

Redes de Computadores

Milena Cristina França

Florianópolis
2010



Copyright © 2010, Instituto Federal de Santa Catarina / Sistema ETEC. Nenhuma parte deste material poderá ser reproduzida, transmitida e gravada, por qualquer meio eletrônico, por fotocópia e outros, sem prévia autorização, por escrito, dos autores.

França, Milena Cristina

Redes de Computadores / Milena Cristina França / Florianópolis:
Publicações do IF-SC, 2010.

84 p. : il. ; 00 cm.

Inclui Bibliografia

ISBN:

1. Informática. 2. Microcomputadores. 3. Rede de computadores – Internet. 4. Protocolo TCP/IP.

Sistema de Bibliotecas Integradas do IF-SC

Biblioteca Dr. Hercílio Luz – Campus Florianópolis

Catalogado por: Augiza Karla Boso – CRB14/1092

Rose Mari Lobo Goulart – CRB 14/277

Organização de conteúdo:

Andrino Fernandes

Elaine Luz Barth

André de Oliveira Leite

Comissão Editorial:

Hamilcar Boing

Andrino Fernandes

Elaine Luz Barth

Produção e design instrucional:

André de Oliveira Leite

Elaine Luz Barth

Diagramação:

Hudson Ricardo Borges

Capa:

Lucio Baggio

Revisão ortográfica:

Marcos Pessoa

Sumário

Capítulo 1 - Introdução às redes de computadores	9
Capítulo 2 - Tipos de redes	13
2.1 Redes Locais (Local Area Network - LAN)	15
2.2 Redes Metropolitanas (Metropolitan Area Network - MAN)	15
2.3 Redes de Longa Distância (Wide Area Network - WAN)	15
Capítulo 3 - Topologias de redes	17
3.1 Principais Topologias	19
Capítulo 4 - Meios de transmissão	23
4.1 Par Trançado	25
4.2 Conectores Utilizados nos Cabos de Par Trançado	27
4.3 Confeccionando um Cabo de Rede	28
4.4 Fibra Ótica	29
4.5 Redes sem Fio (Wireless)	30
Capítulo 5 - Modelo de protocolo TCP/IP	33
Capítulo 6 - Protocolo TCP/IP	37
6.1. Camada de Aplicação	40
6.2 Camada de Transporte	42
6.3 Camada de Internet	43
6.4 Camada de Interface de rede	46
Capítulo 7 - Elementos de uma rede	49
7.1 Placas de rede	51
7.2 Hubs	52
7.3 Repetidores	52
7.4 Switches	53
7.5 Bridges (Pontes)	53
7.6 Roteadores	54
7.7 Gateway	55
Capítulo 8 - Modelos de rede	59
8. 1 Redes Ponto a Ponto	61
8.2 Redes Cliente-Servidor	61
8.3 Tipos de Servidores mais Comuns	62
Apêndice	65
Referências Bibliográficas	83



Apresentação

Prezados estudantes,

Certamente vocês já sabem que é impossível imaginar que o mundo moderno sobreviva ou mesmo exista, sem a existência da comunicação entre as pessoas. Hoje, há computadores interligados por toda a nossa volta, e eles estão presentes em diversas tarefas do nosso cotidiano. A crescente evolução nos sistemas computacionais faz com que um profissional com conhecimentos em redes de computadores, seja cada vez mais requisitado.

Na unidade curricular Redes de Computadores iremos aprofundar nossos conhecimentos exatamente sobre redes de computadores. O objetivo geral desta disciplina é capacitá-lo (a) para adquirir novas habilidades e competências para participar tanto na instalação, configuração quanto na manutenção de um projeto de rede local de computadores.

A cada capítulo você irá vivenciar, de forma panorâmica, assuntos muito relevantes no estudo de redes de computadores. Os computadores fazem parte da nossa vida e muitos de nós temos mais de uma máquina em nossas casas, quer seja um computador pessoal ou notebook... Para que você possa aprimorar o seu aprendizado proponho uma sugestão bastante útil. Que tal você criar a sua rede doméstica para praticar seus conhecimentos?

Ao final de cada capítulo, você encontrará exercícios de fixação e ao final, um apêndice com os laboratórios de aula. Participe das atividades propostas e empenhe-se. Contribua e interaja com seus colegas nos fóruns. Estou à sua disposição para dirimir dúvidas e para qualquer outra necessidade relacionada a disciplina.

Bom Estudo!
Profª Milena Cristina França



CAPÍTULO

1

**INTRODUÇÃO ÀS
REDES DE COMPUTADORES**



Objetivo

Nesta unidade você deverá ser capaz de conceituar redes de computadores bem como identificar e relacionar o significado e a importância das redes de computadores no mundo atual.



Introdução às redes de computadores

Atualmente, é inegável que todos nós vivemos cercados por computadores e que eles estão sempre presentes em diversas tarefas do nosso cotidiano. Escolas, bibliotecas, supermercados,... Todos usam algum tipo de rede para atualizar informações de forma eficiente, rápida e segura. As redes estão em toda parte, tornando-se tão populares quanto o próprio PC.

Por definição, uma rede de computadores é um conjunto de computadores (e equipamentos associados) interligados por meios de transmissão para garantir a troca de informação entre eles.



Fig.1 - Redes de Computadores

A partir da implantação de uma rede de computadores você pode:

- Manter apenas uma impressora em um departamento ou escritório, centralizar arquivos importantes e compartilhá-los com vários computadores.
- Distribuir e controlar o acesso à internet (em vez de usar conexões em cada computador).
- Trocar mensagens entre computadores, mesmo que estejam em locais distantes.
- Interconectar computadores (um avanço incalculável de benefícios que um micro isolado nunca poderia apresentar).

Resumo

Uma rede de computadores é um conjunto de computadores (e equipamentos associados) interligados por meios de transmissão para garantir uma troca de informação entre eles. A interconexão entre computadores gera avanço incalculável de benefícios que um micro isolado nunca poderia apresentar.

Atividades de Aprendizagem

1. Complete:

Por definição, uma rede de computadores é um conjunto de computadores e equipamentos associados interligados por _____ para garantir a troca de _____ entre eles.

2. Responda:

Quais são os possíveis benefícios gerados por uma rede de computadores?

CAPÍTULO

2

TIPOS DE REDES



Objetivo

Nesta unidade você deverá conhecer os tipos de redes, a sua abrangência e ao final identificar as limitações dos tipos de redes mais comuns.

Em um projeto de redes é necessário identificar o escopo da rede, ou seja, ter uma idéia da abrangência das redes de computadores. Desse modo, os tipos de redes mais conhecidos são: LAN, MAN e WAN.

2.1 Redes Locais (Local Area Network - LAN)

As redes locais caracterizam-se por permitir a interconexão de um conjunto de dispositivos dentro de uma pequena área geográfica, em geral, distâncias entre 100m e 25 km. Estamos falando, portanto, de um conjunto de equipamentos interligados (micros, impressoras, etc.), localizados num mesmo prédio ou sala.

Outras características típicas associadas a redes locais são:

- altas taxas de transmissão,
- geralmente pertencem a propriedade privada.

2.2 Redes Metropolitanas (Metropolitan Area Network - MAN)

As redes metropolitanas interligam computadores localizados dentro de uma área geograficamente limitada como uma cidade, um campus universitário ou um conjunto de prédios (40 a 80 km). Uma rede metropolitana apresenta características semelhantes às redes locais, sendo que as MANs em geral, cobrem distâncias maiores que as LANs operando em velocidades maiores.

2.3 Redes de Longa Distância (Wide Area Network - WAN)

As redes de longa distância surgiram da necessidade de se compartilhar recursos por uma comunidade de usuários geograficamente dispersos.

As redes metropolitanas caracterizam-se por possuírem um custo de comunicação elevado devido a uso de meios, tais como, linhas telefônicas, satélites e microondas, baixas velocidades de transmissão (dezenas de Kilobits, podendo chegar a Megabits/segundo), e geralmente são de propriedade pública.

Resumo

Os tipos de redes mais conhecidos são: LAN, MAN e WAN.

- LAN: conjunto de equipamentos interligados (micros, impressoras, etc.), localizados num mesmo prédio ou sala.
- MAN: Interligam computadores localizados dentro de uma área geograficamente limitada como uma cidade, um campus universitário ou um conjunto de prédios.
- WAN: Compartilham recursos por uma comunidade de usuários geograficamente dispersos.

Atividades de Aprendizagem

1. Relacione as colunas:

(a) LAN

(b) MAN

(c) WAN

() Usa meios de comunicação como satélites e micro-ondas.

() Permite interconexões de dispositivos, dentro de uma pequena área geográfica, em geral, distâncias entre 100m e 25 km.

() Interliga computadores dentro de uma área geograficamente limitada como uma cidade, um campus universitário ou um conjunto de prédios (40 a 80 km).

2. Complete:

As redes _____ possuem como características típicas: altas taxas de transmissão e em geral são de propriedade privada.

CAPÍTULO

3

TOPOLOGIAS DE REDES



Objetivo

Nesta unidade você deverá ser capaz de compreender a importância da topologia de rede na construção de sistemas de comunicação e a reconhecer as vantagens e desvantagens das principais topologias de redes.

Topologias de Rede

Entende-se por topologia de rede a forma com que os enlaces físicos e os nós de comunicação (ponto de conexão com a rede) estão organizados.

Podemos diferenciar dois tipos de topologias:

- uma topologia lógica, que é aquela observada sob o ponto de vista das interfaces das estações com a rede;
- uma topologia física, que diz respeito à configuração física utilizada na instalação da rede.

Por exemplo, a utilização de hubs nas instalações físicas das redes corresponde, fisicamente, a implantação de uma topologia em estrela. Porém, a utilização de hubs não exige necessariamente, que as interfaces das estações com a rede o percebam como uma topologia em estrela. O funcionamento continua a ser como no acesso a um barramento ou a um anel.

IMPORTANTE!

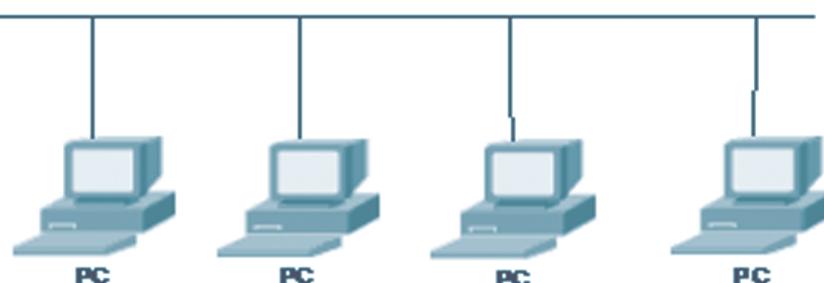
A escolha da topologia apropriada influencia em fatores como: desempenho, segurança e confiabilidade da rede. E também depende da distância entre os nós e do tamanho da rede.

3.1 Principais Topologias

Em todos os tipos de redes, as três topologias mais utilizadas são: Barramento, Estrela e Anel.

a) Barramento (Bus)

Todos os computadores são conectados a um barramento compartilhado. Nessa topologia, cada nó (equipamento) conectado à barra pode ouvir todas as informações transmitidas. Porém, um cabo desconectado poderá fazer a rede cair. A topologia em barramento é pouco utilizada atualmente.



19

Fig.2 - Topologia em Barramento

b) Estrela (Star)

Nesse tipo de topologia cada nó (computador) se conecta a um nó central (comutador ou switch) utilizando uma conexão independente dos outros computadores. Ela é bastante utilizada atualmente, principalmente em redes de pequeno porte. É de fácil manutenção e de fácil identificação de problemas, entretanto, uma falha do nó central pode desativar toda a rede.

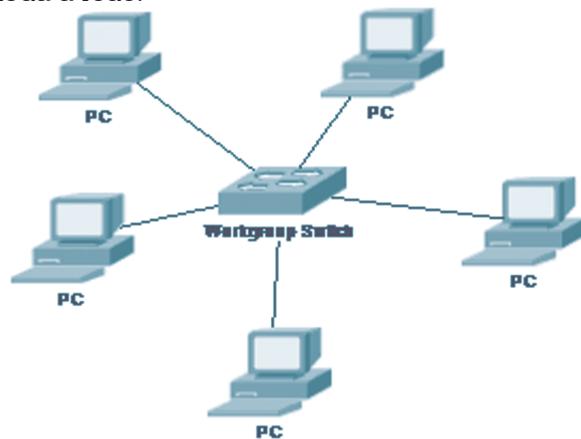


Fig.3 - Topologia em Estrela

c) Anel (Ring)

PARA REFLETIR

Quando as redes token ring foram criadas, elas ofereciam uma taxa de transmissão bem elevada, porém a adição de um número muito grande de máquinas no anel causava problemas de atraso, ruído e sincronização. Por isso, essa topologia é pouco utilizada atualmente para redes locais.

Na topologia em anel, as estações estão conectadas a um mesmo circuito, formando um círculo fechado. As redes conhecidas como Token Ring (criadas pela IBM) são as mais famosas.

