segue no Quadro 2.2, a comparação do modelo TCP/IP com modelo OSI.

Quadro 2.2: Comparação do modelo de referência TCP/IP com o modelo de referência OSI

Modelo de Referência TCP/IP	Modelo de Referência OSI
Aplicação	Aplicação
	Apresentação
	Sessão
Transporte	Transporte
Inter-redes	Rede
Host/Rede	Enlace de Dados
	Física

Fonte: Tanenbaum (2011, p. 30)

Você se lembra do modelo OSI? Ele foi criado pela Internacional Standards Organization ou Organização Internacional para Padronização, ISO. Você não pode confundir OSI com ISO. O modelo OSI, *Open Systems Interconnection*, ou Interconexão de Sistemas Abertos, foi criado com a finalidade de interconectar sistemas que estão abertos a outros sistemas.

Responda às seguintes perguntas e comente no fórum 04 "Atividades da Aula 2".

1. Qual foi o objetivo da ARPANET?
2. Como surgiu o TCP/IP?
3. É correto afirmar que a internet funciona sobre o modelo TCP/IP? Explique.
4. Como as camadas do modelo TCP/IP se comunicam?
5. Qual é a principal diferença entre o modelo TCP/IP e o modelo OSI?

2.2 Camada de aplicação

A camada de aplicação é a mais próxima do usuário. Os programas utilizam os protocolos da camada de aplicação, de acordo com sua finalidade, bate-papo, videoconferência, *e-mail*, etc. Ela contém muitos protocolos que asseguram uma comunicação bem-sucedida entre a heterogeneidade da internet.

Neste exato momento, vários computadores do mundo com diferentes sistemas operacionais e *softwares* aplicativos estão conectados na internet; ela é uma rede heterogênea.

Incluindo diversos protocolos, a camada de aplicação possui muitos protocolos que não são mais utilizados. A dinâmica dessa camada é muito grande; são criados vários protocolos para suprir a necessidade do tráfego na rede; consequentemente, diversos protocolos deixam de ser utilizados.

Estudaremos os principais protocolos da camada de aplicação. Seguem no Quadro 2.3 os principais protocolos da camada de aplicação e suas funções.

Quadro 2.3: Protocolos da camada de aplicação e a sua função

Protocolos da Camada de Aplicação		
Sigla	**Nome**	**Função**
HTTP	*Hypertext Transfer Protocol* ou Protocolo de Transferência de Hipertexto	Trata de pedidos e respostas entre o cliente e o servidor na internet.
FTP	*File Transfer Protocolo* ou Protocolo de Transferência de Arquivos	Transfere documentos hipermídia na internet.
SMTP	*Simple Mail Transfer Protocol* ou Protocolo de Transferência de *e-mail*	Envia *e-mail*.
IMAP	*Internet Message Access Protocol* ou Protocolo de acesso a mensagem da internet	Recebe *e-mail*.
Telnet	*Telnet*	Permite a comunicação remota entre computadores conectados em rede.

(Continua)

SSH	*Secure Shell* ou Terminal Seguro	Permite a comunicação remota entre computadores conectados em rede, utilizando criptografia.
DHCP	*Dynamic Host Configuration Protocol* ou Protocolo de configuração dinâmica de estação	Concede endereços IP e outros parâmetros dinamicamente para estações de trabalho.
DNS	*Domain Name System* ou Sistema de Nome de Domínio	É um sistema de gerenciamento de nomes hierárquico e distribuído; permite acessar outro computador na rede sem ter conhecimento do endereço IP.

(Conclusão)

Fonte: Adaptado de Tanenbaum (2011, p. 467)

Para acessar a internet é necessário um *browser* ou navegador; podemos utilizar o Mozilla, Internet Explorer, Google, Safári, etc. As páginas da *web* são requisitadas por meio do protocolo HTTP ao digitar a URL no navegador. Os programas se comunicam com a camada de Aplicação.

A *Uniform Resource Locator* ou Localizador Padrão de Recursos, URL. Normalmente é um *link* de uma página na internet, por exemplo, **http://www.ifes.edu.br**. A URL; também pode indicar o caminho em uma rede.

2.2.1 Portas de comunicação

Porta
Uma porta adapta a aplicação para que ela possa ser executada em uma plataforma computacional diferente.

Os protocolos precisam de uma **porta** para se conectar, ou seja, é utilizado um canal virtual para a transmissão dos dados.

De acordo com Scrimger et al. (2002, 102), a maioria dos sistemas operacionais mantém um arquivo que contém os números de porta e seus serviços correspondentes. "Entretanto, os valores de um número de porta podem variar, dependendo da plataforma de *hardware* ou *software* na qual o *software* do TCP é executado".

A *Internet Assigned Numbers Authory* ou Autoridade de Atribuição de Números da Internet (IANA) é responsável pela coordenação global do DNS raiz, endereçamento IP, e os protocolos da internet (IANA, 2011).

A IANA é responsável por endereçar os protocolos da internet. Seguem, no Quadro 2.4, alguns protocolos e suas respectivas portas de comunicação.

Quadro 2.4: Protocolos da camada de aplicação e suas respectivas portas padrão

Protocolos da Camada de Aplicação	
Protocolo	**Porta**
HTTP	80
FTP	21
SMTP	25
IMAP	143
Telnet	23
SSH	22
DHCP	67
DNS	53

Fonte: Adaptado de Tanenbaum (2011, p. 467)

Para obter uma lista completa dos protocolos e suas respectivas portas, consulte o *site* **http://www.iana.org/assignments/port-numbers.**

Faça a pesquisa abaixo e comente no fórum 04 "Atividades da Aula 2".

1. Qual é a função da camada de aplicação?
2. O que são portas? Para que elas servem?
3. Descreva cinco protocolos da camada de aplicação que não foram descritos no livro e suas respectivas portas.

2.3 Camada de transporte

Após processar a requisição do programa, o protocolo na camada de aplicação se comunicará com o protocolo na camada de transporte, normalmente, o *Transmission Control Protocol* ou Protocolo de Controle de Transmissão (TCP) ou o *User Datagram Protocol* ou Protocolo de Datagramas de Utilizador (UDP).

Essa camada é responsável por organizar os dados recebidos da camada de aplicação, controlar os erros e fazer o controle de fluxo fim a fim. Ela pega os dados enviados pela camada superior, os divide em segmentos ou datagramas e envia para a camada imediatamente inferior. Durante a recepção dos dados, esta camada é responsável por colocar os segmentos ou datagramas recebidos da rede em ordem.

2.3.1 TCP

O principal motivo do sucesso das aplicações da internet é o protocolo TCP. Ele se adapta a diversas finalidades exigidas pelo usuário e suas aplicações.

As principais características do TCP, de acordo com Scrimger et al. (2002) são a sua transferência de dados, robustez, controle de fluxo, multiplex, conexões lógicas e o fato de ser *full* duplex. Os termos estão descritos abaixo:

- Transferência de fluxo de dados: uma aplicação pode confirmar se todos os segmentos transferidos pelo TCP alcançaram seu destino previsto e obter retorno sobre o sucesso dessa operação.
- Robustez: o TCP do receptor agrupa os segmentos caso eles cheguem fora de ordem.
- Controle de fluxo: o receptor, à medida que recebe os segmentos, envia uma mensagem confirmando a recepção.
- Multiplex: uso paralelo das portas de comunicação.
- Conexões lógicas: são identificadas pelo processo transmissor e receptor, pela combinação dos mecanismos TCP.
- *Full* duplex: a transferência de dados pode ser simultânea em ambas as direções.

O protocolo TCP é orientado à conexão. Permite a entrega confiável dos dados, elimina segmentos duplicados e recupera dados corrompidos. Ele é um protocolo confiável e seguro.

O processo de encaminhamento de pacotes TCP é mais lento do que o UDP. Mas, quando se necessita de garantia e ordenação na entrega dos segmentos, a melhor opção e o TCP.

2.3.2 UDP

O protocolo UDP não utiliza confirmação para se certificar que os datagramas chegaram ao seu destino, não ordena as mensagens que chegam. Assim, os datagramas UDP podem ser perdidos, duplicados ou chegar fora de ordem.

O protocolo UDP não é orientado à conexão. Sua entrega não é confiável, não elimina pacotes duplicados e não faz o controle de dados corrompidos.

De acordo com Comer (2006, p. 114), o protocolo UDP fornece serviço de entrega sem conexão e não é confiável quando usa o IP para transportar datagramas entre as máquinas.

Um programa aplicativo que usa UDP aceita responsabilidade total por lidar com problemas de confiabilidade; porém, o UDP é uma ótima escolha para o fluxo de dados em tempo real, como vídeo, voz e jogos. Por não criar conexões durante uma conexão UDP ela troca menos informações do que o protocolo TCP.

O processo de encaminhamento de datagramas UDP é mais rápido do que o do TCP; muitos programas o utilizam. Os mais famosos são os programas *peer to peer*, que compartilham arquivos na rede e gerenciadores de *download*; normalmente, eles podem ser configurados para utilizar UDP, TCP ou ambos. Com a ativação do UDP, a taxa de transferência de dados aumenta na rede.

Faça o trabalho abaixo e comente no fórum 04 "Atividades da Aula 2".

1. Quais são as principais características do protocolo TCP?
2. Quais são as vantagens e as desvantagens do protocolo TCP?
3. Cite exemplos de aplicações que necessitam utilizar TCP.
4. Quais são as principais características do protocolo UDP?
5. Quais são as vantagens e desvantagens do protocolo UDP?
6. Cite exemplos de aplicações que podem de utilizar UDP.
7. Pesquise na internet dois gerenciadores de *downloads* e descreva suas características.
8. Pesquisa na internet dois compartilhadores de arquivos e descreva suas características.
9. Qual é a diferença entre gerenciador e compartilhador de arquivos?

2.4 Camada de inter-rede

O principal protocolo da camada de internet é o *Internet Protocol* ou Protocolo de Internet (IP). Ele pega os segmentos ou datagramas recebidos da camada de transporte e adiciona informações de endereçamento virtual, isto é, adiciona o endereço do computador que está enviando os pacotes e o endereço do computador que receberá os pacotes.

Para qualquer computador ter acesso à internet, é necessário ter um IP.

Esses endereços virtuais são chamados endereços IP. Em seguida, os pacotes são enviados para a camada imediatamente inferior, a camada interface com a rede. Nessa camada os pacotes são chamados de quadro ou *bits*.

Para Scrimger et al. (2002, p. 107) um endereço IP é semelhante ao endereço que você utiliza para enviar uma carta pelo correio. "O endereço deve apresentar todas as informações requeridas para que ocorra a entrega. Caso o contrário, a carta não chegará ao destino correto. Um endereço incompleto ou incorreto afeta o endereçamento IP da mesma maneira como afeta a entrega de uma carta".

Por muitos anos a internet utilizou o IP versão 4 (IPv4). Porém, a quantidade de computadores cresceu ao redor da Terra e o número IPv4 está escasso. A solução foi criar o IP versão 6 (IPv6). Com essa nova solução não haverá escassez de números IPs no mercado. Muitas empresas estão migrando aos poucos do IPv4 para o IPv6. Na Aula 5, estudaremos com maiores detalhes a diferença entre o IPv4 e o IPv6.

Responda às seguintes perguntas e comente no fórum 04 "Atividades da Aula 2".

1. Como funciona o IP?
2. Por que toda máquina precisa de um IP para se conectar à internet?

2.5 Camada de *host*/rede

A camada *host*/rede receberá os pacotes enviados pela camada de inter-rede e os enviará para a rede ou receberá os dados da rede, caso o computador esteja recebendo dados. Esta camada é responsável por detectar e corrigir erros no nível físico e controlar o fluxo entre transmissão e recepção de quadros em tecnologias de rede.

O controle do fluxo de dados na camada física é feito pelo Controle de *Link* Lógico (LLC). Essa camada detecta e corrige os erros que possam acontecer na camada física. Todo dispositivo de rede possui um endereço de *Media Access Control*, ou Controle de Acesso ao Meio (MAC). Ele é um endereço único e físico do dispositivo de rede. O Institute of Electrical and Electronics Engineers, ou Instituto de Engenheiros Eletricistas e Eletrônicos (IEEE) organiza e controla com os fabricantes de dispositivo de rede esse número. O fabricante deve garantir que não existam dispositivos de rede com MAC repetido.

Existem diversas tecnologias de rede que estão na camada *host*/rede. Atualmente, a maioria dos computadores utiliza a rede ethernet, a qual está disponível em diferentes velocidades.

As redes sem fio são redes ethernet.

O que são redes ethernet? Ethernet é o nome dado a uma tecnologia de comutação de pacotes *Local Area Network* ou Rede de Área local (LAN). Desenvolvida pela Xerox PARC no início da década de 1970, a tecnologia atual é conhecida como ethernet par trançado, como pode ser visto na Figura 2.1, pois permite que um computador se comunique utilizando fios de cobre convencionais, semelhantes aos fios utilizados para conectar telefones (COMER, 2006, p. 11).

Figura 2.1: Cabo par trançado
Fonte: http://www.forum-invaders.com.br/vb/showthread.php/31918-(Mat%C3%A9ria)Cabos-de-Transmiss%C3%A3o

Mostram-se, nas figuras 2.2, 2.3, 2.4 e 2.5, os principais dispositivos de rede encontrados mercado:

Figura 2.2: Placa de rede Ethernet
Fonte: http://imei12joana.blogspot.com/

Figura 2.3: Placa de rede sem fio
Fonte: http://www.tudoditudo.com/wp-content/uploads/2011/09/placa-de-rede-wireless3.jpg

Figura 2.4: *Switch*
Fonte: http://jilmaikelfrancisco.blogspot.com/2010/05/diferenca-entre-switch-hub-e-roteador.html

Figura 2.5: Roteador *wireless*
Fonte: Adaptado de http://www.hardware.com.br/comunidade/wireless-montar/958751/

Dentre as tecnologias de rede que estão ganhando o mercado, podemos destacar as fibras ópticas.

Faça o trabalho abaixo e comente no fórum 04 "Atividades da Aula 2".

1. Qual é a função da camada *host*/rede?
2. O que o LLC faz?
3. O que á um MAC?
4. Qual é a função do IEEE?
5. Quais são as velocidades disponíveis em dispositivos ethernet no mercado?
6. Qual é a velocidade da fibra óptica?

Resumo

A propulsora da internet foi a ARPANET. O modelo de referência TCP/IP surgiu para solucionar o problema de incompatibilidade de protocolos na rede. O modelo TCP/IP é dividido em camadas e cada camada é formada por uma pilha de protocolos. Não é possível a camada de *host*/rede se comunicar com a camada de transporte, se não houver uma comunicação com a camada de inter-redes, mas é possível a camada de transporte se comunicar com a camada de aplicação e inter-redes. Uma camada depende da outra para haver comunicação no modelo de referência TCP/IP.

A camada de aplicação é responsável por identificar e disponibilizar serviços para aplicações entre as estações em rede.

Todo protocolo precisa de uma porta, a qual é responsável por adaptar uma aplicação em plataformas diferentes. O protocolo TCP é confiável, seguro e orientado à conexão, e o protocolo UDP não é orientado à conexão. Ambos transportam os pacotes pela rede.

Diversos livros adotam nomes diferentes para os dados que trafegam nas camadas do modelo de referência TCP/IP. A camada de transporte está relacionada a datagramas "UDP" ou segmentos "TCP"; a camada inter-redes está relacionada a pacotes; e a camada *host*/rede se relaciona a quadros e *bits*. Como pudemos perceber, os dados recebem nomes diferentes em cada camada que passam.

Vídeo produzido pela How Stuff Works, explicando como funciona a fibra óptica, dividido em três partes.

Link 1: http://www.youtube.com/watch?v=ZCMKHqaLi4o>,

link 2: http://www.youtube.com/watch?v=Tc1C2_Jp9Ro> e

link 3: http://www.youtube.com/watch?v=lW7a0SWKICg.

Comente esses vídeos no Ambiente Virtual de Ensino-Aprendizagem no fórum 03 "Vídeos da Aula 2".

Para entender o melhor funcionamento dos protocolos do modelo de referência TCP/IP, segue o *link* de um vídeo produzido pela Medialab, com o nome Guerreiros da Informação, http://www.youtube.com/watch?v=R5POcUkIlAc. Esse vídeo explica quais protocolos, normalmente, são envolvidos no acesso do usuário em um *site*. Comente esse vídeo no Ambiente Virtual de Ensino-Aprendizagem no fórum 03 "Vídeos da Aula 2".

O protocolo IP é responsável por endereçar virtualmente a máquina de origem e a máquina de destino.

O controle de detectar e corrigir o fluxo de dados da camada *host*/rede é realizado pelo controle de *link* lógico. Todos dispositivos de rede fazem parte da camada *host*/rede.

Atividades de aprendizagem

Resolva os exercícios abaixo e comente no fórum 04 "Atividades da Aula 2".

1. Explique como funcionam as camadas do modelo de referência TCP/IP:

   a) Aplicação.

   b) Transporte.

   c) Inter/rede.

   d) *Host*/rede.

2. Descreva dois protocolos que fazem parte das camadas abaixo:

   a) Aplicação.
   b) Transporte.
   c) Inter/rede.

3. Descreva dois dispositivos de rede que fazem parte da camada *host*/rede.

4. Após assistir ao vídeo "Guerreiros da Informação", descreva dois protocolos que não foram estudados neste caderno.

Aula 3 – Serviços de redes na internet

Objetivos

Entender o funcionamento dos protocolos de encaminhamento de dados IPv4 e as vantagens oferecidas pelo IPv6.

Conhecer o sistema de documentos hipermídia, WWW e HTTP.

Entender as funcionalidades e utilidades do protocolo FTP.

Entender o funcionamento do DNS.

Conhecer os protocolos de serviço de *e-mail* IMAP e SMTP.

Conhecer os protocolos de acesso remoto Telnet e SSH.

A Aula 3 é repleta de protocolos que utilizamos em nosso dia a dia.

3.1 IPv4 e IPv6

Na internet, cada computador conectado à rede tem um endereço IP. Todos os endereços IPv4 possuem 32 *bits*. Os endereços IP são atribuídos à interface de rede do computador, normalmente, às placas de rede.

De acordo com Tanenbaum (2003, p. 464), "é importante observar que um endereço IP não se refere realmente a um computador. Na verdade, ele se refere a uma interface de rede;" assim, se um computador estiver em duas redes, ele precisará ter duas interfaces de rede para possuir dois endereços IP.

De acordo com Tanenbaum (2003, p. 464), "é importante observar que um endereço IP não se refere realmente a um computador. Na verdade, ele se refere a uma interface de rede;" assim, se um computador estiver em duas redes, ele precisará ter duas interfaces de rede para possuir dois endereços IP.

O endereçamento IP foi dividido nas cinco categorias listadas no Quadro 3.1.

Quadro 3.1: Formatos de endereços IP

Classe	Intervalo de endereços	Nº de endereços IP por rede
A	1.0.0.0 a 127.255.255.255	16.777.216
B	128.0.0.0 a 191.255.255.255	65.635
C	192.0.0.0 a 223.255.255.255	256
D	224.0.0.0 a 239.255.255.255	*Multicast*
E	240.0.0.0 a 247.255.255.255	Uso futuro

Fonte: Tanenbaum (2011, p. 277)

O intervalo de endereços nas classes limita a quantidade de computadores na rede. As classes A e B são utilizadas normalmente em grandes empresas, governos, organizações globais, etc. A classe C é a mais utilizada por pequenas e médias empresas que possuem até 256 computadores. A classe D é utilizada para *multicast*, isto é, envia dados a múltiplos pontos distintos ao mesmo tempo; ela normalmente é utilizada para aplicações de áudio e vídeo, e por fim, a classe E normalmente é utilizada para testes e reservada para uso futuro.

Porém, o IPv4 passou a apresentar algumas limitações com o passar do tempo, pois o número de computadores na internet aumentou demasiadamente nas últimas décadas (estudamos esse crescimento na Aula 1). Os endereços de 32 *bits* foram se esgotando com o passar dos anos e estima-se que esteja esgotado.

O Comitê Gestor da Internet no Brasil, acessado no *site* http://www.cgi.br/ e o Núcleo de Informação e Coordenação do ponto BR, que se encontra no *site* http://www.nic.br, desenvolvem diversos materiais, cursos e vídeos que auxiliam o profissional de TI a fazer migração do IPv4 para IPv6.

Devido a esse problema, a Internet Engineering Task Force (IEFT), o qual se encontra no *site* **http://www.ietf.org/**. Desenvolveu-se um novo padrão para suprir o problema. Criou-se o IPv6, que foi projetado para facilitar a migração do IPv4.

Atualmente o protocolo IPv6 está sendo implantado gradativamente na internet. De acordo com Albuquerque (2001, p. 36), "o protocolo foi desenvolvido para atender não apenas às necessidades atuais, mas também às necessidades das aplicações futuras". As principais características do IPv6 são:

Vídeo produzido pelo Comitê Gestor da Internet do Brasil e pelo Núcleo de Informação e Coordenação do Ponto BR, que traz informações de suma importância sobre o IPv6: http://www.zappiens.br/portal/VisualizarVideo.do?_InstanceIdentifier=0&_EntityIdentifier=cgiaWABIE9X_5bgN27_3wYUWL7sEvtn2mXb7xBpmr3S_FQ.&idRepositorio=0. Comente esse vídeo no Ambiente Virtual de Ensino-Aprendizagem no fórum 05 "Vídeos da Aula 3".

- protocolos simples;
- endereços de 128 *bits* para identificar as máquinas;
- sem restrições quanto à topologia da rede;
- recursos para autenticação e criptografia dos datagramas;
- independe das características do meio de transmissão;
- suporte para *multicast*;
- modo básico de operação baseado em datagramas;
- eficiente em redes de alta e baixa velocidade.

Responda às seguintes perguntas e comente no fórum 06 "Atividades da Aula 3".

1. Quantas classes existem no IPv4? Explique-as.

2. Explique as principais características do protocolo IPv6?

3.2 WWW e HTTP

A internet é um conjunto de computadores interconectados por redes, com o propósito de compartilhar informações. Ela é um conjunto de redes que utilizam o modelo de referência TCP/IP.

Mas, no início da internet, as informações eram acessadas em forma de texto. A *World Wide Web*, nossa **WWW**, ou ainda *WEB*, foi criada pelo físico Tim Berners Lee. Ele propôs um sistema de hipertexto, no qual, apontar para uma palavra ou frase levaria um usuário para uma nova página na mesma máquina ou para uma máquina na rede.

WWW
De acordo com Scrimger et al. (2002) a "*World Wide Web* é o nome dado ao corpo de informações na internet caracterizado por imagens gráficas coloridas e *links* de hipertexto "HTTP" ". Por outro lado, um navegador é a ferramenta que permite visualizar as informações que contêm as imagens gráficas coloridas e *links*.

Em 1993 foi desenvolvido um programa cliente amigável ao usuário, o qual revolucionou o mundo da informática e desbravou a internet; a partir dele, a maneira de fazer negócios no mundo começou a mudar. Esse programa se chamou Mosaic. Veja na Figura 3.1 a imagem de um dos primeiros navegadores para internet.

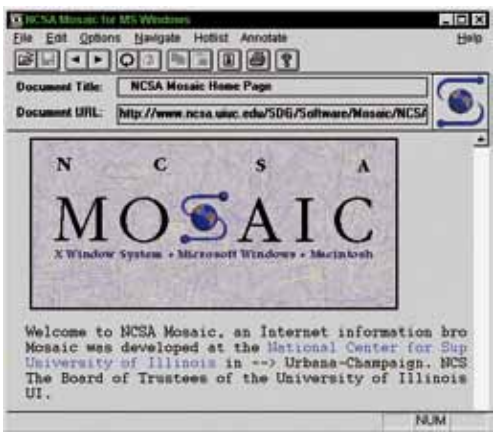


Figura 3.1: Imagem do navegador Mosaic
Fonte: http://infoevo.escolasmoimenta.pt/9f06-mosaic

O *browser* ou navegador é o programa cliente instalado em nossa máquina para ter acesso à internet. Veja no Quadro 3.2 os principais navegadores disponíveis no mercado.

Quadro 3.2: Os principais navegadores do mercado

Símbolo do Navegador	Nome do Navegador
	Google Chrome
	Mozilla Firefox
	Safari
	Internet Explorer
	Netscape

Fonte: Elaborado pelo autor

Na *web*, o usuário solicita ao navegador uma URL. O navegador faz o pedido para o servidor, que pode ser qualquer computador na rede que contenha as informações solicitadas pelo cliente. Na URL, está contido o protocolo HTTP, responsável por transferir hipertextos pela internet. Quando digitamos uma URL no navegador, ele, automaticamente, adiciona o protocolo 'http://' à página *web* solicitada.

Qual é o protocolo responsável por fazer a comunicação entre o cliente e o servidor? Respondeu certo quem pensou no HTTP! Pois é, o HTTP é o protocolo da camada de aplicação responsável por essa comunicação.

Os serviços fornecidos pela *web* ganharam dimensões maiores nas últimas décadas e, principalmente, nós últimos anos. Como dito anteriormente, no início da internet, as páginas trabalhavam somente com texto. Com o passar dos anos, novas tecnologias foram desenvolvidas e o protocolo HTTP passou a trabalhar com diversas informações, como imagens, posteriormente sons e, atualmente, vídeo. Hoje em dia, grande parte dos *sites* possui essas informações. Podemos perceber que as informações que trafegam pela *web* foram aumentando, consequentemente, com o surgimento de novas tecnologias.

Continuando a atividade anterior, responda às seguintes perguntas e comente no fórum 06 "Atividades da Aula 3".

1. Cite exemplos de como o WWW mudou a maneira fazer negócios no mundo.

2. O protocolo HTTP atua em qual camada do modelo de referência TCP/IP?

3. Cite a evolução das informações que são transferidas por hipertextos.

4. É correto afirmar que o WWW trabalha junto com o HTTP? Explique sua afirmação.

3.3 FTP

O protocolo FTP é utilizado na *web* para acesso de arquivos remotos, e em servidores de arquivos locais em uma empresa. Quando estamos fazendo o *download* de um arquivo, normalmente utilizamos o protocolo FTP. Ele também pode ser utilizado para fazer o *upload* de um arquivo de seu computador para a rede.

O protocolo FTP permite transferir arquivos pela internet. Existem vários programas gratuitos na internet que fornecem os serviços de FTP. Através dele, é possível transferir arquivos, autenticar usuários e gerenciar arquivos e diretórios.

Faça a pesquisa abaixo e comente no fórum 06 "Atividades da Aula 3".

1. Cite as características de três programas gratuitos na internet que fornecem o serviço de FTP.

De acordo com Albuquerque (2001, p. 157), "o FTP é o protocolo mais popular para transferência de arquivos, sendo implementado por um processo cliente, executado na máquina na qual a transferência foi solicitada e por um processo servidor". Ele é orientado à conexão, usa o protocolo TCP e o serviço é provido na porta 21.

Um *site* da *web* pode ser identificado de duas maneiras: pelo seu nome de domínio, por exemplo, www.ifes.edu.br, ou pelo endereço de IP do servidor que hospeda o serviço.