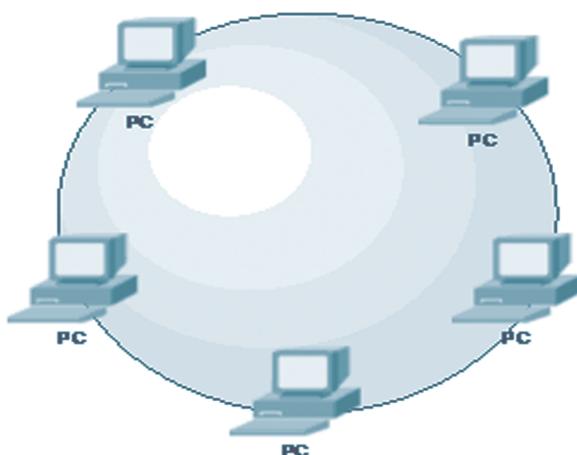


Fig.4 - Topologia em Anel

Topologias de Rede

Veja em seguida, as vantagens e desvantagens das principais topologias de redes.

	Aspectos Positivos	Aspectos Negativos
Topologia Barramento	<ul style="list-style-type: none">• Fácil expansão• Falha de uma estação não afeta as outras	<ul style="list-style-type: none">• Difícil detecção de falha• A rede fica mais lenta em períodos de uso intenso.
Topologia Estrela	<ul style="list-style-type: none">• Simplicidade da conexão• Fácil detecção de falha• Falha de uma estação ou de um cabo não afeta as outras.	<ul style="list-style-type: none">• Dependência de um elemento central;• Custo inicial maior.
Topologia Anel	<ul style="list-style-type: none">• Permite um grande número de estações• Facilidade de expansão	<ul style="list-style-type: none">• Falha numa estação ocasiona parada total na rede.

Tabela 1- Topologia em Barramento

Resumo

A Topologia de Rede é a forma com que os enlaces físicos e os nós de comunicação (ponto de conexão com a rede) estão organizados. Pode ser: Topologia física e lógica. Em todos os tipos de redes, as três topologias mais utilizadas são: Barramento (Bus), onde todos os computadores são conectados a um barramento compartilhado; Estrela (Star), onde cada nó (computador) se conecta a um nó central (comutador ou switch) utilizando uma conexão independente dos outros computadores e Anel (Ring) onde as estações estão conectadas a um mesmo circuito, formando um círculo fechado.



Redes de Computadores

CAPÍTULO

4

MEIOS DE TRANSMISSÃO



Objetivo

Nesta unidade você deverá identificar os meios de transmissão mais comuns nas redes locais e analisar os possíveis problemas dos meios de transmissão.

São diversos os meios de transmissão para dados. Vamos focalizar os meios de transmissão mais comuns nas redes locais e apontar algumas características associadas aos meios de transmissão.

São elas:

- **Atenuação:** Qualquer que seja o tipo de sinal que irá percorrer um meio de transmissão, este sofrerá uma redução em sua potência. Este fenômeno, conhecido por atenuação do sinal se manifesta de forma diferente conforme a natureza do sinal (eletricidade, onda eletromagnética), material do meio (cobre, fibra, etc.) ou frequência do sinal. O desejável é que ocorra o mínimo possível de atenuação.
- **Largura de Banda:** Não é somente a atenuação que interessa qualitativamente para a transmissão em um meio, também a largura de banda deve ser considerada. Entende-se por largura de banda a capacidade de um meio de transportar dados em determinado tempo. Geralmente é medida em quilobits por segundo (Kbps) ou megabits por segundo (Mbps).

4.1 Par Trançado

Os cabos de par trançados vêm substituindo os cabos coaxiais desde o início da década de 90. Hoje em dia é muito raro alguém ainda utilizar cabos coaxiais em novas instalações de redes.

O nome “par trançado” é muito conveniente, pois estes cabos são constituídos justamente por 4 pares de cabos entrelaçados.

O entrelaçamento dos cabos cria um campo eletromagnético que oferece uma razoável proteção contra interferências entre os pares do cabo, fenômeno conhecido por crosstalk (diafonia).

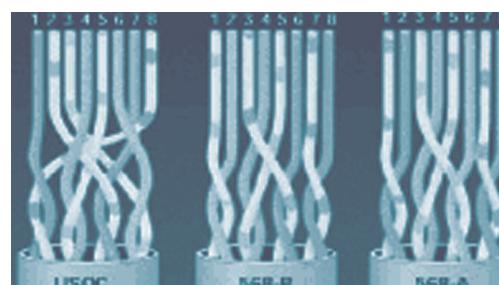


Fig.5 - Cabo par trançado UTP.
Fonte: www.blackbox.com.br

GLOSSÁRIO

Segundo a Wikipédia, o cabo coaxial é constituído por um fio de cobre condutor revestido por um material isolante e rodeado duma blindagem. Utilizado para transportar sinais de alta frequência, como em sinais de TV a cabo.

Existem dois tipos de par trançado:

- UTP (Unshielded Twisted Pair – Par Trançado não Blindado)
- STP (Shielded Twisted Pair – Par Trançado Blindado).

Vamos saber mais sobre eles?

O STP possui uma cobertura metálica (alumínio) melhorando a proteção contra ruídos, sendo mais recomendado para ambientes com fortes fontes de interferências, como grandes motores elétricos e estações de rádio que estejam muito próximas.

Nas instalações de rede, o mais comum é encontrar o UTP. A utilização de tubulação metálica para acondicionamento dos cabos elimina a interferência elétrica externa, porém não com a interferência dos cabos entre si.

Os cabos UTP padronizados pela norma EIA/TIA-568-B são classificados em categorias, e a diferença entre elas está na frequência máxima que suportam, conforme mostra a tabela abaixo.

Tipo	Descrição de uso
Categoria 1	Voz (cabo telefônico)
Categoria 2	Dados a 4 Mbps (Local Talk)
Categoria 3	Transmissão de até 16 MHz, dados até 10 Mbps (Ethernet)
Categoria 4	Transmissão de até 20 MHz, dados até 20 Mbps (16 Mbps Token Ring ou Ethernet)
Categoria 5	Transmissão de até 100 MHz, dados até 100 Mbps (Fast Ethernet)
Categoria 5e	Transmissão de até 100 MHz, dados até 1.000 Mbps (Gigabit Ethernet)
Categoria 6	Transmissão de até 250 MHz, dados até 1.000 Mbps (Gigabit Ethernet) sendo usada atualmente também em redes 10 Gigabit Ethernet.
Categoria 7	Transmissão de até 600 MHz, recomendada para redes 10 Gigabit Ethernet.

Tabela 2 - Categorias de cabos UTP.

Fonte: Baddini. Gerenciamento de Redes com Windows Vista.

Você sabia que...

Os cabos mais comercializados são de categoria 5e (TABELA 2), e eles também apresentam um limite de distância entre um computador e outro equipamento de rede que pode ser outro computador, um hub ou switch e que não pode ultrapassar 100 metros.

É importante ter em mente que um sistema de cabeamento de determinada categoria tem que satisfazer os requisitos dessa categoria. Por exemplo, um sistema de categoria 5e deve utilizar não só o cabo nessa categoria, como os conectores, tomadas e painéis.

É fácil saber a categoria de um cabo, pois vem marcada no próprio cabo.

4.2 Conectores Utilizados nos Cabos de Par Trançado

Eles seguem o padrão RJ-45. São parecidos com conectores de cabos telefônicos, porém, são maiores pois acomodam mais fios. O conector RJ-45 possui oito pinos para acomodar os 4 pares trançados do cabo UTP.

Para os conectores RJ45, também foi definido um padrão conhecido por EIA/TIA (Electronic Industries Alliance / Telecommunications Industry Association), órgão norte-americano responsável pela padronização de sistemas.

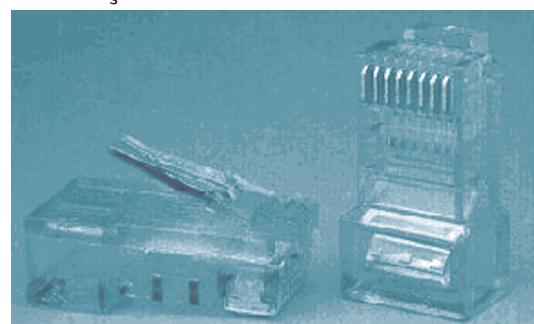


Fig.6 - Plug RJ45.

Fonte: www.clubedohardware.com.br

Para crimpar o cabo, ou seja, para prender o cabo ao conector, usamos um alicate de crimpagem. Após retirar a capa protetora, você precisará tirar as tranças dos cabos e em seguida “arrumá-los” na ordem correta, dentro do conector para o tipo de cabo que estiver construindo.



Fig.7 - Alicate de Crimpagem

Fonte: www.blackbox.com.br

DICA

Você deve retirar apenas a capa externa do cabo e não descascar individualmente os fios, pois isto ao invés de ajudar, iria apenas causar mal contato.

ATENÇÃO!

O que protege o cabo contra as interferências externas são justamente as tranças, por isso, é recomendável deixar apenas os 2 centímetros que entrarão dentro do conector. A função do alicate é fornecer pressão suficiente para que os pinos do conector RJ-45 esmaguem os fios do cabo, alcançando o fio de cobre no conector e criando o contato.

4.3 Confeccionando um Cabo de Rede

Para criar um cabo destinado a conectar computadores a equipamentos de rede (hub, switches), a sequência tanto no conector do micro quanto no conector do equipamento de rede será o seguinte:

Pino	Cor do cabo
1	Verde e branco
2	Verde
3	Laranja e branco
4	Azul
5	Azul e branco
6	Laranja
7	Marrom e branco
8	Marrom

Existe uma posição certa para os cabos dentro do conector. Cada um dos fios do cabo possui uma cor diferente. Metade tem uma cor sólida enquanto a outra metade tem uma cor mesclada com branco.

Tabela 3 - Padrão T568A Direto (Straight Through)

É também possível criar um cabo para ligar diretamente dois micros, sem usar um hub, chamado de cabo cruzado (cross-over). Neste tipo de cabo a posição dos fios é diferente nos dois conectores.

Conector A	
Pino	Cor do cabo
1	Verde e branco
2	Verde
3	Laranja e branco
4	Azul
5	Azul e branco
6	Laranja
7	Marrom e branco
8	Marrom

Tabela 4a - Padrão T568A
Direto (Straight Through)

Conector B	
Pino	Cor do cabo
1	Laranja e branco
2	Laranja
3	Verde e branco
4	Azul
5	Azul e branco
6	Verde
7	Marrom e branco
8	Marrom

Tabela 4b - Padrão T568B
Half Cross (cruzamento parcial)

4.4 Fibra Ótica

Nas fibras óticas apenas a luz é transmitida, e por isso, elas são totalmente imunes a qualquer tipo de interferência eletromagnética. Além disso, como os cabos são feitos de plástico e fibra de vidro (ao invés de metal), eles são resistentes à corrosão.



Fig.8 – Fibra ótica.

As fibras óticas são usadas quando existe a necessidade de interconectar computadores a distâncias maiores do que 100 metros em relação ao equipamento de rede. É bom observar que existem vantagens e desvantagens no seu uso.

- Vantagens: Os cabos de fibra óptica são mais seguros em ambientes onde existe perigo de incêndio ou explosões, pois não soltam faíscas. Também, o sinal transmitido através do cabo é mais difícil de interceptar, sendo mais seguro para transmissões sigilosas.

- Desvantagens: Residem no alto custo dos cabos, tanto quanto o custo das placas de rede. A instalação é mais complicada e exige mais material.

Existem dois tipos de cabos de fibra óptica:

- cabos monomodo;
- cabos multimodo.

O cabo monomodo transmite apenas um sinal de luz enquanto os cabos multimodo contém vários sinais que se movem dentro do cabo. Ao contrário do que parece, os cabos monomodo transmitem mais rápido, pois a luz viaja em linha reta, o que não acontece nos cabos multimodo, onde o sinal viaja batendo continuamente nas paredes do cabo.

4.5 Redes sem Fio (Wireless)

Nas redes sem fio as informações são transmitidas através do ar, em canais de frequência de rádio (na faixa de kHz até GHz) ou infravermelho (frequências da ordem de THz). As redes sem fio são uma alternativa viável onde é difícil, ou mesmo impossível instalar cabos metálicos ou de fibra ótica.

Tipicamente as redes sem fio proporcionam a integração de dispositivos pessoais, como handhelds, Pocket PCs, terminais e notebooks, à rede corporativa, dominada anteriormente por PCs e servidores. A mobilidade é um dos maiores benefícios dessa nova tecnologia.

No início das redes sem fio as tecnologias não eram padronizadas, o que complicava as implantações. Atualmente, os fabricantes e os órgãos técnicos estão se unindo para gerar padrões de mercado, de forma a garantir implantações mais simples. A frequência de transmissão utilizada hoje é de 2.4 GHz (gigahertz) ou de 5 GHz no padrão 802.11.

Em redes wireless, o IEEE (Institute of Electrical and Electronic Engineers) desenvolveu e disponibilizou aos fabricantes o padrão 802.11. E outro grupo formado por fabricantes (Ericsson, IBM, Intel, Nokia e Toshiba), criou o padrão Bluetooth.

Meios de Transmissão

Em redes sem fio existem dois modos de conexão:

- Modo Ad-hoc ou ponto a ponto: Os dispositivos se comunicam diretamente sem a necessidade de um ponto de acesso (AP).
- Modo Infraestrutura: Os dispositivos se comunicam através de um ponto de acesso (AP). Eles também podem comunicar-se com dispositivos em uma rede baseada em cabos.

O Access Point (AP, ou Ponto de Acesso) Interconecta os dispositivos sem fios e permite que os dispositivos sem fio se conectem a computadores ligados à rede baseada em cabos. Os pontos de acesso são limitados normalmente a 50 ou 100 metros, com variações de acordo com os obstáculos. Os pontos de acesso mais conhecidos suportam até 256 dispositivos conectados simultaneamente.



Fig.9 – Access Point.

Fonte: www.dlink.com

Resumo

Os meios de transmissão mais comuns para redes locais são: par trançado, fibra ótica e sem fio.

Par trançado: Existem dois tipos de par trançado o UTP (Unshielded Twisted Pair – Par Trançado não Blindado) e o STP (Shielded Twisted Pair – Par Trançado Blindado).

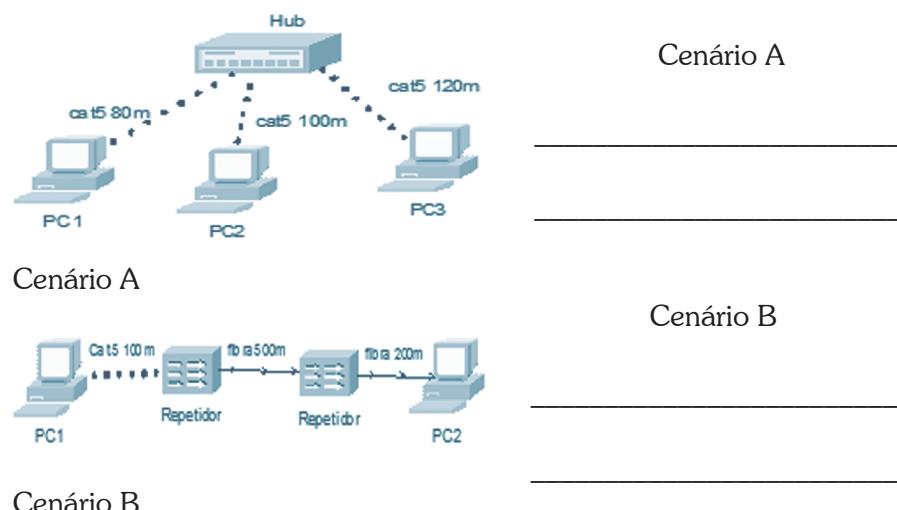
Nas instalações de rede, o mais comum é encontrar o UTP. O entrelacamento dos cabos cria um campo eletromagnético que oferece uma razoável proteção contra interferências entre os pares do cabo, fenômeno conhecido por crosstalk (diafonia).

Fibra ótica: Apenas a luz é transmitida e por isso é totalmente imune a qualquer tipo de interferência eletromagnética. Existem dois tipos de cabos de fibra óptica, chamados de cabos monomodo e multimodo.

Sem fio: As informações são transmitidas através do ar, em canais de frequência de rádio (na faixa de kHz até GHz) ou infravermelho (frequências da ordem de THz). Em redes sem fio existem dois modos de conexão: Modo Ad-hoc ou ponto a ponto e Modo Infraestrutura.

Atividades de Aprendizagem

- Verifique nos cenários propostos abaixo, se as máquinas estão conectadas em conformidade com as especificações técnicas de cabeamento.



- Numere os passos para a confecção de um cabo par trançado:

- () Segurar firme o conector e pressionar o alicate, fazendo com que os finos elementos metálicos apertem os fios dentro do conector, travando-os.
- () Segurar firme as pontas dos fios e inserir com cuidado, observando se a posição de cada um se mantém correta e pressioná-los para entrarem até o final e então colocar o conector no alicate de crimpagem.
- () Preparar os oito fios para serem inseridos no plugue RJ45 ajustando-os na posição correta de acordo com o padrão EIA/TIA e cortar para que todos tenham o mesmo alinhamento.
- () Utilizar a lâmina do alicate de crimpagem para remover 2 cm da capa isolante em uma das extremidades do cabo.

CAPÍTULO

5

**MODELO DE
PROTOCOLO TCP/IP**



Objetivo

Nesta unidade você deverá ser capaz de identificar o modelo de protocolo TCP/IP e sua importância.



Modelo de Protocolo TCP/IP

Na disciplina Internet e Conectividade você estudou que o modelo de referência ISO / OSI (Internacional Organizativo for Standardization / Open Systems Interconnection) nasceu da necessidade de se criar padrões de conectividade para interligar sistemas computacionais. Podemos então, pensar no modelo ISO/OSI como um template para criar protocolos de rede.

Para uma melhor compreensão, de maneira bem simples, podemos pensar em um processador de textos. Existem diversos modelos de documentos (chamados templates) e a partir dos quais podemos criar nossos próprios documentos.

Esse modelo tem servido de base para auxiliar em um entendimento mais claro das funções do modelo de protocolo TCP/IP. Na arquitetura TCP/IP existem 4 camadas básicas, conforme mostra a figura abaixo.

Modelo OSI

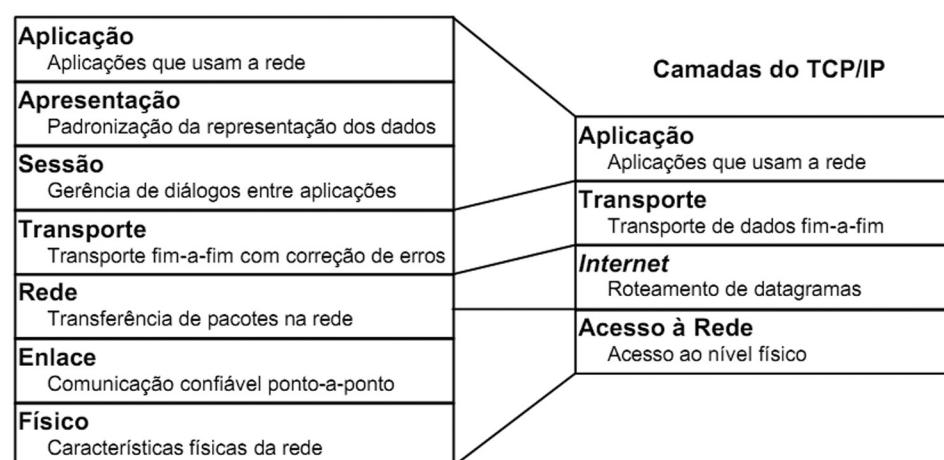


Fig.10 - Comparação de camadas TCP/IP com modelo OSI.

Fonte: Specialski. Arquiteturas de Redes.

Nos próximos capítulos, iremos estudar detalhadamente as camadas do modelo TCP/IP e seus principais serviços, por ser o principal modelo da Internet.

Resumo

Na arquitetura TCP/IP existem 4 camadas básicas: Aplicação, Transporte, Internet e Acesso à rede. As camadas do modelo TCP/IP e seus principais serviços são consideradas importantes por ser o principal modelo da Internet.

Atividades de Aprendizagem

1. Descreva as quatro camadas do TCP/IP.

2. Associe com as camadas do modelo OSI.

- | | |
|-----------------|---|
| 1. Física | () Ethernet, Token Ring, ATM |
| 2. Enlace | () TCP, UDP |
| 3. Rede | () IP, ICMP, ARP |
| 4. Transporte | () NetBIOS, Telnet |
| 5. Sessão | () Par Trançado, Fibra Ótica, Satélite |
| 6. Apresentação | () FTP, HTTP |
| 7. Aplicação | () SSH |

CAPÍTULO

6

PROTOCOLO TCP/IP



Objetivo

Nesta unidade aprenderá como acontece a troca de informações entre as redes de computadores, conhecer HTTP, entender o emulador SSH e instalar e configurar um servidor FTP. Além de configurar manualmente o protocolo TCP/IP nas plataformas Windows/Linux.



Protocolo TCP/IP

O protocolo conhecido como TCP/IP (Transmission Control Protocol/Internet Protocol) é atualmente, o padrão de fato das redes. As definições de protocolos se encontram em documentos publicamente disponíveis denominados RFC (Request for Comments).

O protocolo TCP/IP é organizado em 4 camadas básicas e composto por dois protocolos. O IP (Internet Protocol) e o TCP (Transmission Control Protocol).

O protocolo TCP antes de trocar dados necessita “abrir” uma conexão para estabelecer uma comunicação. Essa conexão é estabelecida entre duas máquinas (hosts) através de um sequência que envolve a troca de três pacotes, e por isso é chamado de “three-way handshake” (aperto de mão em três vias).

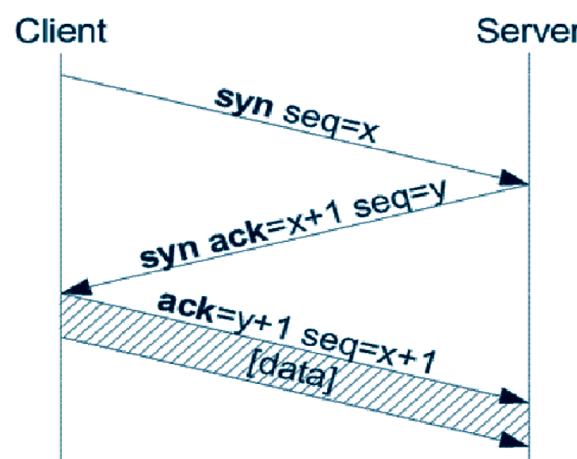


Fig.11 – Three-way Handshake

EXEMPLIFICANDO

Vamos considerar como exemplo um servidor Web. Suponha que o computador cliente deseja se conectar ao servidor e obter dele a página principal index.php. O que deve ser feito para isso acontecer?

- O cliente envia um pacote TCP ao servidor para a porta 80 com o flag SYN (sinal de sincronização) ativado e com um número sequencial que marcará o início da troca de dados.
- O servidor (se estiver escutando naquela porta) responderá com dois flags ativados: o ACK, indicando que reconheceu e aceitou o pacote enviado, e um novo SYN, solicitando que o cliente aceite o seu número sequencial.

- O cliente então responderá com um valor de confirmação ACK indicando que eles podem iniciar a transferência de dados sem problemas.

O que são Portas de Comunicação?

O protocolo TCP/IP permite que muitas aplicações sejam implementadas por meio de serviços que utilizam portas, identificadas por um número inteiro.

As portas são canais de comunicação que variam de 1 a 65.535 para um endereço IP.

Alguns serviços são mais conhecidos, tais como: DNS (porta TCP/UDP 53), SMTP (porta TCP 25), HTTP (porta TCP 80) e outros.

6.1. Camada de Aplicação

Inicialmente, você precisa compreender o que é uma camada de aplicação. Ela se refere aos programas de aplicação que se utilizam dos serviços da camada de transporte. Como exemplo, podemos citar:

- o telnet (emulação de terminal via rede),
- o ftp (protocolo de troca de arquivos),
- o www(serviço de páginas da internet), etc.

a) Protocolo FTP

Protocolo que permite a transferência de arquivos através da rede. Você acessa um servidor FTP com seu nome de usuário e senha onde os arquivos podem ser inseridos ou obtidos. É uma maneira fácil e rápida de transferir dados, muito usada para colocar um site no ar rapidamente.

O FTP é feito através de programas específicos (WS-FTP, Cute FTP, Filezilla). Existe também o TFTP, que é através do protocolo UDP, porém esse não possui autenticação nem confiabilidade. Um programa de computador pode ser copiado para o seu computador, mesmo se você não tiver um programa de FTP.

Os navegadores Web atuais têm contem um programa de FTP e portanto, você pode utilizá-los para isso. No lugar de “<http://>” basta colocar o “<ftp://>”, seguido do nome do servidor de FTP que a conexão será efetuada. Na verdade, apesar do navegador ter o FTP embutido, ele não é tão eficaz quanto um programa especialmente desenvolvido para isso.

b) Protocolo HTTP

HTTP (Hyper Text Transfer Protocol), é o protocolo usado pela World Wide Web, a rede mundial de web sites da Internet. Ele é quem define como as páginas são formatadas e transmitidas e que ações os servidores Web e navegadores(browsers) devem tomar ao responder a certos comandos.

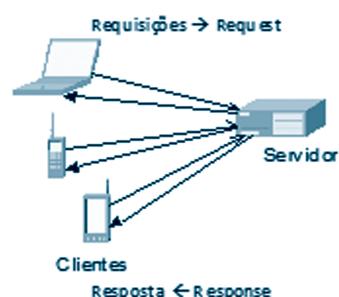


Fig.12 – Request - Response

A comunicação entre o cliente e servidor é feita através do protocolo HTTP, onde o cliente envia requisições (request) ao servidor e o servidor envia respostas (response) aos clientes.

Por exemplo:

Quando você entra com uma URL no seu browser, este envia automaticamente um comando HTTP (comando GET) ao servidor Web, dizendo a ele para transmitir a página Web requisitada. Usamos este método quando são poucas informações e não necessitamos de segurança nos dados.

Já o método HTTP POST transfere os dados via stream (fluxo de dados), ou seja, no pacote HTTP request ao servidor. Este método é muito utilizado para:

- envio de dados em formulários HTML.
- envio de arquivos do cliente para o servidor.
- aumentar a segurança. Ex: login de usuários, onde não queremos que os dados sejam expostos na URL.

c) Telnet/SSH

Telnet é um programa de emulação de terminal para redes TCP/IP. O Telnet roda no computador e possibilita o controle do servidor e a comunicação com outros computadores na rede.

Para iniciar uma sessão de Telnet, você precisa se logar no servidor, entrando com nome de usuário e senha válidos. Às vezes, você não precisa nem se autenticar.