3.4 DNS

O *Domain Name System* ou Sistema de Nomes de Domínios (DNS) é um dos serviços mais importantes da internet. É um sistema de gerenciamento de nomes hierárquico e distribuído e responsável pela conversão do nome das páginas *web* para endereços IP.

Quando digitamos www.ifes.edu.br, significa que estamos nos referindo às informações contidas no Quadro 3.3 a seguir.

A *Internet Corporation for Assigned Names and Number*, ou Corporação da Internet para Atribuição de Nomes (ICANN), é responsável por coordenar o gerenciamento dos elementos técnicos do DNS para garantir sua capacidade de resolução universal, de modo que todos os usuários da internet encontrem todos os endereços válidos. Para isso, ela supervisiona a distribuição dos identificadores técnicos exclusivos usados nas operações da internet e a delegação de nomes de domínio de primeiro nível (como .com, .info, etc.).

Quadro 3.3: Informações do domínio do *site* www.ifes.edu.br

www	ifes	edu	br
Serviço oferecido na rede	Nome de domínio para instituição responsável pelo *site*	Indica que é um domínio com fins educacionais	Indica que está localizado no domínio brasileiro

Fonte: Elaborado pelo autor

- ifes: identifica a organização responsável pelas informações contidas no *site*.
- edu: relativo às instituições educacionais;
- br: é baseado nos códigos dos países, é conhecido como domínio geográfico.

Veja no Quadro 3.4, o nome de domínios genéricos.

Quadro 3.4: Nomes de domínios genéricos

Nome de domínio	Significado
com	Organizações comerciais
edu	Instituições educacionais
gov	Instituições governamentais
mil	Instituições militares
org	Organizações não governamentais
int	Organizações internacionais

Fonte: Adaptado de Tanenbaum (2011, p. 384)

O modelo de referência TCP/IP possui dois níveis de DNS, primário e secundário. O DNS primário é o principal; quando digitamos a URL da página *web* pelo DNS primário, localizamos a página solicitada através do navegador. O DNS secundário funciona da mesma forma que o primário, porém é utilizado quando este não é encontrado; ele nós oferece mais segurança.

Faça o trabalho abaixo e comente no fórum 06 "Atividades da Aula 3".

1. Indique programas gratuitos na *web* que forneçam serviços de DNS e explique as características desses serviços.

3.5 *E-mail*

O *electronic mail*, mais conhecido como "*e-mail*", permite enviar e receber informações por meio de uma rede de computadores. Podemos transmitir informações pela internet ou pela rede interna de uma empresa, a intranet.

Trocar *e-mail* é muito comum no mundo digital. Hoje em dia, olhar a caixa de *e-mail* diariamente é normal. Essa ferramenta de comunicação conquistou os usuários ao redor do mundo e se tornou indispensável no dia a dia. Com ela pode-se fazer compra pela internet, entregar currículo, trocar informação com parentes, amigos e principalmente utilizar na vida profissional. O papel do *e-mail* na sociedade moderna é de suma importância.

Em meio há várias histórias sobre o *e-mail*, o programador Ray Tomlinson foi responsável pela utilização do sinal de arroba "@" no correio eletrônico e é considerado por muitos como o inventor dessa ferramenta de comunicação. O projeto ARPANET foi fundamental para a ampla divulgação do *e-mai*l.

O sinal de @ identifica o domínio de quem envia e de quem recebe a mensagem. Por exemplo: fulano@ifes.edu.br envia um *e-mail* para ciclano@hotmail.com. O fulano envia um *e-mail* do domínio ifes para o domínio hotmail que o ciclano utiliza.

Para Shipley e Schwalbe (2008), os grandes motivos pelos quais amamos o *e-mail* são: ele é a melhor mídia para trocar informações essenciais; é possível entrar em contato com qualquer pessoa que possui *e-mail*; fuso horário não é problema, é uma maneira eficiente e econômica de se comunicar; os *e-mails* podem ser gravados e sofrer buscas, o telefone não; o *e-mail* permite que você componha as suas mensagens sob suas condições e no seu próprio tempo; o *e-mail* permite anexar e incluir informações que o destinatário poderá recuperar quando desejar. E os motivos para não querer usar o *e-mail* são: a facilidade com que o *e-mail* estimula trocas desnecessárias; o *e-mail* substituiu em grande parte o telefonema, mas nem todo telefonema é substituído; você pode entrar em contato com todo mundo, mas todo mundo pode entrar em contato com você; o fato de o *e-mail* deixar rastros pode fazer você ser responsabilizado pela sua correspondência eletrônica; as palavras que você escreveu por *e-mail* podem ser alteradas; *e-mail* propagam vírus.

De acordo com Falbriard (2002, 36), as principais dicas em relação à ética e à atitude profissional a ser tomada em *e-mail* e grupos de notícias é: "Faça do *e-mail* seu canal de clareza; leia primeiro, depois responda; quando acha que escreveu muita prosa, apague tudo; não propague cartas em cadeia; não defenda causas desconhecidas; não comente o conteúdo de correios particulares de alheios. Você viu, você leu, entretanto eles não existem. Lembre-se, calar é a melhor solução."

Faça a pesquisa abaixo e comente no fórum 06 "Atividades da Aula 3".

1. Quais são os provedores de *e-mail* gratuito no mercado. Cite-os e explique os serviços oferecidos.

2. A informação é útil é preciosa. Quais dicas não citadas no livro podem ser utilizadas no envio de *e-mail*.

3.5.1 IMAP

A equipe da CGI produziu quatro vídeos que abrangem uma parte da história da internet de forma simples e divertida. As quatro animações são: Navegar é Preciso, disponível em: http://www.antispam.br/videos/cgi-navegar-p.wmv; Os Invasores, disponível em: http://www.antispam.br/videos/cgi-invasores-p.wmv; *Spam*, disponível em: http://www.antispam.br/videos/cgi-spam-p.wmv e A Defesa, disponível em: http://www.antispam.br/videos/cgi-defesa-p.wmv. Os vídeos informam e esclarecem sobre os perigos aos quais os usuários estão expostos, explicam o que é *Spam* e dão dicas de como navegar com mais segurança na rede. Comente esses vídeos no Ambiente Virtual de Ensino-Aprendizagem no fórum 05 "Vídeos da Aula 3".

No início do correio eletrônico, o protocolo *Post Office Protocol*, mais conhecido como POP, foi muito utilizado para que as mensagens do *e-mail* sejam transferidas para o computador local do usuário. A versão mais utilizada do protocolo POP é o POP3.

Se você acessar seu *e-mail* do computador em casa, no trabalho, na escola, etc., o protocolo POP3 baixa todas as mensagens do seu *e-mail* para o computador local, excluindo as mensagens do servidor; esse modo de trabalho do POP3 é conhecido como *off-line*. Isto é, as mensagens enviadas para o computador local são excluídas do servidor, ocasionando a distribuição de seu *e-mail* em vários locais diferentes, causando diversas dificuldades de organização ao usuário.

Nesse cenário, entra em cena um protocolo alternativo para correio eletrônico, o IMAP. O mais utilizado é o IMAP4. De acordo com Tanenbaum (2003, p. 372), esse protocolo pressupõe que todas as mensagens de correio eletrônico permaneçam no servidor, em várias caixas de correio. Mesmo baixando as mensagens para o computador local, elas estarão disponíveis no *e-mail*. Com o IMAP4 é possível trabalhar com os modos de mensagens *off-line*, *on-line* e desconectado.

No mundo da informática, normalmente, tudo que é bom exige mais recursos; com o passar do tempo, ou a tecnologia é atualizada ou ela é substituída por outra melhor. Foi assim com o POP3.

Dentre os principais programas que fornecem serviços de *e-mail* no mercado, destacam-se: Mozilla Thunderbird e o Outlook Express.

O modo *on-line* permite que as mensagens permaneçam no servidor de *e-mail*. O usuário pode acessar, bem como manipular as mensagens pelos programas de correio eletrônico.

Pelo programa de correio eletrônico, o modo desconectado permite fazer uma cópia das mensagens selecionadas em *cache* antes de se desconectar. Quando o programa é executado, as mensagens são ressincronizadas, isto é, permanecem no servidor.

Faça o trabalho abaixo e comente no fórum 06 "Atividades da Aula 3".

1. Qual é a porta em que funciona o protocolo IMAP4 e o POP3?

2. Quais programas podem configurar o serviço IMAP?

3. Quais são as principais vantagens do protocolo IMAP4 sobre o POP3?

3.5.2 SMTP

Para usuários que simplesmente apertam o botão "enviar", o envio do *e-mail* é relativamente simples. Porém, o processo de envio de *e-mail* envolve muitos passos.

O protocolo SMTP, de acordo com Scrimger et al. (2002), trata a transferência de *e-mails* de um sistema de correio eletrônico para o outro. Ele assegura um método eficiente e confiável. A mensagem é armazenada no servidor SMTP até que seja transferida para o servidor de destino.

A mensagem enviada pelo *e-mail* é armazenada no servidor SMTP até ser transferida para o servidor de destino. Ele é baseado na entrega ponta a ponta, isto é, conecta ao servidor de destino para transferir a mensagem.

Quando o usuário do domínio **@gmail.com** envia uma mensagem utilizando o programa Outlook Express, a mensagem é direcionada ao servidor SMTP do serviço gmail. Com base no endereço de *e-mail* enviado, ex: **@yahoo.com.br**, o servidor SMTP envia a mensagem para o servidor yahoo apropriado.

Faça o trabalho abaixo e comente no fórum 06 "Atividades da Aula 3".

1. Qual é a porta em que funciona o protocolo SMTP?

2. Quais programas podem configurar o serviço SMTP? Nesses programas funciona o protocolo IMAP ou POP3?

3.6 Acesso remoto

Hoje em dia, várias empresas recebem suporte *on-line*, e o acesso remoto é uma das principais ferramentas para quem trabalha fornecendo o atendimento remoto. Com o acesso remoto, é possível ter controle sobre outra máquina a distância.

Quando um *cracker* invade um sistema, ele está realizando um acesso remoto não autorizado.

O acesso remoto pode ser feito de forma segura, com criptografia e autenticação dos dados. A segurança é definida de acordo com a configuração do administrador e a aplicação a ser definida. Estudaremos, a seguir, os protocolos de acesso remoto TELNET e SSH.

Responda às seguintes perguntas e comente no fórum 06 "Atividades da Aula 3".

1. O que é acesso remoto?

2. O que é um *cracker*?

3. Em quais situações poderíamos utilizar o acesso remoto?

3.6.1 TELNET

No início da internet, o TELNET foi o protocolo mais utilizado pelos usuários e administradores no acesso remoto entre o cliente e o servidor. Grande parte de sua utilização deve-se à sua estabilidade.

O TELNET opera na camada de aplicação e utiliza o protocolo TCP para transportar as informações. A conexão com um servidor de TELNET é geralmente iniciada por um cliente, quando ele fornece acesso a programas do servidor, *login* simultâneo, etc. Opera tanto graficamente quanto com linhas de comando, em que as instruções são enviadas para serem executadas no servidor. Em geral, os comandos básicos tem nomes curtos.

A década de 1990 marcou o início da internet no setor privado, e o TELNET passou a ser muito requisitado. Porém, a limitação de segurança combinada com sua utilização generalizada o tornou obsoleto. Um protocolo de dados sem criptografia pode ser interceptado por *crackers*. O TELNET não tem capacidade para tomar medidas contra invasões.

3.6.2 SSH

O protocolo SSH oferece uma funcionalidade semelhante ao TELNET; porém, fornece duas melhorias significantes, sendo elas a comunicação segura e a transferência de dados adicionais e independentes pela mesma conexão.

Embora o SSH e o TELNET sejam parte da pilha de protocolos TCP/IP, existem muitos outros protocolos de acesso remoto. Livros e internet são uma boa fonte de pesquisa.

De acordo com Comer (2006, p. 300), o SSH oferece três mecanismos que formam a base dos serviços que ele fornece.

- Um protocolo de camada de transporte que fornece autenticação de servidor, confidencialidade de dados e integridade de dados com privacidade de encaminhamento perfeita (ou seja, se uma chave for comprometida durante uma sessão, o conhecimento não afeta a segurança das sessões anteriores).

- Um protocolo de autenticação de usuário que autentica o usuário para o servidor. Assim, um servidor pode dizer exatamente que o usuário está tentando formar uma conexão.

- Um protocolo de conexão que multiplexa diversos canais de comunicação lógicos através de uma única conexão SSH subjacente.

Responda às seguintes perguntas e comente no fórum 06 "Atividades da Aula 3".

1. Explique o TELNET.

2. Em qual porta funciona o SSH e o TELNET?

3. O SSH tem criptografia? Quais recursos ele oferece?

Criptografia é a técnica que permite criptografar as informações, em forma de cifras ou de códigos.

Resumo

O protocolo IPv4 não atende mais à demanda atual da internet; para suprir suas limitações, entrou no mercado o IPv6. Os protocolos WWW e HTTP são responsáveis pelo sucesso da internet nos dias atuais; eles estão sempre trabalhando com o protocolo mais utilizado na rede para transferir arquivos, que é o FTP.

Para organizar os *sites* que foram surgindo na internet, surgiu o DNS, protocolo responsável por gerenciar os nomes de domínio na rede. Com tantas novidades tecnológicas, surgiu o *e-mail*, o qual atualmente é indispensável. Para gerenciar ou ter acesso a um computador distante, surgiram várias maneiras de fazer acesso remoto na internet. As tecnologias estudadas nesta aula foram o TELNET e SSH.

Atividades de aprendizagem

Resolva os exercícios abaixo, e comente no fórum 06 "Atividades da Aula 3".

1. Quais são as principais diferenças entre o IPv4 e o IPv6?

2. Explique por que o WWW possui a mesma porta do HTTP?

3. É possível fazer *download* e *upload* com o protocolo FTP. Explique a afirmação.