ATENÇÃO!

SSH (Secure Shell) é uma evolução do Telnet e possui um excelente sistema de autenticação e criptografia em meios inseguros como a Internet, por exemplo.

6.2 Camada de Transporte

A camada de transporte possibilita a comunicação entre os programas de aplicação, de uma forma fim-a-fim, ou seja, o transporte garante que os dados transmitidos/recebidos estarão corretos. Os protocolos de transporte típicos da internet são o TCP e o UDP. Vamos agora, conhecer melhor estes protocolos.

- O protocolo TCP (Transmission Control Protocol) oferece uma comunicação segura, ordenada e confiável entre duas máquinas. Ele estabelece a conexão antes do envio das informações, caso não consiga, retorna como erro. Podemos ver esse protocolo em ação ao conectarmos um messenger, um servidor de FTP, uma página Web ou mesmo ao enviarmos um e-mail.
- O protocolo UDP (User Datagram Protocol) é um protocolo de transporte de dados não-orientado a conexão, ou seja, não faz nenhum tipo de conexão e não possui a robustez do TCP. Porém, a sua velocidade de transmissão é maior que a do TCP. Uma das utilizações em que se pode notar isso é no streaming de vídeo pela Internet., onde é possível perceber pequenas falhas, alguns cortes, etc.

6.3 Camada de Internet

Representada pelo protocolo IP, a camada de internet recebe pedidos de transporte para envio de pacotes e os conduz até a estação final de destino. É nessa camada que os pacotes são roteados para atingir seu destino final.

Vamos conhecer o Protocolo IP?

Dentro de uma rede TCP/IP, cada micro recebe um endereço IP único que o identifica na rede. Um número de IP contém 4 bytes com tamanho específicos no formato: 000.000.000.000, em que cada byte pode incorporar um valor que vai de 0 até 255, como em 198.254.10.1.

O protocolo IP está atualmente na sua quarta versão, o IPv4, em uso desde 1982. As crescentes necessidades de endereçamento e segurança impulsionaram o desenvolvimento da próxima versão, o IPv6 ou next generation.

No protocolo IP os dados são transmitidos em blocos denominados datagramas ou de forma mais coloquial, pacotes (packets).

Cada endereço é um par (netid, hostid) que identifica portanto uma rede (net identifier) e um computador (host identifier).

Os endereços podem estar incluídos em 5 classes:

- Classe A são associados a grandes redes (mais do que 65.536 computadores),
- Classe B para redes de tamanho médio (entre 257 e 65.536 computadores)
- Classe C para pequenas redes (até 256 pontos).
- Classe D é para endereçamento multicast (endereço de grupo de estações)
- Classe E é para expansão futura.

O endereço Classe A 127.0.0.0 é um endereço de **loopback**. Qualquer estação que enviar um quadro com este endereço estará enviando para ela mesma, ou seja, não é colocado na rede.

PARA REFLETIR



Não deve haver duas máquinas com o mesmo endereço IP em uma mesma rede, pois isso causaria conflito nas máquinas e uma delas estaria impossibilitada de se conectar a rede.

Os endereços Internet são unicamente atribuídos por uma autoridade central, o Network Information Center (NIC). Este centro atribui apenas os endereços de rede (netid) deixando a cargo das organizações requisitantes as atribuições de endereços de estações.



PARA REFLETIR

Cada estação de trabalho, servidor e outros elementos de rede necessitam de um endereço IP único. Conforme uma rede de computadores cresce, gerenciar os endereços pode se tornar difícil. Já existe uma solução para esta situação?

Sim. Algumas médias empresas utilizam IPs estáticos, o que gera tarefas administrativas adicionais e alguns problemas de rede, como os conflitos de endereço IP.

Como é formada uma Máscara de Rede?

Além do endereço IP cada computador possui uma máscara de rede (network mask ou sunet mask) que é formado por valores entre 0 e 255, a máscara de sub-rede é formada por apenas dois valores: 0 e 255, como em 255.255.0.0 ou 255.0.0.0 onde um valor 255 indica a parte endereço IP referente à rede, e um valor 0 indica a parte endereço IP referente ao host.

Dentro de uma mesma sub-rede, todos os hosts deverão ser configurados com a mesma máscara de sub-rede, caso contrário eles poderão não conseguir comunicar-se, pois pensarão estar conectados a redes diferentes.

Se houver dois micros dentro de uma mesma sub-rede, configurados com os endereços 200.133.103.1 e 200.133.103.2, mas configurados com máscaras diferentes, 255.255.255.0 para o primeiro e 255.255.0.0 para o segundo, teremos um erro de configuração.

O protocolo DHCP resolve todos estes problemas de forma rápida, simples e eficiente.



Então, o que é o DHCP e como ele funciona?

O DHCP é um protocolo que permite o gerenciamento dos endereços e configurações IPs dentro de uma rede a partir de um ponto centralizado - uma base de dados central gerenciada dinamicamente e de forma automatizada, que fornece e registra o uso de endereços IP a partir de uma faixa de endereços definidos.

O DHCP funciona da seguinte forma:

1. Os computadores configurados para utilizar endereços automáticos enviam um pacote de requisição na rede por meio de um broadcast (veremos mais à frente).
2. O servidor DHCP disponível responde à requisição, oferecendo um endereço IP livre ao computador.
3. O computador seleciona o endereço IP e retorna, confirmando que deseja utilizar esse endereço.



Protocolo TCP/IP

4. O servidor DHCP responde à mensagem. O endereço é definido para aquele computador e uma confirmação é enviada a ele.

Obs.: Esse IP “emprestado” para o computador fica alocado por um tempo configurável, e após esse período o endereço é renovado, atribuindo-se um novo ou mantendo o mesmo, se estiver livre no servidor.

E quanto a Resolução de Nomes?

Para que tudo fique mais fácil na Internet (e mesmo em Intranets), por exemplo, ao invés de dizer, meu email é `joão@200.200.200.200`, o protocolo TCP/IP utiliza técnicas para associar nomes amigáveis aos endereços IP.

Existem dois tipos de resolução de nomes:

- DNS (Domain Name System ou Sistema de Nome de Domínios)
- NetBIOS ou nome de redes Microsoft.

DNS

Permite usar nomes amigáveis ao invés de endereços IP para acessar servidores. Quando você se conecta a Internet e acessa um endereço usando o navegador é um servidor DNS que converte o “nome fantasia” no endereço IP real do servidor, permitindo ao navegador acessá-lo.

Para tanto, o servidor DNS mantém uma tabela com todos os nomes fantasia, relacionados com os respectivos endereços IP. A maior dificuldade em manter um servidor DNS é justamente manter esta tabela atualizada, pois o serviço tem que ser feito manualmente. Dentro da Internet, temos várias instituições que cuidam desta tarefa.

No Brasil, por exemplo, temos a FAPESP. Para registrar um domínio é preciso fornecer à FAPESP o endereço IP real do servidor onde a página ficará hospedada.

A configuração do servidor DNS pode ser feita tanto manualmente em cada estação, quanto automaticamente através do servidor DHCP.

DICA

O termo “NetBEUI” se refere ao protocolo de rede em si.

O termo NetBIOS é usado quando queremos nos referir aos comandos deste mesmo protocolo usado pelos programas para acessar a rede.

NetBIOS / NetBEUI

Foi concebido pela IBM e trata de extensões de entrada/saída para que o sistema operacional MS-DOS e seus descendentes possam acessar redes locais.

Com o tempo, o NetBIOS foi incorporado como uma API de programação do recente protocolo conhecido como NetBEUI (NetBIOS Enhanced User Interface).

NetBIOS/NetBEUI sempre foram considerados por seu desempenho em redes locais (normalmente pequenas). Porém, para redes maiores e intranets de qualquer tamanho, o uso do TCP/IP é mais recomendável.

O que é o Protocolo IPX/SPX?

O IPX/SPX (Internet Packet Exchange/Sequenced Packet Exchange) é o protocolo nativo dos sistemas operacionais da empresa NOVELL.

Você sabia que...

Atualmente a própria Novell utiliza o protocolo TCP/IP em seus produtos. Porém, ainda encontramos muitas redes de computadores que utilizam o IPX/SPX como protocolo padrão.

Nos sistemas operacionais Windows, a Microsoft inclui uma versão para o IPX/SPX chamada, NWLink, que permite a interligação de várias redes.

6.4 Camada de Interface de rede

A interface de rede está associada à rede física (Ethernet) e fisicamente constitui-se em um driver de acesso a esta rede (device driver). É a camada que se relaciona a tudo aquilo que um pacote IP necessita para realmente estabelecer um link físico.

6.4.1 Tipos de Transmissão de Dados

A quantidade de tráfego gerada em uma rede pode ser de três tipos:

- unicast
- broadcast
- multicast.

a) Unicast

Em uma transmissão unicast, uma cópia dos dados é enviada de sua origem para cada computador cliente que os requisite. Nenhum outro computador na rede recebe o tráfego. Em uma rede com muitos computadores não é sempre eficiente, pois o equipamento de origem terá que transmitir múltiplas cópias dos dados.

b) Broadcast

Nesse tipo de transmissão, os dados são enviados apenas uma vez, mas para toda a rede. Esse processo não é muito eficiente, pois faz a velocidade cair bastante, uma vez que todos os computadores irão receber os dados.

c) Multicast

É enviada apenas uma cópia dos dados e somente os computadores que fizeram o pedido os recebem, evitando, assim, um tráfego muito intenso, e consequentemente, um congestionamento na rede. Muitos serviços de Internet usam multicast para se comunicar com clientes.

Resumo

O protocolo TCP/IP é organizado em 4 camadas básicas:

- **Camada de aplicação:** Refere-se aos programas de aplicação que se utilizam dos serviços da camada de transporte. Exemplo: Telnet (emulação de terminal via rede), ftp (protocolo de troca de arquivos), www (serviço de páginas da internet), etc.
- **Camada Internet:** Representada pelo protocolo IP, recebe pedidos de transporte para envio de pacotes e conduz estes até a estação final de destino.
- **Camada de transporte:** Possibilita a comunicação entre os programas de aplicação, de uma forma fim-a-fim, ou seja, garante que os dados transmitidos/recebidos estarão corretos.
- **Camada de interface de rede:** Se relaciona a tudo aquilo que um pacote IP necessita para realmente estabelecer um link físico.

Atividades de Aprendizagem

CAPÍTULO

7

ELEMENTOS DE UMA REDE



Objetivo

Nesta unidade você deverá conhecer os principais elementos (hardware) de uma rede para a resolução de problemas.





Elementos de uma rede

Os elementos de rede constituem-se nos principais componentes de hardware que fazem a interconexão entre segmentos de rede.

7.1 Placas de rede

As placas de rede, ou interface de rede permitem que computadores se comuniquem em uma rede de computadores. No mercado, existem diversos modelos de placas, que variam de acordo com a arquitetura, ou seja são específicas para determinada tecnologia de rede.

Quando escolher uma placa...

- Não utilize uma placa de rede padrão Token Ring em uma rede padrão Ethernet, pois ela não conseguirá comunicar-se com as demais.
- Ao escolher uma placa de rede é importante verificar se ela suporta a taxa de transmissão desejada.
- Não utilize um hub ou switch de 1 Gbps e placas de rede que suportam apenas 100 Mbps. Pois a taxa resultante será de 100 Mbps, ou seja, sempre de acordo com o dispositivo mais lento.
- Verifique se a sua placa de rede possui LEDs próximos ao conector, pois normalmente indicam o status da placa, como link estabelecido (luz verde piscando) no painel traseiro do seu computador.

SAIBA MAIS



As placas de rede possuem um endereço único que as identificam na rede, como uma espécie de número de identidade (um "RG"). Esse endereço segue um padrão mundial estabelecido pelo IEEE (International Organization for Standardization / Open Systems Interconnection) disponibilizado aos fabricantes. Esse endereço atribuído as placas de rede chama-se MAC Address (Media Access Control Address).

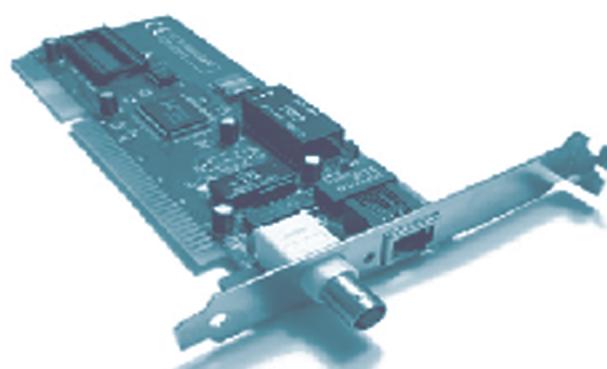


Fig.13 – Placa Adaptadora de Rede

7.2 Hubs

Os hubs atuam na camada 1 (física). São dispositivos de rede repetidores para múltiplas portas. Os modelos de hubs possuem entre 4 e 48 portas (4, 8, 12, 16, 24, 32, 48 portas). Quando um pacote é recebido em uma porta, ele é copiado para as outras portas.

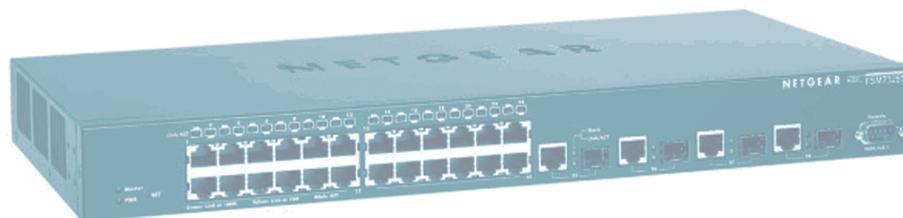


Fig.14 – Hub.

Fonte: <http://www.netgear.com/>

Os modelos de hub mais modernos chamam-se gerenciáveis, porque permitem por meio de um software de gerenciamento, que o administrador de redes monitore o tráfego nas portas do hub, habilitando e desabilitando-as remotamente.

7.3 Repetidores

Geralmente, os repetidores são utilizados para a interligação de duas ou mais redes idênticas. Atuando no nível físico, os repetidores simplesmente recebem os pacotes de cada uma das redes que interligam, regeneram e os retransmitem nas demais redes, sem realizar qualquer tipo de tratamento.



Fig.15 – Repetidor.

Fonte: www.trellis.com.br

Obs.: Caso você precise unir dois hubs que estejam muito distantes, você poderá usar um repetidor.

7.4 Switches

Esse dispositivo de rede atua como filtro e encaminhador de pacotes com base no endereço de destino. Os switches atuam na camada 2 (camada de enlace). Também existem switches que atuam na camada 3 (camada de rede) que podem filtrar os pacotes de forma ainda mais inteligente.

O principal benefício no uso do switch é o desempenho da rede. Pois, diferentemente do hub que entrega o pacote recebido em todas as portas, o switch analisa o pacote, e encaminha para a porta específica do endereço destino.



Fig16 – Switch

7.5 Bridges (Pontes)

Atuam no protocolo em nível de enlace e apenas conectam múltiplos segmentos de rede. Realizam a comunicação de computadores em diferentes arquiteturas de redes. Por exemplo: Se você tem duas redes, uma Ethernet e outra Token Ring, interligadas por uma bridge, e se o micro da rede Ethernet transmitir algo para o micro da rede Token Ring, o bridge detectará (ao ler o pacote) que o endereço destino pertence a outro segmento e encaminhará o pacote.

GLOSSÁRIO



Ethernet é o protocolo mais utilizado a nível de enlace e é baseado em uma tecnologia para interconexão de redes locais.



Fig.17 – Bridge.

Fonte: www.trellis.com.br

IMPORTANTE!

Para uma rede muito grande, que fique lenta devido ao tráfego intenso, você pode utilizar uma bridge para segmentar a rede, dividindo o tráfego pela metade.

7.6 Roteadores

Os roteadores servem para interligar duas redes separadas. Eles atuam na camada de rede do modelo OSI, e por isso conseguem rotear os pacotes que destinam-se à outra rede, diferentemente do bridge. Esses dispositivos possuem tabelas de roteamento que identificam em que porta do roteador o pacote precisa ser entregue.



Fig.18 – Roteador.

Fonte: www.3com.com

Os roteadores podem interligar várias redes diferentes, situadas em localidades remotas. A internet, por exemplo, é formada por milhares de roteadores. Por exemplo, quando acessamos uma página o sinal deve passar por vários roteadores. A página carregará rapidamente, se todos os roteadores estiverem livres, caso contrário, pode ser que a página demore a carregar.

7.7 Gateway

Serve como uma porta de entrada e saída de uma rede para outra. Normalmente, o gateway padrão é o endereço de um roteador ou um servidor que age como gateway para Internet ou outra rede qualquer.

Resumo

Os elementos de rede constituem nos principais componentes de hardware que fazem a interconexão entre segmentos de rede.

Placas de Rede: Permitem que computadores se comuniquem em uma rede de computadores;

Hubs: Atuam na camada 1 (física). São dispositivos de rede repetidores para múltiplas portas.

Repetidores: Atuam na camada 1 (física). São utilizados, geralmente para interligação de duas ou mais redes idênticas.

Switches: Atuam na camada 2 (enlace) e 3 (rede). Esse dispositivo de rede atua como filtro e encaminhador de pacotes com base no endereço de destino.

Bridges: Atuam na camada 1 (física). Realiza a comunicação de computadores em diferentes arquiteturas de redes.

Roteadores: Atuam na camada 3 (rede). Servem para interligar duas redes separadas.

Gateway: Serve como uma porta de entrada e saída de uma rede para outra. Normalmente o gateway padrão é o endereço de um roteador ou um servidor.

Atividades de Aprendizagem

1. A figura a seguir representa um segmento de uma rede local com baixo tráfego. Conforme aumenta a utilização (tráfego) da rede local, esta torna-se mais lenta. O que deve ser feito para solucionar o problema? Associe as

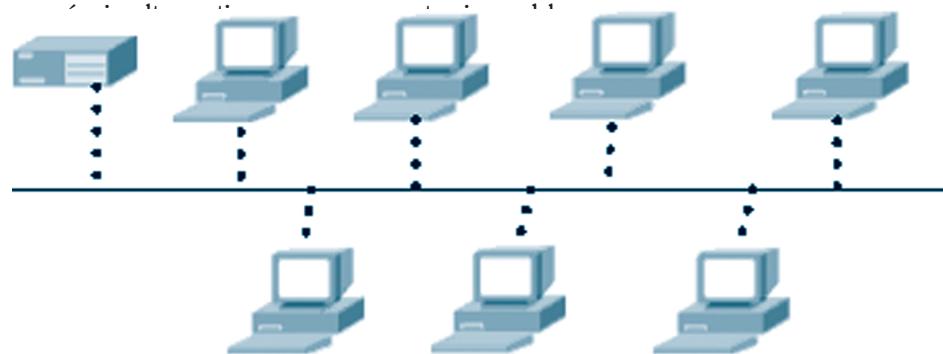


Fig.19 – Rede Local.

Alternativa 1: Acrescentar um servidor de arquivos maior e mais veloz.

Alternativa 2: Usar conexões de maior velocidade, pois tem boas chances de resolver o problema.

Alternativa 3: Dividir a rede em segmentos menores, com o uso de switches ou roteadores. Normalmente soluciona o problema e ainda proporciona escalabilidade.

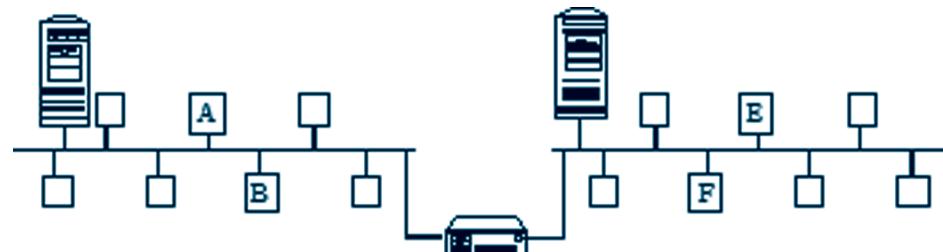


Fig.20 – Segmentação da rede.

Alternativa 4: Criar um backbone (cabeamento vertical) para interligar os diversos segmentos.

Elementos de uma rede

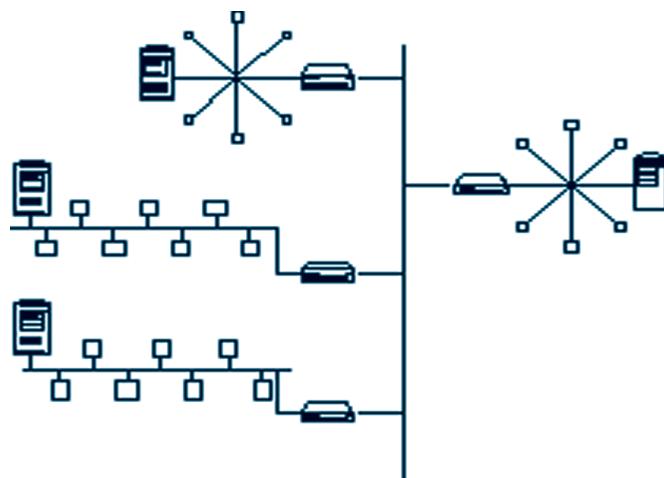


Fig.21 – Backbone.

Alternativa 5: Utilizar um backbone corporativo (switches implementando VPN na camada 3).

Uma VPN é um ambiente onde estações podem ser agrupadas independentemente de sua posição física na rede, formando redes locais isoladas, mesmo que não pertençam ao mesmo segmento físico.

Possíveis Problemas:

() Porém não dá para ir aumentando o número de equipamentos aleatoriamente à medida que a rede fica lenta. Com várias pontes/switches, um pacote gerado no primeiro segmento teria que passar por todos os outros para chegar no último, gerando um tráfego desnecessário.

() É uma solução de curto prazo; O problema reaparecerá, mantidas as atuais taxas de crescimento da rede. O problema pode ser a rede muito lenta.

() Porém é necessário atualizar todas as placas de rede, e talvez o meio físico e pode tornar uma solução cara.

() O problema que começa a se delinear é a velocidade do backbone corporativo. Caso tenha a mesma velocidade dos segmentos de rede local, vai criar um “gargalo” para comunicação entre segmentos.



CAPÍTULO

8

MODELOS DE REDE



Objetivo

Ao final desta unidade você deverá avaliar as vantagens e desvantagens dos modelos de redes ponto-a-ponto e das redes cliente-servidor e conhecer os tipos de servidores mais utilizados.



Modelos de rede

Entende-se por modelos de rede os formatos de estrutura, física e lógica, de redes de computadores. Existem dois modelos básicos de redes: a rede ponto a ponto e a rede cliente-servidor.

8. 1 Redes Ponto a Ponto

As redes ponto a ponto são mais simples, sem nenhuma estrutura centralizada de administração, segurança e recursos compartilhados. Recomenda-se esse modelo de rede para pequenos escritórios (no máximo dez computadores) e todos atuam como clientes (computador que acessa um recurso pela rede) e servidores (computador que disponibiliza um recurso na rede).

A desvantagem de uma rede desse tipo é a descentralização, ou seja, tarefas administrativas como backup dos dados, controle de acesso a recursos (arquivos ou impressoras) e o gerenciamento do protocolo são de difícil controle.

8.2 Redes Cliente-Servidor

Nessas redes administração, segurança e recursos são centralizados em um único lugar. Arquivos, impressoras, acesso à Internet, e outros serviços serão controlados pelo servidor. Para isso, é necessário instalar um sistema operacional de rede. Existem vários sistemas no mercado, sendo os mais usados atualmente o Windows 2003 Server, Windows NT Server, Novell Netware e versões do Linux.

As redes cliente-servidor tem um custo inicial mais alto do que as redes ponto-a-ponto e requerem mais conhecimento técnico para serem instaladas e gerenciadas devido ao poderoso hardware/software que utilizam.

A maioria das aplicações da Internet utilizam o modelo de redes chamado “cliente/servidor”.

- *Cliente* corresponde ao programa (software) executado em um host que solicita informações a outro programa, normalmente através da rede. Exemplos de programas cliente: navegador Web (Internet Explorer, Firefox).

- *Servidor* corresponde ao programa que fica em espera, aguardando solicitações de clientes e que fornece os dados solicitados quando recebe uma solicitação de um cliente. Exemplo de servidor: servidores Web (Apache e IIS).



Fig.22 – Arquitetura Cliente-Servidor.

8.3 Tipos de Servidores mais Comuns

Existem vários tipos de servidores dependendo da aplicação na rede, tais como:

a) Servidor de Arquivos

Tem como principais vantagens: centralizar os arquivos de uso comum na empresa, oferecer aos clientes serviço de armazenamento, compartilhamento de disco possibilitando liberar espaço em disco das estações de trabalho, maior controle dos aplicativos e segurança no armazenamento dos arquivos de usuários.

b) Servidor de Impressão

O servidor de impressão oferece recursos para o controle das impressões em rede, sendo responsável por receber as tarefas de impressão de programas aplicativos das estações clientes. Ele define a estação de trabalho que pode usar a impressora e também pode apresentar um relatório detalhado sobre o seu uso em determinado tempo.

c) Servidor Web (Internet)

Responsável por aceitar requisições HTTP de clientes, geralmente os navegadores e servi-los com respostas HTTP, através de páginas web. Ex.: Servidor Apache.



Modelos de rede

d) Servidor de Banco de Dados

Apresentam como principais benefícios: armazenamento de dados (garantindo o sigilo, segurança das informações) e aumento no desempenho do acesso aos dados. Muito utilizado por empresas que trabalham com grandes volumes de dados. Ex.: Oracle, SQL Windows, mySQL, etc.

e) Servidor de FTP

Responsável pela comunicação com os clientes de FTP (ex. WS-FTP). É ele que permite o download e upload de arquivos entre um cliente e o servidor.

f) Servidor de e-mail

Responsável por gerenciar os e-mails que são enviados, recebidos e armazenados. Ex.: Sendmail (Unix).

Resumo

Existem dois modelos básicos de redes, a rede ponto a ponto e a rede cliente-servidor.

- **Redes ponto a ponto:** Não possui estrutura centralizada de administração, segurança e recursos compartilhados. Recomenda-se esse modelo de rede para pequenos escritórios.
- **Redes cliente servidor:** Nessas redes, administração, segurança e recursos são centralizados em único lugar. As redes cliente-servidor tem um custo inicial mais alto do que as redes ponto-a-ponto.