4. Qual é a diferença entre o DNS primário e o DNS secundário?

5. Qual serviço o protocolo SMTP oferece?

6. Cite as principais diferenças entre o IMAP4 e o POP3.

7. O que caracteriza o acesso remoto?

8. Qual é a desvantagem do protocolo TELNET para o SSH?

9. O protocolo SSH possui autenticação, integridade e confidencialidade. O que isto significa?

10. Cite outros programas que fornecem o serviço de acesso remoto?

Aula 4 – Serviços de redes cliente-servidor

Objetivos

Compreender a utilidade do *gateway*.

Entender a dinâmica das funcionalidades do DHCP.

Compreender o funcionamento do *proxy*.

Compreender as utilidades e vantagens do *firewall*.

Demonstrar as principais diferenças dos serviços de *firewall* oferecidos no mercado, apresentando os *firewalls* de *hardware* e *software*.

Nesta aula serão apresentados a você os principais serviços cliente-servidor que, normalmente, são utilizados em uma rede de computadores. Para que os serviços sejam utilizados pelas máquinas clientes, é necessário ter um servidor que forneça o serviço desejado. O servidor pode ser uma máquina ou um dispositivo de rede, dedicado ou não. No mundo empresarial, é importante obter o máximo de conhecimento das tecnologias atuais. Dessa maneira, o profissional de TI pode propor a melhor solução para seu cliente, e consequentemente, se tornar uma referência para atender ao mercado.

4.1 *Gateway*

Em uma rede de computadores, o *gateway* ou "porta de entrada", é um computador intermediário ou um dispositivo dedicado, responsável por fornecer determinados tipos de serviços. Entre suas principais funcionalidades, podemos destacar a interligação de duas redes que possuem protocolos diferentes, compartilhamento da conexão de internet, roteadores, *proxy*, *firewalls*, etc. Para configurá-lo como cliente, é necessário informar o endereço *gateway* do serviço nas propriedades de rede de seu sistema operacional. Veja na Figura 4.1 as propriedades de rede do protocolo TCP/IP versão 4 no Windows Vista.

Figura 4.1: Propriedades do protocolo TCP/IP versão 4
Fonte: Windows Vista

Quando estamos conectados à internet por meio de um roteador, ele é a porta de ligação com esse serviço. Para que uma máquina tenha acesso a ele, é necessário configurar o endereço *gateway* do roteador no computador que terá acesso à internet. Esse serviço pode ser configurado, automaticamente, ou manualmente. Com esses procedimentos, estamos indicando a porta de entrada da internet.

De acordo com Tanembaum e Wetherall (2011, p. 17), "o nome geral para uma máquina que faz uma conexão entre duas ou mais redes e oferece a conversão necessária, tanto em termos de *hardware* e *software*, é um *gateway*". Os *gateways* são distinguidos pela camada em que operam na hierarquia de protocolos.

Faça a pesquisa abaixo e comente no fórum 08 "Atividades da Aula 4".

1. O que é um *gateway*?

2. Descreva o passo a passo para acessar a configuração *gateway* no Windows.

3. Descreva qual a função básica dos dispositivos abaixo; em seguida, informe se eles fornecem serviços de *gateway*.

a) *modem*;

b) *hub*;

c) *switch*;

d) roteador;

e) *firewall*;

f) *proxy*.

4.2 DHCP

Imagine um profissional de TI gerenciando uma rede com cem computadores. Agora, imagine gerenciar centenas de computadores. Configurar o TCP/IP manualmente em cada dispositivo de rede envolveria tempo e uma equipe técnica maior para efetivar o trabalho. Atualmente, as empresas estão migrando aos poucos do protocolo IPv4 para o IPv6. A reconfiguração desses dispositivos pode ser mais rápida? Sim, pode.

O protocolo DHCP é a abreviatura de *Dynamic Host Configuration Protocol* ou Protocolo de configuração dinâmica de endereços de rede. É um serviço intensamente utilizado para atualizar as configurações de rede nos dispositivos que estejam utilizando o protocolo TCP/IP.

Sem utilizar o protocolo DHCP, o profissional de TI teria que configurar, manualmente, as propriedades do protocolo TCP/IP em cada dispositivo que esteja conectado a rede, denominado pelo protocolo como *host*.

O exemplo de Comer (2006, p. 271) diz que um servidor DHCP aluga um endereço de rede para um cliente, por um período finito de tempo. O servidor especifica o aluguel quando ele aloca o endereço. Durante o período de aluguel, o servidor não alugará o mesmo endereço para outro cliente. Isto é, quando um computador recebe os dados DHCP, ele configura a rede do cliente. O usuário não precisa configurar o endereço IP, máscara de sub-rede, *gateway* padrão, DNS, etc.

Sistemas operacionais como Windows Server 2003 e 2008 possuem o serviço DHCP. Para ele funcionar, é necessário instalar o servidor DHCP através do *Active Directory*. Após esse procedimento, o administrador da rede configura o serviço DHCP de acordo com a solução que ele propôs para a empresa. Ele define a faixa IP, máscaras de sub-rede, *gateway*, DNS, etc. Como podemos perceber, a máquina que está instalada e configurada com o serviço DHCP é denominada servidor.

O servidor DHCP do Windows Server 2000, 2003 e 2008 não pode ser instalado no Windows XP, Vista, etc.

O termo cliente descreve as estações de trabalho que estão obtendo configurações a partir do servidor DHCP. Durante a inicialização de uma estação de trabalho, é estabelecida uma comunicação pela rede e, dinamicamente, a estação recebe todas as configurações TCP/IP definidas pelo administrador de rede.

Normalmente, a estação de trabalho está preparada para receber as informações do servidor DHCP pela rede, não sendo necessário configurá-la. Segue, na Figura 4.2, a configuração padrão nas propriedades do protocolo TCP/IP.

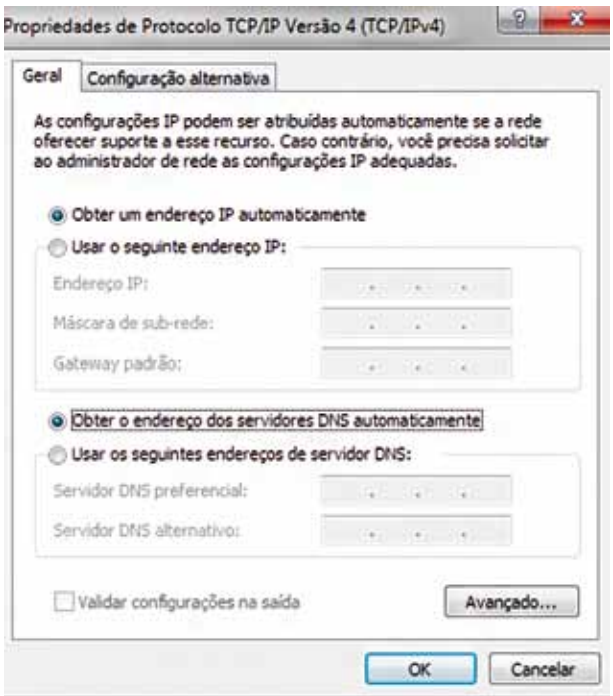


Figura 4.2: Configuração padrão do protocolo TCP/IP
Fonte: Windows Vista

Responda às seguintes perguntas e comente no fórum 08 "Atividades da Aula 4".

1. O que é DHCP?

2. Quais dispositivos podem utilizar o protocolo TCP/IP?

3. Descreva quais informações o DHCP pode configurar para o dispositivo cliente.

4. O que é o *Active Directory*?

5. Qual é a diferença entre configurar o IP de uma máquina dinamicamente e estaticamente?

6. Por que as estações de trabalho são descritas como clientes?

4.3 *Proxy*

Ao acessar um computador em que a página da internet solicitada está bloqueada, normalmente, o *proxy* é o responsável por não permitir o acesso. Então, o *proxy* bloqueia as páginas da internet? Também. O servidor *proxy* possui várias funcionalidades e uma delas é bloquear as páginas da internet.

O *proxy* funciona de forma intermediária entre o usuário e a internet. Veja na Figura 4.3 a atuação do *proxy* desempenhando a conexão da estação de trabalho com a rede externa. Ao solicitarmos um endereço *web*, o endereço da URL é enviado para o servidor *proxy*, que, por sua vez, filtra as informações que podem ser acessadas ou não.

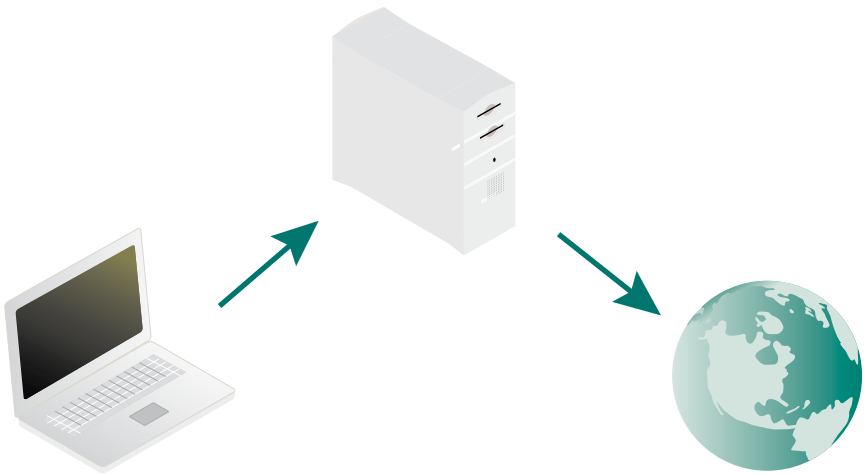


Figura 4.3 : O Proxy atua entre o usuário e a internet
Fonte: http://guiadicas.net/o-que-e-servidor-proxy/

Existem vários programas de *proxy* grátis no mercado, o administrador da rede é responsável por gerenciar o conteúdo que será acessado. Muitas empresas do Brasil e do mundo bloqueiam *sites* como Facebook, Orkut e entre outros. Alguns especialistas dizem que os funcionários perdem muito tempo de trabalho diante de *sites* que os distraiam. Outros dizem que o bom funcionário sabe a hora certa de navegar. Opiniões à parte, o profissional de TI é o responsável por detectar a necessidade de colocar o *proxy* dentro de uma empresa e viabilizar o seu correto funcionamento.

Outra importante função do *proxy* é manter uma área de acesso rápido às informações já acessadas por outros usuários, evitando a retransmissão das mesmas informações pela rede. Ao solicitar uma página como **www.ifes.edu.br**, o servidor *Proxy* captura os dados da página *web* solicitada, guardando-os em um espaço em disco. Se outro usuário da rede solicitar a mesma página, ela será apresentada em seu navegador de forma rápida, diminuindo o tempo de requisição ao servidor *web*.

Ao solicitar uma página *web* em uma rede que possui o serviço de *Proxy*, o navegador fará primeiro uma procura do conteúdo em *cache*, isto é, na memória que foi utilizada para guardar as informações de acesso. Caso não encontrar, o acesso será feito diretamente no *site web* solicitado.

Dentre as várias funcionalidades do *proxy*, é importante ressaltar que a configuração do serviço varia muito de administrador para administrador de rede. Um *proxy* bem configurado permite saber quais páginas da *web* o funcionário está acessando, e por quanto tempo. Pode-se criar políticas que permitam aos funcionários acessarem páginas como Myspace, *blog*, etc., durante o horário de almoço. Por isso, é importante sempre estar estudando e se qualificando cada vez mais no mercado de TI.

Responda às seguintes perguntas e comente no fórum 08 "Atividades da Aula 4".

1. O que é *proxy*?

2. Quem define o que pode e o que não pode ser acessado na internet?

3. Como funciona o *cache*?

4. Alem da política de acesso e o *cache*, é possível fazer utilizar outros recursos do *proxy*? Explique sua afirmação.

5. Cite três programas gratuitos que fornecem o serviço de *proxy.* Explique-os.

O *link* abaixo demonstra como funciona o *proxy*: http://olhardigital.uol.com.br/produtos/central_de_videos/proxy-mais-do-que-uma-mensagem-de-erro
E no *link* http://olhardigital.uol.com.br/produtos/central_de_videos/proxy-error-server-error-404-503 são destacados os principais erros que podem acontecer com o *proxy*. Comente esses vídeos no Ambiente Virtual de Ensino-Aprendizagem no fórum 07 "Vídeos da Aula 4".

4.4 *Firewall*

Quem nunca escutou falar em segurança na internet? Palavras como *crackers*, *hackers*, vírus, antivírus, etc., estão se tornando normais no mundo da *web*. E o *firewall* ou "Muro antichamas" é o serviço responsável por aplicar uma política de segurança nas informações que trafegam na rede. Ele é responsável por bloquear qualquer tentativa de acesso ao seu computador sem autorização. A Figura 4.4 demonstra o *firewall* atuando entre a rede e a internet.

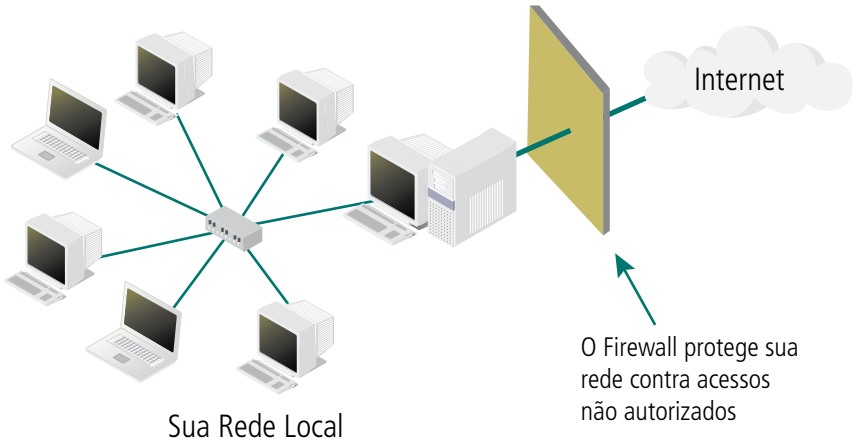


Figura 4.4: *Firewall* atuando entre a rede e a internet
Fonte: http://www.gta.ufrj.br/grad/08_1/Firewall/definition.html

Assim como o *proxy*, um mesmo *firewall* pode ser configurado por maneiras diferentes, e a configuração depende do grau de conhecimento do administrador da rede. Por isso, é de suma importância sempre estudar, pois, assim, o profissional de TI vai ficar atualizado com as novas tecnologias.

Através do *firewall* é possível bloquear portas de programas, IPs, etc.; com ele, o administrador da rede configura o que é permitido entrar através da internet. Podemos perceber que, ao contrário do *proxy*, o *firewall* bloqueia o que entra na rede pela internet. Já o *proxy*, bloqueia o que o usuário vai acessar na internet. Uma empresa que possui esses dois serviços, tem um antivírus atualizado em suas máquinas, está menos sujeita a ataques de *crackers*, menos problemas relacionados a vírus e maior segurança nas informações que estão trafegando na rede.

A importância do *firewall* fica evidente na afirmação de Comer (2006, p. 364): uma organização que possui várias conexões externas precisa instalar um *firewall* em cada uma delas e precisa coordenar todos os *firewalls*. Deixar de restringir o acesso de forma idêntica em todos os *firewalls* pode deixar a organização vulnerável.

Firewall não é antivírus. Apesar de ambos serem voltados para segurança, o antivírus atualizado protege o computador do ataque de diversos vírus e *softwares* maliciosos.

Atualmente no mercado, temos *firewalls* gerenciados por *hardware* e por *software*; para fazer a aquisição de um dos dois, é necessário que o profissional de TI saiba o tamanho da rede, quantidades de interfaces, política de segurança, volume de tráfego, valor disponível para investir, etc. Somente assim será possível fazer uma escolha coerente. A combinação de ambos em uma rede recebe o nome de *appliance*, que é a combinação entre *hardware* e *software*.

Existem diversos *firewalls* controlados por *software* grátis no mercado; muitos estão disponíveis no **http://www.baixaki.com.br**.

Normalmente, dentre as características que podemos destacar nos *firewalls* de *hardware* é a de que eles possuem serviços de rede agregados, como VPN, acesso remoto, etc. Veja na Figura 4.5 um *firewall* de *hardware*.

No *link* a seguir http://olhardigital.uol.com.br/produtos/central_de_videos/Firewall-o-guardiao-do-nosso-pc você vai encontrar uma reportagem do programa "Olhar Digital" explicando o que é um *firewall*. Comente esse vídeo no Ambiente Virtual de Ensino-Aprendizagem no fórum 07 "Vídeos da Aula 4".

Figura 4.5: *Firewall* de *hardware*
Fonte: http://blog.microsafe.com.br/index.php/2012/01/25/medo-de-ataques-saiba-como-escolher-um-firewall-da-sonicwall/

Dentre os principais fabricantes desse produto, pode-se destacar a Cisco, Checkpoint, Juniper, Sonicwall, Palo Alto redes, etc.

Faça o trabalho abaixo e comente no fórum 08 "Atividades da Aula 4".

1. O que é *firewall*?
2. Um mesmo *firewall* pode ser configurado de forma diferente pelo administrador da rede. Explique esta afirmação.
3. Quais são as diferenças entre *firewall* por *software* e por *hardware*?
4. Qual é a diferença entre um serviço de *proxy* e um serviço de *firewall*?
5. O *firewall* é um antivírus?
6. Cite três *firewalls* de *software* grátis na internet?
7. Como surgiu o *firewall*?
8. O que o *firewall* do Windows faz e o que ele não faz.

Resumo

Dentre diversos serviços fornecidos pelos servidores, podemos destacar que eles proporcionam ao administrador da rede: segurança, flexibilidade e principalmente autonomia.

O *gateway* é um computador intermediário ou um dispositivo dedicado, responsável por fornecer determinados tipos de serviços, como conectar à internet. O protocolo DHCP é um serviço de rede que fornece as configurações TCP/IP aos computadores clientes da rede. O serviço de *proxy* permite ao profissional de TI criar uma política de privacidade dentro de empresas, universidades, etc., bloqueando diversos acessos externos na internet. A outra função do *proxy* é fazer *cache* das páginas recentemente acessadas pelo usuário, permitindo abrir as páginas com maior velocidade. A necessidade de instalação do serviço de *firewalls* em uma empresa cresce a cada dia. Esse serviço bem configurado permite controlar o que entra na rede, assim como prevenir contra ataque de *crackers*.

Atividades de aprendizagem

Resolva os exercícios abaixo e os comentem no fórum 08 "Atividades da Aula 4".

1. Cite dois exemplos de *gateway* em uma rede de computadores.

2. Qual é a diferença entre configurar um cliente dinamicamente e estaticamente?

3. Qual a diferença entre *gateway* e DHCP?

4. É correto afirmar que o DHCP pode configurar o *gateway* em uma máquina cliente? Explique sua resposta.

5. O que o *proxy* e o *firewall* possuem em comum?

6. Qual é a principal diferença entre um *proxy* e um *firewall*?

7. O que é *appliance*?

8. O que é política de segurança? E tráfego na rede?

9. Qual solução de segurança você indicaria para uma empresa que está começando com um servidor e seis computadores? Justifique sua resposta.

10. Qual solução de segurança você aplicaria em uma empresa que possui dois servidores e 50 computadores? Justifique sua resposta.

Aula 5 – Serviços de Redes WAN

Objetivos

Apresentar a tecnologia de rede de alta velocidade ATM.

Demonstrar como funciona a tecnologia de banda larga mais utilizada no Brasil, ADSL.

Compreender o que é roteamento e roteadores.

Apresentar o que são sistemas autônomos.

Apresentar as VPNs, uma tecnologia em ascensão no mercado de TI.

As redes WAN são conhecidas como redes de longa distância. Nesta aula, serão apresentadas algumas tecnologias, serviços e protocolos de redes WAN que funcionam na internet. Estamos partindo da visão micro, para a visão macro. No final dos anos 1980, surgiram novas tecnologias de rede que permitiram o crescimento da rede, conectando cada vez mais usuários na *web*. Compreender os serviços de redes *WAN* proporciona ligar vários pontos com as aulas anteriores. A partir desta Aula, os pontos começam a se ligar e a visão macro sobre como funciona a internet se torna concreta! Esta aula é um prato cheio para quem quer conhecer a fundo as principais tecnologias que conectam o brasileiro na internet.

5.1 ATM

A sigla ATM, do inglês *Asynchronous Transfer Mode*, ou comutação de pacotes, surgiu no fim da década de 1980 e início da década de 1990. Entre suas principais tecnologias, se destaca a arquitetura de rede de alta velocidade orientada à conexão e baseada na comutação de pacotes de dados, tratando dados como vídeo e áudio em tempo real. Para Scrimger et al. (2002, p. 89):

> ATM foi proclamada como a estrela ascendente da tecnologia de rede pelo fato de fornecer um transporte de dados confiável e com velocidade muito alta tanto em distâncias curtas como longas, suportando um amplo espectro de aplicativos.

Essa tecnologia de alta velocidade comuta as informações, isto é, encaminha os dados pelas redes, sendo responsável direta ao impulsionar o crescimento da banda larga.

Você se lembra do conceito de topologia? Ela descreve como é o *layout* de uma rede. Existem várias topologias de redes; dentre elas, podemos destacar a estrela, a árvore e a híbrida. O protocolo ATM, foi desenhado para ser de alta velocidade, independendo da topologia utilizada pela rede.

Para fazer uma rede ATM é necessário ter um *switch* ATM entre as redes para se conectar. Veja na Figura 5.1 a representação de uma conexão entre duas redes ATM.

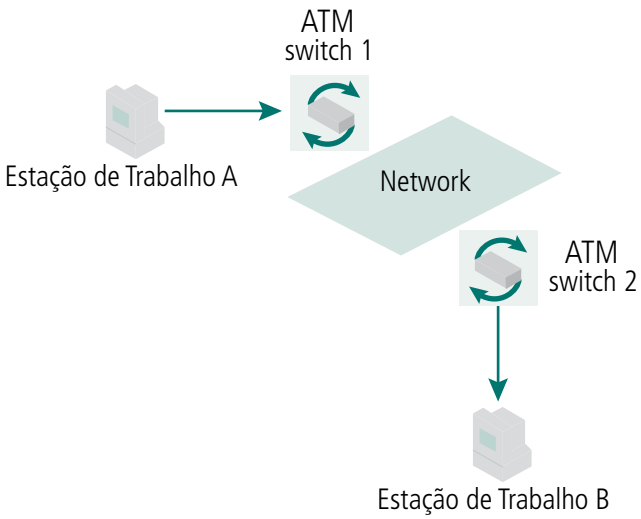


Figura 5.1: Conexão entre duas redes ATM
Fonte: Adaptado de http://technet.microsoft.com/pt-br/library/cc736757(WS.10).aspx

A tecnologia ATM trabalha com o conceito de células, isto é, com uma analogia ao pacote de dados, utiliza e suporta meios físicos como cabos coaxiais, par trançado e cabeamento de fibra óptica, que permitem atingir grandes taxas de velocidade. Outra grande vantagem é a utilização do *quality of service* (Qos) ou, qualidade de serviço; com essa tecnologia é possível definir níveis de prioridade para os diferentes fluxos de rede, reservar recursos, determinar o tamanho da banda, etc.

As células encaminham as informações pelos canais e caminhos virtuais estabelecidos entre as redes ATM. O caminho virtual utilizado pela ATM é chamado de *Virtual Path Identifier* (VPI). O canal virtual é denominado *Virtual Chaneel Identifier* (VCI). Na seção 5.2 demonstra-se qual é a importância do VPI/VCI na internet banda larga ADSL.

O protocolo ATM utiliza vários conceitos de interface/protocolos. Veja na Figura 5.2 a representação de uma interconexão de switchs ATM, chamada de "NNI", que conecta sistemas ATM, e a interconexão do usuário com switch ATM, denominada "UNI".

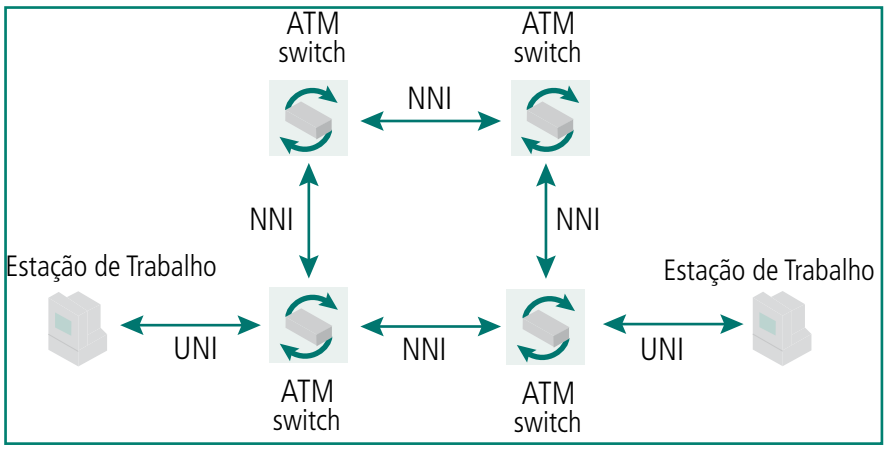


Figura 5.2: Interconexão NNI e UNI
Fonte: Adaptado de http://technet.microsoft.com/pt-br/library/cc782635(WS.10).aspx

Responda às seguintes perguntas e comente no fórum 10 "Atividades da Aula 5".

1. O que é ATM?

2. Quando o protocolo ATM surgiu?

3. Por que o ATM é uma tecnologia de alta velocidade?

4. Qual é a diferença entre VPI e VCI?

5. O que é possível fazer com o Qos?

6. Qual é a diferença entre UNI e NNI?

5.2 ADSL

O protocolo ADSL, *Asymmetric Digital Subscriber Line*, ou Linha de Assinante Digital Assimétrica, é uma tecnologia de comunicação que permite a transmissão de dados através da linha telefônica. O ADSL faz parte da família de tecnologias xDSL, que foi inventada em 1989 por um engenheiro da Bell Labs. O seu uso começou no final da década de 1990, aproveitando a própria rede de telefonia que chega à maioria das residências.

A linha telefônica, quando utilizada para voz, utiliza as frequências entre 300 Hz e 4000 Hz. O ADSL utiliza as frequências que não são utilizadas pela linha telefônica, sendo possível transmitir dados e voz utilizando mais de uma frequência ao mesmo tempo. Veja na Figura 5.3 a demonstração das informações que passam pela linha telefônica.

Figura 5.3: Informações que passam pela linha telefônica
Fonte: Adaptado de http://www.infowester.com/adsl.php

A taxa de *upload* na linha ADSL é menor do que a taxa de *download*.

Para o usuário ter acesso à banda larga com ADSL, é necessário que o provedor tenha acesso ao local que pretende utilizar o serviço. Após a instalação da linha telefônica, é necessário ter um *modem* para receber os dados do provedor. Veja na Figura 5.4 um modelo de *modem*.

Figura 5.4: Modelo de *modem*
Fonte: http://www.fotosimagens.net/modem.html

O sinal da linha telefônica é enviado ao *modem*, que, ao recebê-lo, modula e demodula as informações que serão trafegadas entre o usuário e o provedor de acesso à internet. Quando estamos configurando um *modem*, é necessário informar o VPI e o VCI do provedor. Mesmo quando os dados chegam à central telefônica do provedor, os dados são transmitidos pela internet através da rede ATM. Veja na Figura 5.5 uma ilustração do *modem* conectado à linha telefônica e ao computador.