A maioria das aplicações da Internet utilizam o modelo de redes chamado “cliente/servidor”. Os tipos de servidores mais comuns são: servidores de arquivos, servidores de impressão, servidores de web, servidores de banco de dados, servidores de FTP, servidores de e-mail, etc.



Apêndice

LABORATÓRIO DE AULA I

Você sabe qual é um dos principais benefícios proporcionado pelas redes de computadores?

É o compartilhamento de arquivos e impressoras no sistema operacional. No nosso caso, o Windows Vista! Vamos então, estudar compartilhamento verificando a configuração para compartilhamento, o compartilhamento de impressora de rede e o compartilhamento de arquivos e pastas.

❖ CONFERINDO CONFIGURAÇÃO PARA COMPARTILHAMENTO:

1. Clique no Menu Iniciar em seguida, Painel de Controle.
2. Em Rede e Internet, clique em Configurar compartilhamento de arquivos.
3. Em Compartilhamento e Descoberta, clique no botão expandir para Ativar o Compartilhamento de arquivos e o Compartilhamento de impressora.
4. Pronto. Agora você pode compartilhar qualquer pasta e impressora do seu computador na rede.

❖ COMPARTILHANDO IMPRESSORA EM REDE:

1. Para compartilhamento de impressora em rede, clique no menu Iniciar/Configurações e em seguida clique em Impressoras.
2. Selecione a impressora a ser compartilhada e clique sobre a mesma com o botão direito do mouse, selecionando “Compartilhamento”.
3. Clique no botão “Alterar Opções de Compartilhamento”;
4. Clique em Continuar na caixa de diálogo do Controle de Conta de Usuário;
5. E habilite a opção Compartilhar esta impressora.
6. Vá até outro computador e veja se você consegue adicionar a impressora da rede.

❖ COMPARTILHANDO ARQUIVOS E PASTAS:

1. Agora vamos compartilhar uma pasta para disponibilizarmos a outros computadores na rede, por clicar com o botão direito do mouse, em Propriedades na guia Compartilhamento.
2. Clique em Compartilhamento Avançado.
3. Clique em Continuar na caixa de diálogo do Controle de Conta de Usuário.



SAIBA MAIS

As permissões NTFS possibilitam diferentes permissões de acesso para arquivos e pastas, ou seja, em uma mesma pasta, pode-se ter arquivos com permissões diferentes para usuários diferentes. Isso confere um controle de acesso de forma mais detalhado.

4. Habilite a opção Compartilhar esta pasta e pressione o botão Permissões.
5. Na tela permissões de compartilhamento é possível adicionar ou remover usuários ou grupos, bem como atribuir para os mesmos permissões de controle total, alteração e leitura.
6. Após definidas as permissões de compartilhamento, pressione o botão OK e mais uma vez, clique no botão OK, para compartilhar a pasta.
7. No Windows existem dois tipos de controle de acesso disponíveis: a nível de compartilhamento, que acabamos de definir e a nível de permissão NTFS que iremos definir agora.
8. Após ter definido o compartilhamento, clique com o botão direito do mouse em Propriedades na guia Segurança. É aí que serão definidas as permissões NTFS.
9. Clique no botão Editar e adicione ou remova o usuário ou grupo para quem você irá compartilhar.
10. Em seguida defina as permissões NTFS que podem ser: controle total, modificar, ler e executar, leitura, gravar e listar conteúdo de pasta.
11. Clique em OK e pronto. Agora você pode acessar de outro computador a pasta compartilhada, clicando em Iniciar, Executar e por digitar:
`\nome_do_computador\pasta_compartilhada\`

Nota 1:

No Windows Vista versão Ultimate, para adicionar usuários e grupos, você deve ir em Configurações, clicar em Painel de Controle em seguida clicar duas vezes em Ferramentas Administrativas e em Gerenciamento do Computador. Expandir a árvore Usuários e Grupos Locais e clicar com o botão direito do mouse sobre usuários ou grupos para criá-los. Para outras versões Windows, no Painel de Controle em Contas de Usuário, é possível apenas criar as contas de usuários, não há opção para criar grupos locais.

Nota 2:

Para os dois tipos de controle de acesso, tanto a nível de compartilhamento quanto a nível de permissão NTFS, vai prevalecer a permissão mais restritiva entre eles ou seja, se você define que um usuário terá direito de alteração por meio de permissão de compartilhamento e não determinar permissão a nível de NTFS, a permissão resultante será a mais restritiva ou seja, o usuário não terá permissão de acesso a pasta.

LABORATÓRIO DE AULA II

Objetivos:

1. Ter contato com uma ferramenta de simulação de redes de computadores;
2. Desenhar as principais topologias de rede.

Packet Tracert é um programa educacional gratuito desenvolvido pela empresa Cisco com o objetivo de gerar uma simulação de rede de computadores, através equipamentos e configurações presente em situações reais. O programa apresenta uma interface gráfica simples, com suporte multimídia (gráfica e sonora) que auxiliam na confecção das simulações. Atua com recurso drag-and-drop (arrastar e soltar) também com comandos de console em um modo mais avançado e é capaz de, quando configurado corretamente, encontrar as melhores rotas para os pacotes. Roda em sistema operacional Windows (XP, 2000 e Vista) e Linux (Ubuntu e Fedora). As versões atuais do programa já oferecem suporte para os novos protocolos utilizados nas indústrias e pelos governos como o IPv6, RSTP, SSH e outros.

❖ Procedimentos:

1. Baixar, instalar e executar o aplicativo Packet Tracert.
2. Assistir o vídeo “Como criar uma rede”: <http://www.youtube.com/watch?v=lymq6hnKOP0>
3. Desenhar as principais topologias de rede (barramento, estrela e anel)

LABORATÓRIO DE AULA III

Objetivo:

- Utilização de comandos do TCP/IP para resolver problemas durante uma conexão (internet ou rede local).

Procedimentos:

WINDOWS

1. Executar o prompt de comando do MS-DOS, normalmente localizado em Iniciar > Programas, ou ainda na pasta Acessórios.



Para testar a instalação do seu adaptador de rede execute:
ping 127.0.0.1. Esse endereço IP envia uma mensagem para si mesmo podendo testar sua própria placa. O endereço de qualquer computador como site Web ou ftp pode ser descoberto também.

Ex: ping www.ifsc.edu.br

2. Digitar ipconfig <ENTER>
Saída: Mostra qual o endereço IP, máscara de rede e default gateway.
3. Digitar hostname <ENTER>
Saída: Exibe o nome do computador atual.
4. Digitar ping [nome_maquina] <ENTER>
Saída: Verifica pelo nome da máquina se a mesma está ativa na rede.
5. Digitar ping [ipdestino] <ENTER>
Saída: Verifica pelo número ip se a máquina está ativa na rede.
6. Digitar arp -a <ENTER>
Saída: Mostra a tabela arp (endereço IP associado a cada endereço MAC) de cada placa de rede.
7. Digitar netstat -a <ENTER>
Saída: Exibe as conexões atuais que utilizam o protocolo IP, TCP e UDP.
8. Digitar tracert www.ifsc.edu.br
Saída: Mostra qual é o caminho que uma mensagem percorre até atingir o destinatário, a partir do seu computador.

LINUX: (UBUNTU):

1. Executar o terminal, normalmente localizado em Aplicativos>Acessórios e digitar os comandos.
2. Digitar ifconfig <ENTER>
Saída: Mostra qual o endereço IP, máscara de rede e default gateway.
3. Digitar hostname <ENTER>
Saída: Exibe o diretório corrente.
4. Digitar ping [hostname] <ENTER>
Saída: Verifica pelo nome da máquina se a mesma está ativa na rede.
5. Digitar ping [ipdestino] <ENTER>
Saída: Verifica pelo número ip se a máquina está ativa na rede.

6. Digitar arp -a <ENTER>

Saída: Mostra a tabela arp (endereço IP associado a cada endereço MAC) de cada placa de rede.

7. Digitar netstat -a <ENTER>

Saída: Exibe as conexões atuais que utilizam o protocolo IP, TCP e UDP.

8. Digitar traceroute www.ifsc.edu.br

Saída: Mostra qual é o caminho que uma mensagem percorre até atingir o destinatário, a partir do seu computador.

LABORATÓRIO DE AULA IV

Objetivos:

Instalar e configurar um servidor FTP para as plataformas Windows e Linux.

No Windows usaremos o servidor ftp Cesar-Ftp, por ser um dos melhores e mais simples de usar.

No Linux (Ubuntu) usaremos o servidor ftp Vsftpd por ser mais seguro e rápido para sistemas Unix e seus derivados.

O software Cesar-FTP para Windows e o software Vsftpd possuem versão gratuita para download.

Procedimentos:

Como Configurar um Servidor FTP no Windows

Fonte: <http://www.baboforum.com.br/forum/index.php?/topic/232337-tutorial-como-criar-um-servidor-ftp/>

Passo 1 – Após instalar o software, executar o aplicativo por clicar no atalho localizado na Área de trabalho ou através do Menu Iniciar. Após isso, clique no menu Settings, na opção Edit Users & Groups.



Fig.23 – Users & Groups

Passo 2: Na janela “User & Group settings” clique no botão Add User. No campo User/Group name digite o seu nome. Habilite a caixa “Enable account”.

Se quiser disponibilizar um site FTP com acesso somente com usuário e senha, preencha o campo Login com um nome de usuário e marque a caixa Password para digitar uma senha. Senão, você pode deixar o site FTP com permissão de acesso a todos, por clicar no botão Anonymous Access, deixando a caixa Password desmarcada.

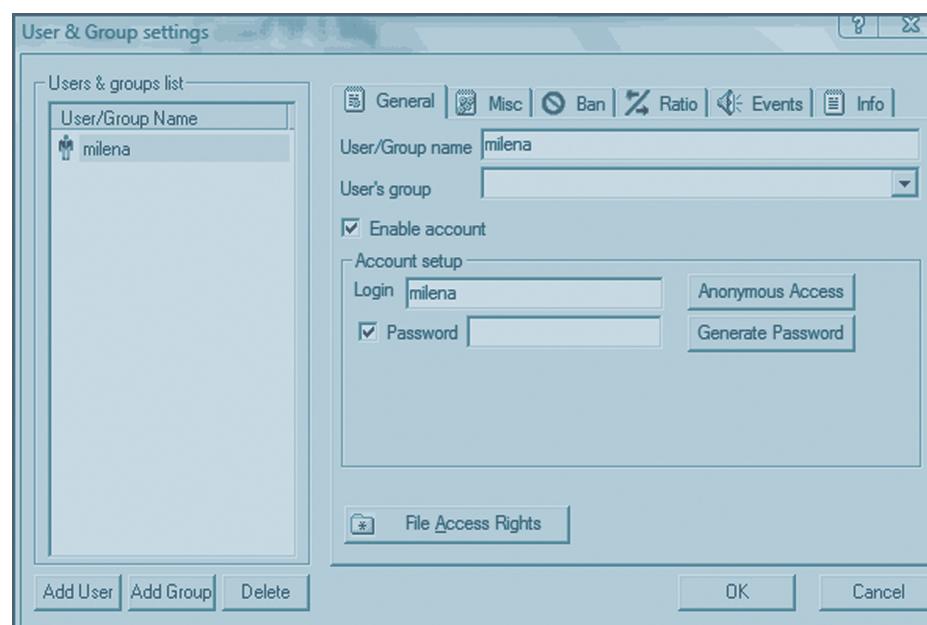


Fig.24 – Adicionando Usuário

Passo 3: Clique no botão File Access Rights. Para compartilhar arquivos por FTP, basta arrastar os arquivos da parte superior da janela para a parte inferior.

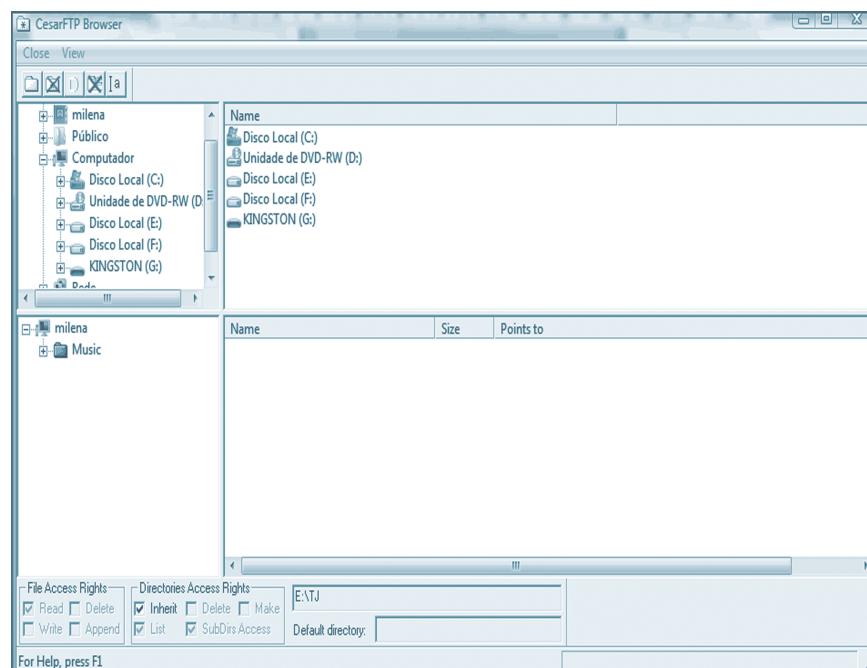


Fig.25 – Compartilhando arquivos

Passo 4: Você pode criar uma nova pasta no seu FTP por clicar com o botão direito do mouse na área em branco da parte inferior da janela e selecionar Add a virtual directory. Após terminar de compartilhar os arquivos, clique em Close.