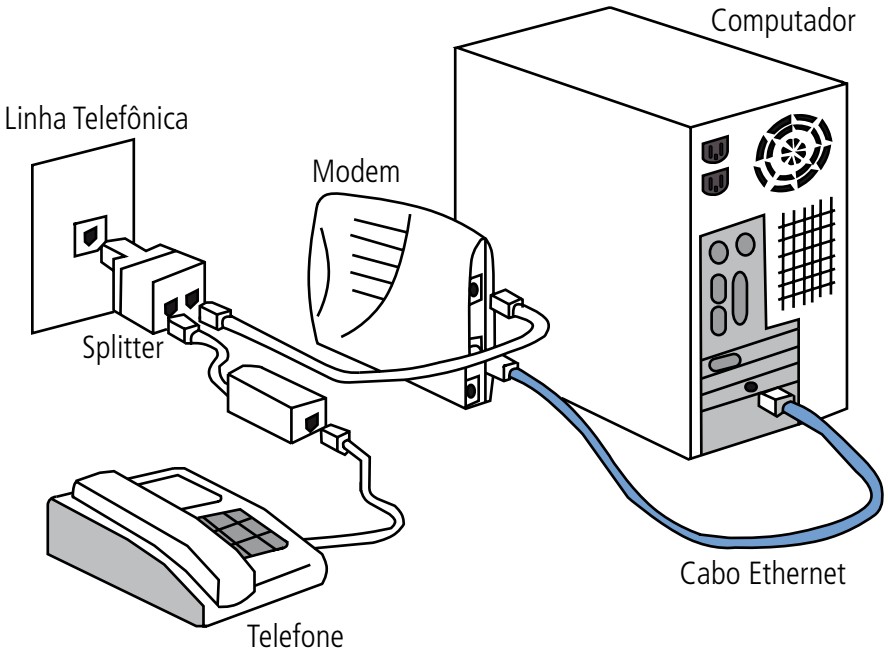


Figura 5.5: *Modem* conectado à linha telefônica e ao computador
Fonte: Elaborada pelo autor

Para configurar um *modem*, não existe segredo. O *site* **http://www.portaladsl.com.br** é especializado neste assunto. Quando houver alguma dúvida, você encontra nele o tutorial do modelo que deseja configurar.

Os provedores de serviço ADSL podem oferecer dois tipos de endereço IP: fixo ou dinâmico. O endereço fixo pode ser mais vantajoso para aqueles que usam a conexão ADSL para jogos, para se conectarem a servidores *web* e numa rede virtual privada VPN. Já para os usuários domésticos, o endereço IP dinâmico pode ser uma vantagem, pois dificulta o ataque de *hackers*.

A tecnologia ADSL está ganhando força com a ADSL2 e ADSL 2+. Ambas utilizam a linha telefônica para acessar a internet. Hoje, no Brasil, várias empresas prestam esse serviço. Dentre elas, destacam-se a Oi Velox (Oi), MegaTrinn (TrinnPhone), Speedy (Telefônica), Turbonet MAXX (GVT), NetSuper (CTBC), SuperVIA (Sercomtel), Power GVT (GVT), etc. É importante verificar qual provedor fornece os serviços em sua localidade.

Um trecho muito interessante da história, descrito por Tanenbaum (2003, p. 139), diz que os telefones foram inventados para transportar voz humana e o sistema inteiro foi cuidadosamente otimizado para esse propósito. Os dados sempre estiveram em segundo plano. Esse trecho do livro de Tanenbaum é bastante reflexivo, pois, como podemos perceber, em menos de uma década estamos presenciando as mudanças que estão acontecendo no Brasil e no mundo. Hoje as linhas fixas estão sendo trocadas por linhas móveis, o motivo de muitas famílias terem linha fixa em casa é o acesso à internet.

Faça a pesquisa abaixo e comente no fórum 10 "Atividades da Aula 5".

1. Por que a ADSL faz parte da família xDSL?

2. Quais dados podem trafegar em uma linha telefônica?

3. Qual é a diferença entre *upload* e *download*?

4. Por que é necessário o *modem* na tecnologia ADSL?

5. O que a tecnologia ADSL tem em comum com a tecnologia ATM?

6. Quais os principais provedores da tecnologia ADSL?

7. Quais tecnologias estão surgindo na família DSL?

8. Explique um pouco mais sobre ADSL 2 e ADSL 2+?

5.3 Roteamento

O roteamento é feito por um equipamento denominado *router* ou roteador, que seleciona a rota mais apropriada para encaminhar informações pela rede. O seu principal objetivo é escolher o melhor caminho disponível na rede para encaminhar pacotes.

Quando o modem residencial recebe as informações da central telefônica, ele possui apenas um número IP. Como é possível dividir a internet com vários computadores, se eu tenho apenas um número IP? A resposta é simples, basta fazer o roteamento desse número IP. Para isso, é necessário ter um roteador conectado ao *modem* e configurá-lo. Ele nos permite utilizar o protocolo DHCP, cadastrar máquinas, utilizar políticas de segurança, etc. Com o advento das redes sem fio, normalmente os roteadores possuem quatro portas para conexões de cabo par trançado e transmissão sem fio. Veja na Figura 5.6 um roteador sem fio.

Figura 5.6: Roteador sem fio
Fonte: http://www.hardware.com.br/comunidade/wireless-montar/958751/

O roteador pode fornecer IPs estáticos e dinâmicos às estações de trabalho do cliente. Isto é, o IP estático é fornecido manualmente à estação de trabalho pelo administrador da rede. O IP dinâmico é distribuído, dinamicamente, pelo roteador através do DHCP; o mesmo computador normalmente não recebe o mesmo IP quando se conecta novamente à rede. Veja na Figura 5.7 a representação de uma rede doméstica conectada por um roteador sem fio.

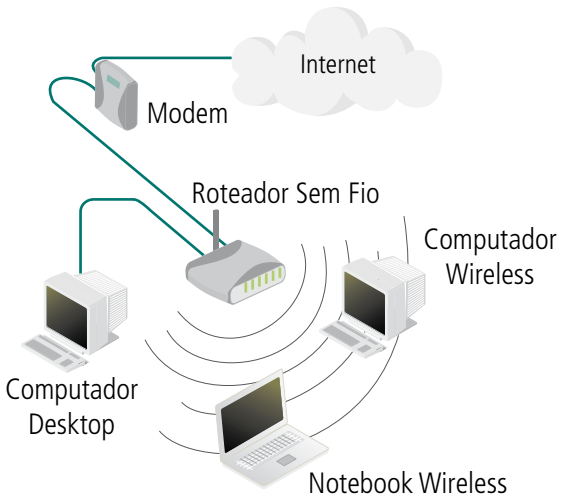


Figura 5.7: Rede conectada por um roteador sem fio.
Fonte: Adaptado de http://www.efetividade.net/2009/06/24/wireless-maior-alcance-para-sua-rede-sem-fio-com-um-repetidor-wi-fi/

Existem vários modelos de roteadores no mercado que são integrados com *modem*, o qual permite receber o sinal da linha telefônica e rotear a internet ao mesmo tempo.

Responda às seguintes perguntas e comente no fórum 10 "Atividades da Aula 5".

1. O que é roteamento?

2. Qual é a diferença entre IP estático e IP dinâmico?

5.3.1 Sistemas autônomos

Uma rede interna administrada por uma entidade é um sistema autônomo. Cada rede interna conectada à internet possui estações de trabalho e roteadores administrados por uma única entidade. Logo, a internet é um conjunto de sistemas autônomos interligados. Na internet atual, Comer (2006, p. 166) descreve que cada grande ISP, provedor de serviço para internet, é um sistema autônomo. Normalmente no Brasil, os ISP são os provedores de internet.

Uma rede interna de uma empresa na China pode acessar, pela internet, os arquivos que estão disponibilizados no *site* do Ifes, servidor que está em outra rede interna. Tudo isso é possível porque essas redes internas estão interligadas por sistemas autônomos.

Quando falamos sobre roteamento na internet, constatamos que é inimaginável haver *web* sem esses equipamentos. A internet possui milhares de roteadores que enviam as mensagens aos seus destinos; esses equipamentos fazem a internet funcionar. Os roteadores que fazem o roteamento global normalmente estão conectados aos provedores de serviço para internet. Entre as principais diferenças do roteador doméstico estão os algoritmos de roteamento, capacidade de processamento, políticas de segurança, etc.

Os protocolos de roteamento se dividem em dois grupos:

- EGP (*Exterior Gateway Protocol*): é um grupo de protocolos utilizados para fazer a comunicação entre os sistemas autônomos, ou seja, entre os roteadores.

- IGP (*Interior Gateway Protocol*): é um grupo de protocolos que fazem a comunicação entre os roteadores de um mesmo sistema autônomo.

Esses dois grupos de protocolos permitem o funcionamento do roteamento global. A Figura 5.8 apresenta exemplos da utilização dos dois grupos de protocolos em sistemas autônomos.

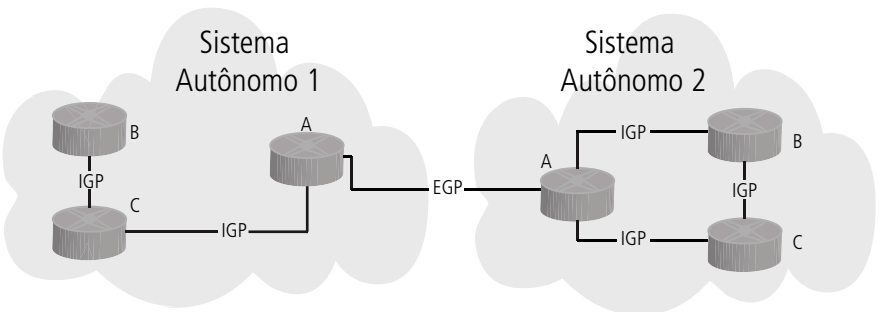


Figura 5.8: Exemplo da utilização do grupo de protocolo EGP e IGP em sistemas autônomos

Fonte: Adaptado de http://gtrh.tche.br/ovni/roteamento3/introducao.htm

Como podemos perceber, o grupo de protocolo IGP é utilizado em roteadores que conectam a mesma rede, como por exemplo a conexão da matriz com a filial. Já o grupo de protocolos IGP é utilizado para interconectar os sistemas autônomos.

Há vários fabricantes de roteadores EGP e BGP; nesse caso, é importante o profissional de TI fazer uma consultoria sobre qual a melhor solução custo x benefício para atender o mercado.

Responda às seguintes perguntas e comente no fórum 10 "Atividades da Aula 5".

1. Qual é a função do roteador?

2. Quais as principais funcionalidades que encontramos na configuração de um roteador?

3. O que são sistemas autônomos?

4. Quais as principais características dos sistemas autônomos?

5. Qual é a diferença entre o grupo de protocolos EGP e BGP?

5.4 VPN

De acordo com Guimarães, Lins e Oliveira (2006, p. 76), a "VPN se apresenta como opção de segurança cada vez mais popular para a interconexão de redes corporativas utilizando a internet". A VPN cria um canal de comunicação com criptografia fim a fim, possibilitando uma conexão mais segura entre duas redes distintas, fornecendo privacidade, integridade e autenticidade aos dados transmitidos na rede.

Diversas empresas interligam suas bases operacionais por meio de um VPN na internet. Um sistema de comunicação por VPN tem um custo de implementação e manutenção insignificante, se comparado ao custo de antigos sistemas de comunicação física. Por esse motivo, muitos sistemas de comunicação estão sendo substituídos por uma VPN, que além do baixo custo, oferece também uma alta confiabilidade, integridade e disponibilidade dos dados trafegados.

O tráfego de dados ocorre pela rede pública utilizando protocolos padrão, não necessariamente seguros.

Sistemas de comunicação por VPN estão sendo amplamente utilizados em diversos setores do mundo inteiro. Veja na Figura 5.9 o exemplo da comunicação por VPN de um cliente com a empresa e a faculdade.

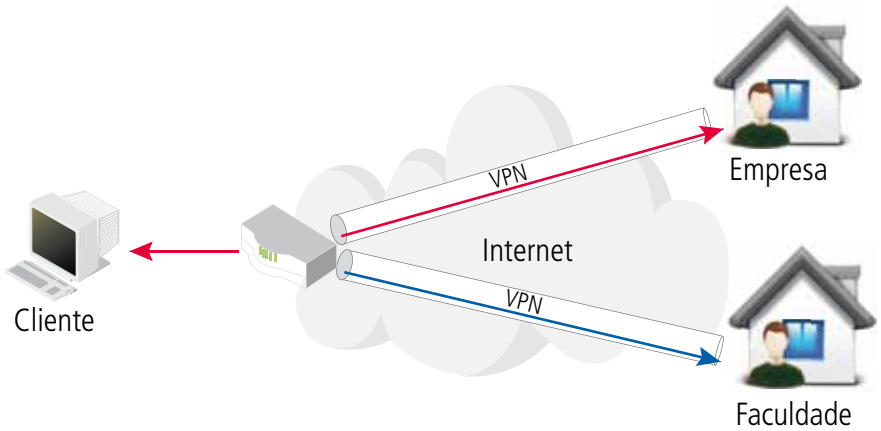


Figura 5.9: Comunicação por VPN de um cliente com a empresa e a faculdade
Fonte: Adaptado de http://www.fc.up.pt/cca/servicos/acesso/vpn/vpn.html?item=265

Na área de segurança de redes, a privacidade é o serviço que permite que somente pessoas autorizadas tenham acesso à informação. Autenticidade é o serviço que assegura uma comunicação autêntica entre o destino e a origem. E a integridade assegura que os dados não serão alterados durante uma transmissão.

Nesse exemplo, o acesso por VPN permite estabelecer uma conexão segura entre o computador do cliente e o servidor da empresa ou da faculdade. A grande vantagem do VPN é que o cliente somente pode ter acesso se ele estiver devidamente autenticado para acessar os recursos da empresa ou faculdade.

As VPNs usam protocolos de criptografia por tunelamento que fornecem a confidencialidade, autenticação e integridade necessárias para garantir a privacidade das comunicações requeridas. Quando adequadamente implementados, esses protocolos podem assegurar comunicações seguras através de redes inseguras. Segue na Figura 5.10 um exemplo de conexão VPN entre uma rede corporativa e um escritório filial.

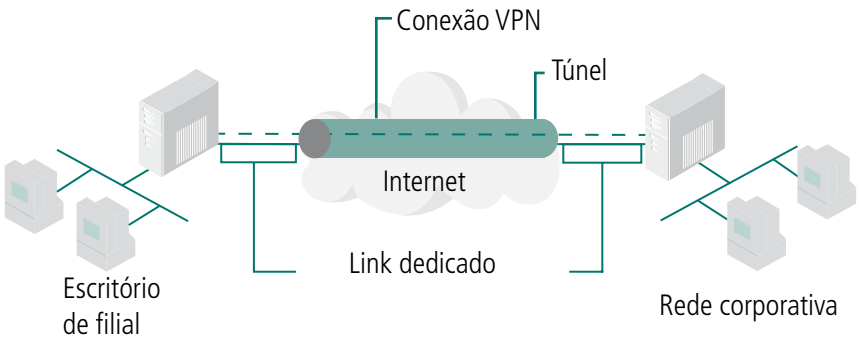


Figura 5.10 Conexão VPN entre uma rede corporativa e um escritório filial
Fonte: http://www.portalchapeco.com.br/jackson/vpn.htm

Os principais protocolos que permitem fazer uma VPN são:

- PPP (*Point-to-Point Protocol* ou Protocolo Ponto a Ponto);
- PPTP (*Point-to-Point Tunneling Protocol* ou Protocolo de Tunelamento ponto a ponto);

- L2TP *(Layer* 2 *Tunneling Protocol* ou Protocolo de Tunelamento de duas camadas);

- MPLS (*Multiprotocol Label Switching* ou Protocolo de Comutação de Rótulo);

- IPsec (*IP Security* ou IP seguro);

Responda às seguintes perguntas e comente no fórum 10 "Atividades da Aula 5".

1. O que é uma VPN?

2. Quais as vantagens de utilizar uma VPN?

3. Quais os principais protocolos da VPN?

4. Explique o que é:

a) Tunelamento.

b) Privacidade.

c) Autenticidade.

d) Integridade.

Resumo

As tecnologias ATM, ADSL, VPN e Roteamento permitem interconectar as redes a longas distâncias. Entender como funciona cada uma dessas tecnologias torna o profissional da TI mais completo.

O protocolo ATM possui uma flexibilidade muito grande com os meios físicos, suporta diversos tipos de aplicativos, etc.; dentre suas principais vantagens, podemos destacar a alta velocidade e o Qos.

A tecnologia ADSL ganha novos usuários todos os dias; essa é a conexão banda larga mais utilizada no Brasil e uma das mais conhecidas no mundo. Ela funciona a partir de um provedor que disponibiliza a linha telefônica para ser conectada ao *modem*, que por sua vez conecta o computador à internet.

O roteador é o equipamento responsável por distribuir as informações pela rede, indicando a melhor rota para encaminhar os pacotes. Os sistemas autônomos são formados por roteadores, e a internet é o conjunto de vários sistemas autônomos interconectados.

A VPN é uma rede de comunicação privada, normalmente utilizada por uma empresa ou um conjunto de empresas ou instituições. Ela é constituída sobre uma rede de comunicação pública, como por exemplo, a internet. Essa área da tecnologia é muito promissora para profissional de TI.

Atividades de aprendizagem

Resolva os exercícios abaixo e comente no fórum 10 "Atividades da Aula 5".

1. Em relação à tecnologia ATM, explique o que é:

a) VCI.

b) VPI.

c) Qos.

d) Célula.

e) UNI.

f) NNI.

2. As tecnologias ADSL e ATM trabalham juntas. Explique esta afirmação.

3. O que é provedor de acesso à internet?

4. Por que é necessário fazer o roteamento de uma rede de computadores?

5. É correto afirmar que a internet é um conjunto de sistemas autônomos? Justifique sua resposta.

6. Quando é necessário utilizar uma VPN?

7. Quais são os principais requisitos na segurança de uma rede VPN?

8. Explique como funciona a internet, descrevendo-a com as tecnologias estudadas nesta aula.

9. Quais as vantagens da ADSL 2 e ADSL 2+ para a tecnologia ADSL?

Aula 6 – Segurança em redes *Wi-Fi*

Objetivos

Apresentar as redes *Wi-Fi*, seus padrões e a importância de mantê-las seguras.

Demonstrar como identificar o endereço MAC das interfaces de rede e como esse endereço pode ser usado para adicionar mais segurança em ambientes *wireless*.

Compreender as vulnerabilidades que possui o protocolo WEP.

Apresentar as chaves de criptografia seguras WPA e WPA2.

A tecnologia é muito impressionante! Em poucos anos de uso comercial, os nomes *Wi-Fi*, *Wireless*, *HotSpot* e sem fio tornaram-se normais em nosso dia a dia. Nesta aula, estudaremos as principais soluções de segurança em redes *Wi-Fi*. A instalação de uma rede *Wi-Fi* é simples. Porém, se ela não for bem configurada e administrada, as informações pertencentes à rede estarão extremamente vulneráveis. O profissional de TI ético, qualidade de suma importância no mercado de trabalho, não invade nenhuma rede de computadores, mas as protege.

6.1 Redes *Wi-Fi*

O termo *Wi-Fi* deriva da abreviação *Wireless Fidelity* ou Fidelidade sem Fio. As redes sem fio funcionam através de ondas de rádio, assim como telefones e televisores. De acordo com Rufino (2005, p. 15):

> As redes sem fio são algo novo na vida da maioria das pessoas e, diferentemente das redes cabeadas, em que era necessário conhecimento técnico um pouco mais específico, a montagem e instalação de redes *Wi-Fi* são absolutamente factíveis por um usuário iniciante.

Veja no *link* a seguir http://olhardigital.uol.com.br/produtos/central_de_videos/voce-sabe-como-o-wi-fi-funciona, como funcionam as redes *Wi-Fi*. Comente esse vídeo no Ambiente Virtual de Ensino-Aprendizagem, no fórum 09 "Vídeos da Aula 6".

As redes sem fio estão divididas em várias tecnologias, sendo elas: Infravermelho, *Bluetooth*, *Wi-Fi* "tecnologia que estamos estudando nesta aula", *Wimax*, GSM, etc.

Para fazer uma rede sem fio é necessário um *Access Point* ou um Ponto de Acesso, isto é, um adaptador sem fio para transformar as informações em ondas de rádio para ser emitidas através da antena. Veja na Figura 6.1 o símbolo padrão para ambientes *Wi-Fi*.

Figura 6.1: Símbolo padrão de ambientes *Wi-Fi*
Fonte: http://www.techlider.com.br/2011/02/detectados-pela-primeira-vez-casos-de-alergia-a-wi-fi/

Para a estação de trabalho se conectar à rede *Wi-Fi*, é necessário ter uma interface de rede *Wi-Fi*. Veja na Figura 6.2 uma interface de rede *Wi-Fi*, modelo PCI.

Figura 6.2: Interface de rede *Wi-Fi*, modelo PCI
Fonte: http://xtech.com.br/lojaxt/placa-rede-wireless-mbps-3com-p-8269.html

Os principais padrões das redes *Wi-Fi* são:

- IEEE 802.11a: que opera na frequência de 5 GHz, com a taxa de transmissão de 54 Mbps;
- IEEE 802.11b: que opera na frequência de 2.4 GHz, com a taxa de transmissão de dados de 11 Mbps;
- IEEE 802.11g: Atualmente, a mais utilizada no Brasil, operando na frequência de 2.4 GHz, com a taxa de transferência de 54 Mbps;

- IEEE 802.11n: É o padrão que esta substituindo o padrão 802.11g, opera nas frequências de 2.4 GHz a 5GHz, com a taxa de transmissão de dados variando de 65 Mbps a 600 Mbps.

Reportagem sobre *Wireless*-N no *link* http://olhardigital.uol.com.br/produtos/central_de_videos/acelere-e-va-mais-longe-com-wireless-n e comente esse vídeo no Ambiente Virtual de Aprendizagem no fórum 09 "Vídeos da Aula 6".

O que é *HotSpot*? Você já entrou em um local *HotSpot*? Este é o nome dado ao local onde a tecnologia *Wi-Fi* está disponível de graça. São encontrados, geralmente, em locais públicos como cafés, restaurantes, hotéis e aeroportos. É possível conectar-se à internet utilizando qualquer computador portátil que esteja adaptado com uma interface de rede *Wireless*. Veja na Figura 6.3 a imagem utilizada para indicar que o ambiente é *HotSpot*.

Figura 6.3: Imagens utilizadas para indicar que o ambiente é *HotSpot*
Fonte: http://www.billingwarnet.com/hotspot.html

Para entender melhor como funciona a comunicação *Wireless* com as estações clientes de uma rede, segue, na Figura 6.4, o exemplo de uma conexão *Wi-Fi*.

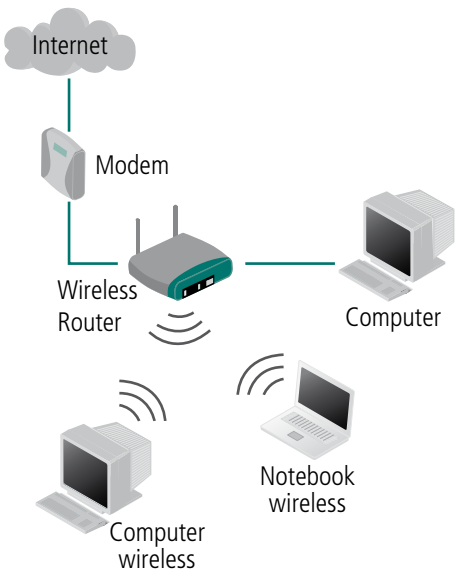


Figura 6.4: Exemplo de uma rede *Wi-Fi*
Fonte: http://professorwellingtontelles.blogspot.com/2009/10/como-criar-uma-rede-com-windows-xp.html

De acordo com Rufino (2005, p. 16), as facilidades de instalação de uma rede sem fio geram um risco associado; portanto toda essa simplicidade de instalação tem feito com que muitas redes *Wi-Fi* (caseiras ou não) sejam montadas com padrões de fábrica, ou seja, completamente imunes a vários tipos de ataque. Nas seções 6.2, 6.3 e 6.4, apresentam-se quais tipos de segurança podem ser configurados em uma rede *Wireless* para prevenir contra invasões.

Responda às seguintes perguntas e comente no fórum 11 "Atividades da Aula 6".

1. O que significa *Wi-Fi*?
2. Quais as vantagens em utilizar redes *Wi-Fi*?
3. Como a informação é transmitida pela rede sem fio?
4. Quais são os principais padrões *Wi-Fi*?
5. O que é *HotSpot*?

6.2 MAC

O endereço MAC, *Media Access Control* ou Controle de Acesso ao Meio, é o endereço físico da interface de rede. Esse endereço possui 48 *bits* e é representado por 12 dígitos hexadecimais agrupados dois a dois. Ex.: 02:22:26:1C:F5:91. Atualmente, existem no mercado várias interfaces de redes, que podem ser placas de rede par trançado, *Wireless*, fibra óptica, etc.

De acordo com Tanembaum e Wetherall (2011, p. 177):

"Uma característica interessante dos endereços de origem da estação é que eles são globalmente exclusivos, atribuídos de forma centralizada pela IEEE para garantir que duas estações em qualquer lugar do mundo nunca tenham o mesmo endereço."

Para encontrar o endereço físico da interface de rede no Windows, é necessário acessar o *prompt* de comando do MS-DOS. Para isso, vá até o menu iniciar/ executar e digite **cmd** no "Windows Vista ou Seven", caso seja o Windows XP, faça o percurso iniciar/todos os programas/ acessórios (*prompt* de comando). Aparecerá a janela do MS-DOS, como se pode ver na Figura 6.5.

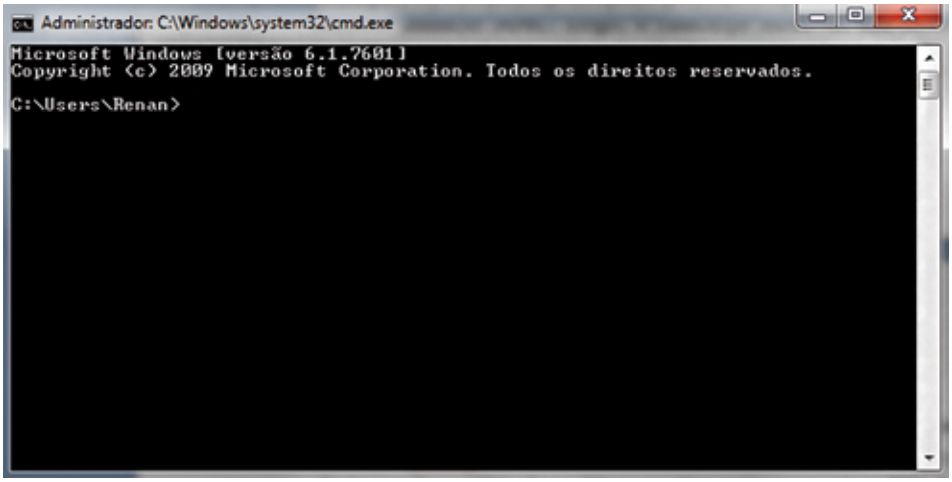


Figura 6.5: Janela do MS-DOS
Fonte: Windows Vista

Dentro dessa janela, digite o comando *getmac ou ipconfig/all*; com esses comandos aparecerá o endereço MAC de sua interface de rede na frente da palavra endereço físico.