Nesse momento, o servidor está pronto e já pode ser acessado.

Para acessar o site, abra o seu Navegador e digite o seu endereço IP, precedido de 'ftp://' na barra de endereços do seu browser (Ex.: <ftp://127.0.0.1>).

Observações:

1. Você será notificado e poderá monitorar os usuários conectados no seu site FTP. Poderá fazer isso por clicar no menu Statistics e em seguida em Show.
2. Você pode determinar o acesso dos usuários no seu site em um dado momento. Para isso, é necessário clicar no ícone de Semáforo da barra de ferramentas. Quando mudar para vermelho, o servidor será fechado e nenhum usuário poderá acessar. Aqueles que estiverem navegando, serão desconectados do FTP.

Ao clicar no ícone de um cadeado, o semáforo mudará para amarelo e o seu servidor ficará fechado apenas para quem quiser entrar. Ao clicar novamente no ícone de semáforo, ele mudará para verde, e significa que o servidor estará aberto para quem quiser acessar.

Como Configurar um Servidor FTP no Ubuntu

Fonte: <http://pplware.sapo.pt/linux/como-montar-um-servidor-ftp-no-ubuntu/#more-35283>

Passo 1 - No terminal, instalar o vsftpd, por digitar no prompt:

```
$ sudo apt-get install vsftpd
```

Observação: O arquivo de configuração do vsftpd está em /etc/vsftpd.conf

- Para habilitar o acesso “anônimo”, basta digitar:

```
$ sudo nano -w /etc/vsftpd.conf
```

- Alterar a linha:

```
anonymous_enable=YES
```

Passo 2 – Para não permitir a autenticação de outros usuários FTP, é possível adicionar um falso shell (shell fake).

- Para isso, vamos digitar:

```
$ sudo nano -w /etc/shells
```

- E adicionar a linha /bin/false:

```
# /etc/shells: valid login shells  
/bin/sh  
/bin/bash  
/bin/false
```

Passo 3 – Agora vamos criar uma pasta para o usuário (ex. /home/ftp/maria)

```
$sudo mkdir -p /home/ftp/maria
```

Passo 4 - Cadastrar usuário, definir qual seu diretório e associá-lo ao shell “fake” (ex. user maria)

```
$sudo useradd maria -d /home/ftp/maria/ -s /bin/false
```

Passo 5 – Vamos criar/mudar a password do usuário (com o comando passwd)

```
$sudo passwd maria
```

Passo 6 - Também temos que dar permissões de escrita para o usuário acessar a sua pasta, uma vez que a pasta criada está associada ao root. Para isso, vamos digitar:

```
$sudo chown maria /home/ftp/maria
```

Passo 7 – Depois de prontas as configurações, apenas será necessário reiniciar o serviço vsftpd através do comando:

```
$ sudo /etc/init.d/vsftpd restart
```

Passo 8 – Para acessar o FTP basta carregar o navegador e digitar: ftp:// seguido do seu endereço IP. Ou acesse através de uma aplicação cliente para FTP (ex. filezilla, fireFTP).



Fig.26 – Acesso ao Vsftpd.

Passo 9: Inserir os dados de autenticação.

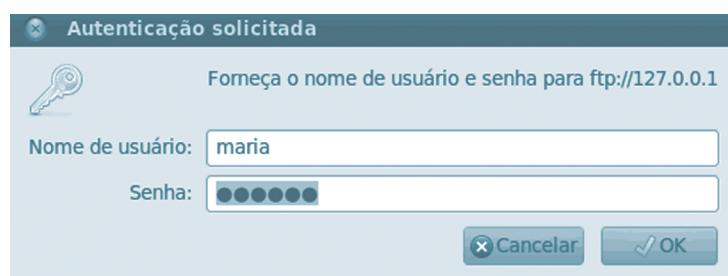


Fig.27 – Autenticação Vsftpd.

Pronto. Agora você pode disponibilizar conteúdo para compartilhar.

LABORATÓRIO DE AULA V

Objetivo:

Para entender como os pacotes trafegam entre suas conexões (seu computador com a Internet, com o cliente de email, ftp,...) e entender como as conexões são estabelecidas e mantidas, usaremos o Wireshark.

Ele é um poderoso sniffer (farejador de rede), que permite capturar o tráfego da rede, fornecendo uma ferramenta poderosa para detectar problemas e entender melhor o funcionamento de cada protocolo.

O Wireshark possui versão gratuita para download.

Redes de Computadores

Procedimentos:

Fonte: <http://www.numaboa.com/informatica/oficina/163-rede/720-wireshark>

Passo 1: Durante a instalação do Wireshark, o WinPcap deve ser instalado para o funcionamento da captura de pacotes.

Passo 2: Execute o Wireshark.

Passo 3: Selecione a interface de rede para a captura dos pacotes, por clicar no menu

Capture/Interfaces



Fig.28 – Ativando a captura Wireshark.

Passo 4: Escolha uma interface de rede para teste e clique no botão “Start”. Abra o navegador e digite um site para observar que imediatamente o Wireshark mostra em tela os pacotes capturados.

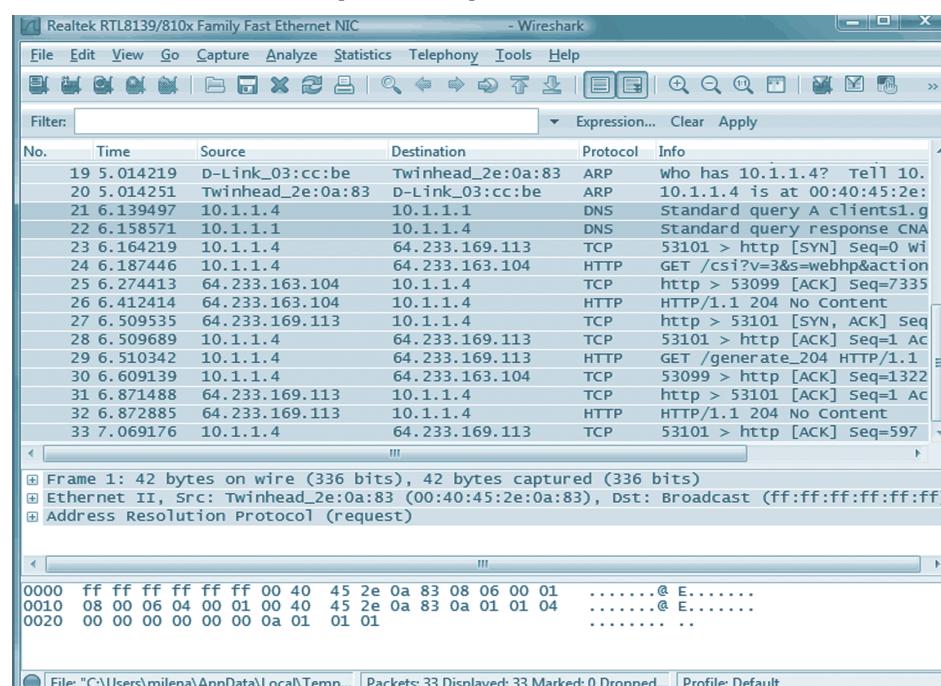


Fig.29 – Interface de captura Wireshark.

Observação: Para interromper a captura de pacotes clique no menu Capture / Interfaces no botão “Stop”.

Passo 5: Vamos observar os pacotes capturados.

- O primeiro pacote envia uma mensagem broadcast ARP (Address Resolution Protocol - Protocolo de Resolução de Endereço). Pois, foi solicitado ao navegador um domínio (no caso, o site que você digitou) fora da rede local. Para estabelecer comunicação com a máquina externa, o roteador da rede local deve atribuir para a placa de rede um endereço MAC da sua placa Ethernet.
- O segundo pacote obtém como resposta através do mesmo protocolo ARP o endereço MAC.
- O terceiro pacote DNS realiza a tradução de nome de domínio em endereço IP. Existem máquinas especializadas em fazer estas traduções - são os chamados servidores de nomes ou DNS.
- O quarto pacote traz a tradução solicitada e a comunicação é estabelecida a partir do envio do quinto pacote pelo protocolo TCP.

Passo 6: Analisar como o pacote irá navegar pela internet.

Com o quinto pacote do protocolo TCP selecionado, na tela intermediária do Wireshark, vamos clicar no botão “+” para expandir o título “Transmission Control Protocol”. Observe na tela inferior que a porta TCP de origem é 53101 e servirá para redirecionar a resposta. A porta TCP do destino deve ser a 80 (reservada para o HTTP).

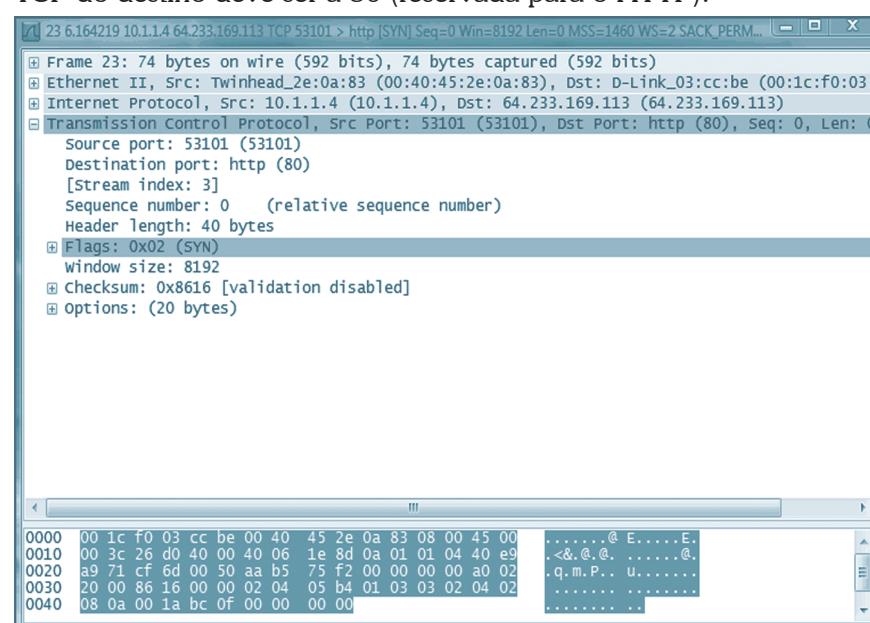


Fig.30 – Analisando pacote Wireshark.

Também, é possível observar que para estabelecer a comunicação o pacote envia um pedido de sincronização através da flag SYN.

Usando estas informações, a placa de rede encaminha o pacote na rede e até que chegue ao destino e que a máquina receba uma resposta.

Revisão:

Com o uso do Wireshark:

- ❖ Capturamos pacotes ao navegar na internet;
- ❖ Compreendemos a importância do protocolo ARP ao estabelecer comunicação com uma rede externa.

O nome de domínio que digitamos no navegador, endereço “www”, necessita de um DNS que é um serviço de tradução de nome.

O protocolo TCP estabelece a comunicação entre duas máquinas enviando o pacote ao destino.

LABORATÓRIO DE AULA VI

Objetivo:

- Configuração Manual do Protocolo TCP/IP nas plataformas Windows Vista/Linux (Ubuntu).

Antes de começar a configurar o protocolo TCP/IP, verifique se o driver (software) do adaptador de rede está instalado.

Também você notará que por padrão, o Windows Vista utiliza o endereço automático (DHCP).

Procedimento:

Windows Vista:

Passo1: Acesse o Painel de Controle e clique duas vezes no item Centro de Rede e Compartilhamento.

Passo2: Na guia Tarefas clique em Gerenciar conexões de rede.

Passo3: Ao instalar o adaptador de rede, uma conexão chamada Conexão de rede local (caso seja um adaptador de rede cabeada) ou conexão de rede sem fio é criada pelo Windows Vista. Clique com o botão direito do mouse no item e selecione Propriedades.

Passo4: Se a caixa de diálogo Controle de Conta de Usuário aparecer, clique em Continuar.

Passo5: Na guia Rede é possível configurar o protocolo TCP/IP. Basta selecionar a opção Protocolo TCP/IP versão 4 (TCP/IPv4) e clicar em Propriedades.

Passo6: Na guia Geral do protocolo TCP/IP você pode configurar o endereço IP, a máscara de sub-rede e o gateway padrão do host e ainda o endereço IP dos servidores DNS.

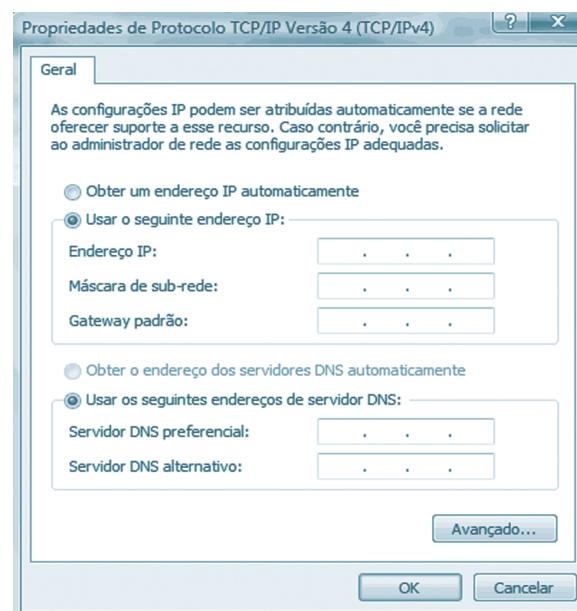


Fig.31 – Propriedades do Protocolo TCP/IP.