Por que esse endereço é tão importante? Dentre as várias utilidades do endereço MAC, é importante destacar o quanto ele é importante para a segurança da rede cabeada e sem fio. Com ele é possível cadastrar no *Firewall Wi-Fi* / *Wi-Fi* / *Proxy*, roteador sem fio, etc., qual máquina terá acesso aos serviços oferecidos na rede; se for o caso, não permitir ou restringir o acesso à rede. Veja na Figura 6.6 o endereço MAC de uma estação de trabalho sendo cadastrada em um roteador.

Figura 6.6: Cadastro de endereço MAC em roteador sem fio
Fonte: Cisco

Muitos bancos cadastram o endereço MAC da máquina do cliente, para terem acesso ao *site*. Isso permite garantir que o acesso está partindo da máquina do cliente, e não de terceiros. Se a máquina estragar ou for roubada, o cliente entra em contato com o banco e ele bloqueia o MAC do cliente; dessa maneira, a máquina não terá acesso ao *site*.

Responda às seguintes perguntas e comente no fórum 11 "Atividades da Aula 6".

1. O que é o endereço MAC?
2. Como é formado o endereço MAC?
3. Como o endereço MAC pode ser útil na segurança de uma rede sem fio?

6.3 WEP

Nas redes cabeadas, o acesso à informação requer comunicação física por algum componente da rede. Na rede sem fio, basta ter uma antena que receba o sinal para ter acesso à rede, caso não tenha segurança. Por essa razão, inicialmente o protocolo utilizado para resolver esse problema foi o *Wired Equivalent Privacy* (WEP), ou Privacidade Equivalente com Fio. Esse protocolo está presente em todos os produtos que estão no padrão *Wi-Fi*.

De acordo com Rufino (2005, p. 36), "WEP é um protocolo que utiliza algoritmos simétricos; portanto existe uma chave secreta que deve ser compartilhada entre as estações de trabalho e o concentrador, para cifrar e decifrar as mensagens trafegadas". Os critérios que foram levados em consideração para o desenho do protocolo foi ser suficientemente forte, autossincronismo, requerer poucos recursos computacionais, exportável e de uso opcional.

É possível configurar a chave WEP com 64 *bits* ou 128 *bits*. Veja na Figura 6.7 um roteador da Linksys sendo configurado com a chave de criptografia WEP.

Figura 6.7: Roteador sendo configurado com a chave de criptografia WEP
Fonte: Cisco

A chave WEP passou a ser vulnerável com o passar dos anos e foi perdendo a credibilidade. Várias ferramentas foram desenvolvidas para descobrir as chaves WEP; dentre elas destacam-se alguns *softwares* como: Airsort, WepCrack, WepAttack, Wep_tools, Weplab, Aircrack, etc. Esses *softwares* podem ser utilizados para descobrir a chave de criptografia WEP de uma rede e invadi-la, com maior ou menor grau de eficiência.

Logo, essa chave não é recomendada para ser utilizada em uma rede sem fio, já que a possibilidade de descobrir a criptografia WEP é grande.

Responda às seguintes perguntas e comente no fórum 11 "Atividades da Aula 6".

1. O que é WEP?
2. É possível configurar uma chave WEP com quantos *bits*?
3. Quais programas podem quebrar a chave WEP com menor ou maior grau de eficiência?

6.4 WPA e WPA2

Com os problemas de segurança na chave WEP, foi lançado o protocolo WPA, *Wi-Fi Protected Access,* ou Acesso Protegido sem Fio. Segundo Rufino (2005, p. 37):

> Ela atua em duas áreas distintas: a primeira, que visa substituir completamente o WEP, trata da cifração dos dados objetivando garantir a privacidade das informações trafegadas; e a segunda, foca a autenticação do usuário (área não coberta efetivamente pelo padrão WEP).

Veja no *link*: http://olhardigital.uol.com.br/produtos/central_de_videos/rede_wireless_como_configurar_a_sua_com_seguranca, uma reportagem sobre como configurar a sua rede *Wireless* com segurança. Comente esse vídeo no Ambiente Virtual de Ensino-Aprendizagem fórum 09 "Vídeos da Aula 6".

De acordo com a Linksys (2011), a WPA usa criptografia de chave dinâmica, o que significa que a chave muda constantemente e torna a invasão de uma rede sem fio mais difícil do que a WEP. A WPA é considerada um dos mais altos níveis de segurança sem fio para a rede e é recomendada se os seus dispositivos suportarem esse tipo de criptografia. Veja na Figura 6.8 o roteador da Linksys sendo configurado com a chave de criptografia WPA.

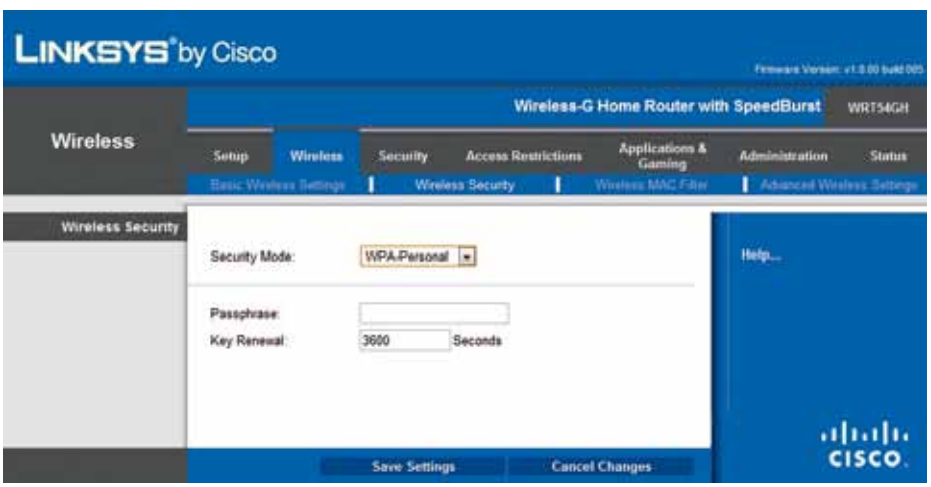


Figura 6.8: Roteador sendo configurado com a chave de criptografia WPA
Fonte: Cisco

Na WPA, há duas versões que usam diferentes processos para autenticação:

- TKIP (*Temporal Key Integrity Protocol* ou Protocolo de Integridade de Chave Temporária), que é um mecanismo usado para criar criptografia de chave dinâmica e autenticação mútua. O TKIP fornece os recursos de segurança que corrigem as limitações da WEP. Como as chaves estão sempre mudando, ele proporciona um nível muito alto de segurança para sua rede.

- O EAP (*Extensible Authentication Protocol* ou Protocolo de Autenticação Extensivel) é usado para troca de mensagens durante o processo de autenticação. Ele utiliza Tecnologia 802.1x Server para autenticar usuários via servidor RADIUS, *Remote Authentication Dial-In User Service* ou Serviço de usuário discado para autenticação remota. Ele fornece segurança de nível industrial para sua rede, mas requer um servidor RADIUS.

Os roteadores mais novos oferecem segurança WPA2. A WPA2 é compatível com a WPA, mas oferece maior nível de segurança. Para a Linksys (2011), ela cumpre os altos padrões de muitos órgãos governamentais. Se o roteador e o computador suportarem WPA2, esta deve ser a sua escolha. Veja na Figura 6.9 o roteador da Linksys sendo configurado com a chave de criptografia WPA2.

Figura 6.9: Roteador sendo configurado com a chave de criptografia WPA2
Fonte: Cisco

O WPA2 é a segunda geração da WPA, mas não foi criado para solucionar nenhuma limitação da WPA. Ele é compatível com versões anteriores de produtos que suportam WPA. A principal diferença entre a WPA original e a WPA2 é que a WPA2 exige AES (*Advanced Encryption Standard*) para criptografia de dados, enquanto a WPA original usa TKIP. O AES fornece segurança suficiente para cumprir os padrões de alto nível de muitos órgãos governamentais federais.

Existem vários fabricantes de roteador sem fio no mercado; nesta aula, o roteador Linksys foi utilizado como exemplo.

Responda às seguintes perguntas e comente no fórum 11 "Atividades da Aula 6".

1. Qual foi a motivação do desenvolvimento do WPA?
2. O que o WPA oferece de segurança em uma rede sem fio?
3. Qual é a diferença entre WPA-TKIP e EAP?
4. O WPA2 é compatível com versões anteriores do WPA?
5. Qual dessas opções de criptografia em redes sem fio é a melhor atualmente? Justifique sua resposta.

Resumo

A adoção das redes sem fio traz muitas vantagens, e em alguns casos é inevitável. É fundamental que o administrador de rede ou usuário doméstico entenda as implicações de segurança de cada escolha na configuração das redes *Wi-Fi*.

A IEEE é responsável por definir as faixas de endereço MAC que os fabricantes colocam nas interfaces de redes. Esse controle é feito para não haver interfaces de redes com o mesmo endereço MAC. Logo, o endereço MAC de sua interface de rede é único na internet. Essa característica fornece muita segurança em redes sem fio ao cadastrar o endereço MAC das estações de trabalho no roteador sem fio.

Para colocar segurança nas redes sem fio *Wi-Fi,* inicialmente foi projetada a chave de criptografia WEP. Mas, com o passar dos anos, ela passou a perder a credibilidade por não ser mais segura. Muitos *softwares* são capazes de encontrar a chave WEP das redes sem fio e, consequentemente, isso torna a rede vulnerável.

Para suprir a vulnerabilidade da rede sem fio, foi criada a chave de segurança WPA, evolução da WEP. A chave WPA permite fazer a criptografia por TKIP e EAP. Apesar de não haver limitação na chave WPA, foi criada a chave WPA2, que fornece maior segurança em redes sem fio.

Atividades de aprendizagem

Resolva os exercícios abaixo e os comente no fórum 11 "Atividades da Aula 6".

1. É correto afirma que existem interfaces de rede com o endereço MAC igual? Justifique sua resposta.

2. Como podemos utilizar o endereço MAC para tornar a rede cabeada ou sem fio mais segura?

3. Cite quatro tecnologias de redes sem fio e as descreva.

4. Normalmente, em quais locais encontramos redes *HotSpot*?

5. O que é criptografia?

6. A chave WEP é segura? Justifique sua resposta.

7. Quais a principais vantagens do WPA sobre o WEP?

8. O WPA2 foi criado para suprir limitações do WPA?

Referências

ALBUQUERQUE, F. **TCP/IP – Internet:** protocolos e tecnologias. Rio de Janeiro: Axcel Books, 2001.

COMER, D. E. **Interligação de redes com TCP/IP.** Rio de Janeiro: Elsevier, 2006.

FALBRIARD, C. **Protocolos e aplicações para redes de computadores**. São Paulo: Érika, 2002.

GUIMARÃES, A. G.; LINS, R. D.; OLIVEIRA, R. **Segurança com redes privadas virtuais VPNs.** Rio de Janeiro: Brasport, 2006.

IANA. Internet Assigned Numbers Authority. IANA. Disponivel em: <http://www.iana.org/>. Acesso em: 12 jul. 2011.

ICANN. ICANN. Corporação da Internet para Atribuição de Nomes**.** Disponivel em: <http://www.icann.org.br/new.html>. Acesso em: 16 jul. 2011.

LINKSYS**. WPA e WPA2** Disponível em: <http://www.linksysbycisco.com/LATAM/pt/learningcenter/WPAandWPA2-LApt>. Acesso em: 7 set. 2011.

RUFINO, N. M. D. O. **Segurança em redes sem fio:** aprenda a proteger suas informações em ambientes *Wi-Fi* e *Bluetooth*. São Paulo: Novatec, 2005.

SCRIMGER, R. et al. **TCP/IP:** a Bíblia**.** Rio de Janeiro: Elseiver, 2002.

SHIPLEY**,** D.; SCHWALBE, W. **Enviar:** o guia essencial de como usar o *e-mail* com inteligência e elegância**.** Rio de Janeiro: Sextante, 2008.

TANENBAUM, A. S. **Redes de computadores.** Rio de Janeiro: Campus, 2003.

_____; WETHERALL, D. **Redes de computadores.** São Paulo: Pearson Prentice-Hall, 2011. v. 5.

Currículo do professor-autor

Renan Osório Rios é mestre em Modelagem Matemática e Computacional pelo Centro Federal de Educação Tecnológica de Minas Gerais (CEFET-MG). Graduado em Sistemas de Informação pelo Centro Universitário do Espírito Santo (UNESC). Técnico de Informática pelo Centro Federal de Educação Tecnológica do Espírito Santo (CEFET-ES).

Atuou no suporte técnico da empresa Exata Informática, lecionou no instituto Modal e na Point Informática. Ficou em 3º lugar no Desafio Sebrae no Espírito Santo em 2007. Em seu mestrado, publicou 7 artigos e 3 resumos em congressos no Brasil, e recebeu a menção honrosa de pesquisa ambiental pela prefeitura de Vitória. Atualmente, é professor do Instituto Federal do Espírito Santo (Ifes) - Campus Colatina e coordenador da empresa júnior *Tech Inside*. O *link* para acessar o currículo Lattes é **http://lattes.cnpq.br/3555360133532677**.

ISBN 978-85-62934-36-0