Passo7: Caso a interface de rede esteja conectada a uma rede local sem servidor DHCP, como é o caso de redes baseadas no Windows Vista, você pode atribuir um endereço privado de classe C, como por exemplo, 192.168.1.X, em que X varia entre 1 e 254 com valores únicos em cada computador. Neste caso a máscara de sub-rede deve ter valor igual a 255.255.255.0

Passo8: Caso um dos computadores da rede compartilhe a Internet, pelo recurso de compartilhamento do Windows Vista você deve manter o endereçamento automático nos outros computadores.

Ubuntu:

Passo1: Acesse Sistema / Preferências e clique em conexões de rede.
Note que aparecem as pastas Com fio, Sem fio, Banda larga móvel, VPN e DSL.

Passo2: Na pasta Com fio, clicar em Auto Eth0 e pressionar o botão editar.

Passo3: Desmarcar a opção “conectar automaticamente”.

Passo4: Na pasta “Configurações IPv4 selecionar o método manual.

Passo5: Pressionar o botão “Adicionar” e digitar o endereço, máscara de rede e gateway default. Informar o servidor de DNS, caso exista.

Passo6: Clicar no botão Aplicar.

LABORATÓRIO DE AULA VII

Objetivos:

- Configuração da Rede Windows Vista nas plataformas Windows Vista/Linux (Ubuntu).

Procedimentos:

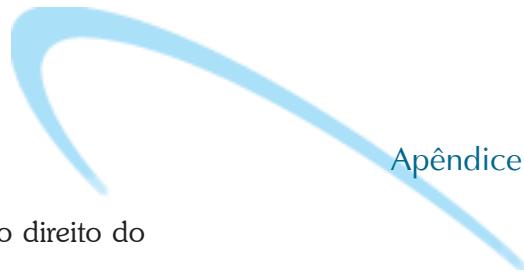
Antes de iniciar a configuração da rede, verifique se o adaptador de rede está instalado.

Windows Vista:

Passo1: Clique em Iniciar > Painel de Controle > Centro de Rede e Compartilhamento.

Passo2: Clique em Gerenciar conexões de rede.

Passo3: Observe se o adaptador de rede do computador está presente. Caso contrário, utilize o gerenciador de dispositivos para instalar os drivers do adaptador de rede.



Apêndice

Passo4: Caso a conexão seja exibida, clique com o botão direito do mouse na conexão e selecione Propriedades.

Passo5: Clique em Continuar na caixa de diálogo do Controle de Conta de Usuário.

Passo6: A configuração padrão apresenta o cliente para redes Microsoft (utilizado para acesso a redes ponto a ponto ou baseadas em domínios (Windows NT/2000/2003/2008), o compartilhamento de arquivos e impressoras para rede Microsoft (permite que seu computador compartilhe uma impressora ligada localmente ou ainda arquivos armazenados localmente), o agendador de pacotes QoS (que permite melhor gerenciamento da largura de banda alocada pelo computador) e o protocolo TCP/IP (o mais utilizado tanto na Internet como em redes locais).

Passo7: Na janela de propriedades da conexão, clique duas vezes no componente Protocolo TCP/IP versão 4 e se precisar configurá-lo, volte ao último laboratório de aula.

Passo8: Para verificar todos os detalhes da conexão, basta clicar duas vezes na conexão configurada, dentro da janela de Conexões de Rede.

Passo9: Ao ser exibida a janela de status da conexão, clique no botão Detalhes e verifique todas as informações sobre a conexão.

Passo10: Se a sua conexão de rede for baseada no padrão 802.11, ou seja, uma rede sem fios Wi-Fi, clique com o botão direito do mouse na conexão (na janela de conexões de rede) e selecione Conectar/Desconectar.

Passo11: Para conectar-se a uma rede, clique duas vezes nela e siga as orientações do assistente, informando a chave de segurança e o tipo de rede.

Linux (Ubuntu)

Passo1: Acesse Sistema / Preferências e clique em conexões de rede.

Passo2: Na pasta Com fio, clicar em Auto Eth0 e pressionar o botão editar.

Passo3: Caso seja necessário configurar o protocolo TCP/IP manualmente, desmarque a opção “Conectar automaticamente” e volte ao último laboratório de aula.

Passo4: Para identificar a placa de rede, acessar: Sistema -> Administração -> Ferramentas de Rede.

LABORATÓRIO DE AULA VIII

Objetivos:

- Realizar a instalação e configuração de um servidor Web na plataforma Windows.
- Disponibilizar uma página para acesso em uma rede local.

Para instalação do servidor Web usaremos o programa Apache Server que possui versões para Windows e Linux e pode ser baixado pelo site: <http://www.apache.org/dist/httpd/binaries/win32/>
As versões disponíveis para download são gratuitas.

Procedimentos:

Passo 1: Execute o instalador do programa.

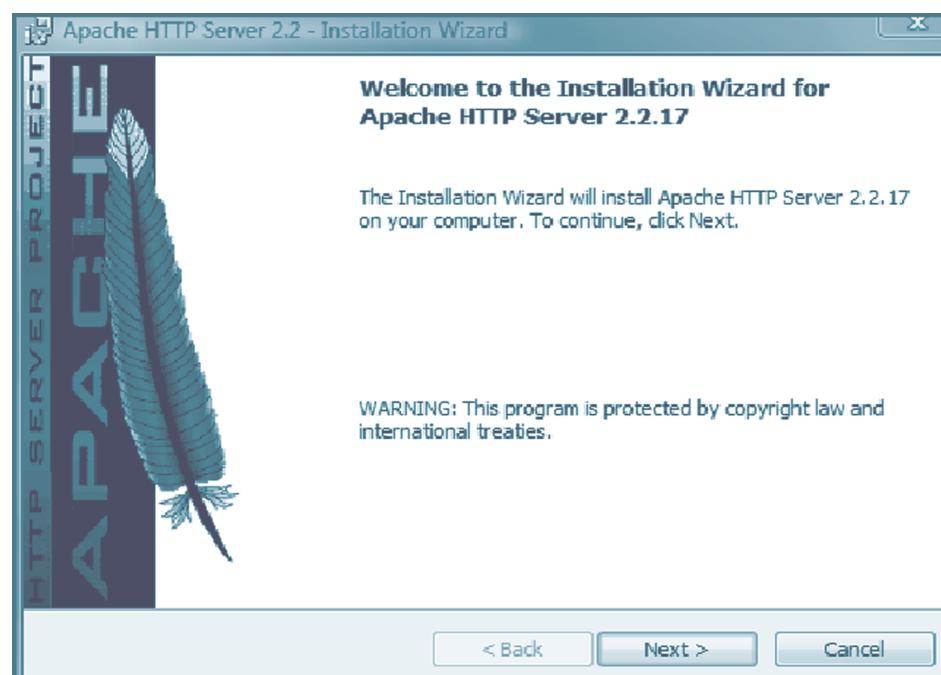


Fig.32 – Instalação do Apache.

Passo 2: Clique no botão “Next”.

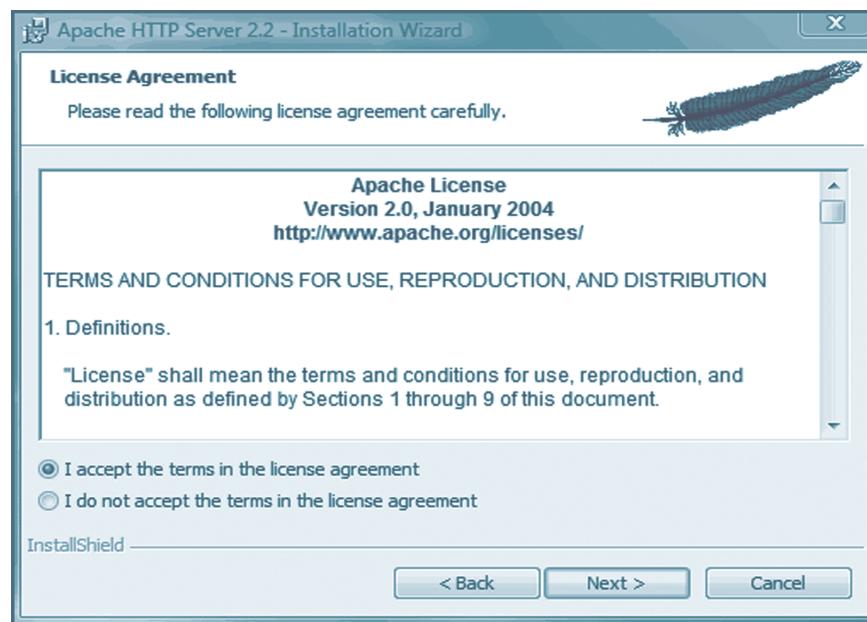


Fig.33 – Termos de Licença Apache.

Passo 3: Marque a opção “I accept the terms in the license agreement” e clique no botão “Next” duas vezes.

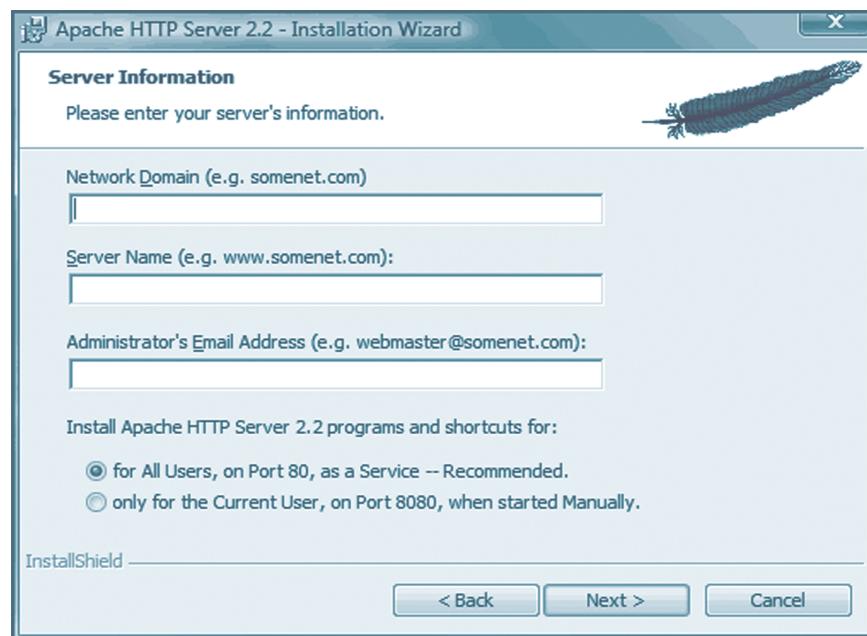


Fig.34 – Informações sobre o Servidor Apache

Passo 4: Agora vamos configurar o endereço do servidor. No campo Network Domain, digite o endereço do servidor. Para rede local (intranet) deverá ser preenchido com: localdomain. Se usarmos endereço internet (www) devemos preencher com um endereço de conta. No campo Server Name digite o nome do servidor. Para rede local deverá ser preenchido com localhost. Se usarmos endereço internet (www) coloque o endereço de sua conta. No campo Administrator's Email Address preencha com o email do administrador do servidor.

Passo 5: Clique no botão "Next", e aparecerá a tela do tipo de instalação.

Passo 6: Clique no botão "Next" e aparecerá o local de instalação do Apache.

Passo 7: Clique no botão "Next" e no botão Install para iniciar a instalação.

Passo 8: Clique no botão "Finish" para concluir.

Passo 9: Agora, vamos disponibilizar uma página no servidor Apache. Para isso, devemos salvá-la como index.html no diretório: "C:\Program Files\Apache Software Foundation\Apache2.2\htdocs"

Passo 10: Clique duas vezes no ícone ao lado do relógio do Windows. Na janela "Apache Service Monitor", clique no botão "Restart".

Passo 11: Verifique se o servidor está configurado corretamente para a nova página, para isso, abra o navegador e digite: <http://localhost>

Observações:

1. Para outras pessoas acessarem a página na rede local, devem digitar no navegador: http://seu_ip:80 (http seguido do endereço ip da sua máquina e o número da porta.)
2. Para alterar o endereço do servidor Apache, o arquivo de configuração a ser editado pode ser acessado em: "Menu Iniciar/ Todos os Programas/ Apache HTTP Server 2.2/ Configure Apache Server / Edit the Apache httpd.conf Configuration File"

Referências Bibliográficas

Assunção, Marcos Flávio Araújo. Segredos do Hacker Ético, 3^a Edição, Editora Visual Books, Santa Catarina, Rio de Janeiro, 2010

Baddini, Francisco, Gerenciamento de Redes com Windows Vista, Editora Erica, São Paulo, 2009

Marimoto, Carlos E.; <http://www.guiadohardware.net>

Packet Tracer, http://pt.wikipedia.org/wiki/Packet_Tracer

Specialski, Elizabeth Sueli. Apostila Arquitetura de Redes de Computadores, 2000.

Wikipédia, http://pt.wikipedia.org/wiki/Cabo_coaxial

Ulbrich, Henrique César. Universidade Hacker, Editora Digerati Books, São Paulo, 2007.

