TCP/IP - Internet e Intranet

Mauro Roisenberg
mauro@inf.ufsc.br

OBJETIVOS

- Familiarizar os participantes com conceitos e terminologias empregadas em Redes de Computadores.
- Expor os principais conceitos, teorias e definições presentes no protocolo TCP/IP.
- Apresentar as principais aplicações presentes em ambientes Internet e Intranet.

SÚMULA

- PARTE 1: REVISÃO DE CONCEITOS BÁSICOS
  - HISTÓRICO
  - ARQUITETURA DE REDES
  - O MODELO DE REFERÊNCIA OSI da ISO.
- PARTE 2: NÍVEL DE ENLACE
  - REDES LOCAIS - ETHERNET
  - PROTOCOLOS PARA ACESSO VIA PROVEDORES: SLIP & PPP

SÚMULA

- PARTE 3: O CONJUNTO DE PROTOCOLOS TCP/IP
  - MODELO CONCEITUAL
  - O PROTOCOLO IP
    - **O ENDEREÇAMENTO IP**
    - **O PROTOCOLO ARP**
  - O ROTEAMENTO
    - **O ROTEAMENTO IP**
    - **ROTEADORES E SEUS PROTOCOLOS**
  - O PROTOCOLO ICMP

SÚMULA

- PARTE 3: O CONJUNTO DE PROTOCOLOS TCP/IP
  - O PROTOCOLO TCP
  - O PROTOCOLO UDP
- PARTE 4: FERRAMENTAS E APLICAÇÕES
  - PARADIGMA CLIENTE X SERVIDOR
  - WELL-KNOWN PORTS
  - DOMÍNIOS
  - APLICAÇÕES
  - GERENCIAMENTO

SÚMULA

- PARTE 5: INTRODUÇÃO A INTRANETS
  - ADMINISTRAÇÂO DE INTRANETS
  - CONEXÃO A INTERNET
- PARTE 7: FERRAMENTAS DE AUTORIA
- PARTE 6: SEGURANÇA NA INTERNET
  - FORMAS DE ATAQUE
  - MECANISMOS DE PROTEÇÂO

BIBLIOGRAFIA

1. TAROUCO, L. Redes de Computadores. McGraw-Hill, 1986.
2. TANNEBAUM, A. Computer Networks. 1989.
3. STALLING, W. ISDN and Broadband ISDN. USA, Mc Millian, 1992.
4. SOARES, L. F. G., LEMOS, G., COLCHER, S. Redes de Computadores. Das LANS, MANS e WANS às Redes ATM. Editora Campus. 1995.
5. COMER, D. Internetworking with TCP/IP. V. I, Third Edition, 1995.
6. COMER, D. Internetworking with TCP/IP. V. II, Second Edition, 1995.
7. ABLAN, J., REINER, E. Developing Intranet Applications With Java. Book & Cd edition, 1996.

BIBLIOGRAFIA

8. CARVALHO, T. et alli.,*"Arquiteturas de Redes de Computadores: OSI e TCP/IP"*, Makron Books/BRISA, Rio de Janeiro, 1994.
9. EVANS, T. *"Building an Intranet"*, 1ª edição, Ed. Sams Net, Indiana, 1996.
10. GASPARINI, A. F. L.; BARRELLA, F. E. *"TCP/IP: Solução para Conectividade"*, Ed. Érica, São Paulo, 1993.
11. MAZZOLA, V. B. "Internet e Intranet" Notas de Aula - CPGCC-UFSC

Pré-Teste

1- Quantas camadas possui o Modelo de Referência OSI da ISO?

2- Diga se as seguintes topologias de são de Difusão (Broadcast) (D) ou Ponto-a-Ponto (P).

( ) Barramento
( ) Estrela
( ) Árvore
( ) Anel
( ) Satélite

Pré-Teste

3- Entre as razões listadas abaixo, qual a principal para a utilização das redes de computadores atualmente?

(a) Compartilhamento de recursos (disco e impressora)
(b) Acesso remoto ao computador
(c) Compartilhamento de informações (groupware e bases de dados)
(d) Homebanking
(e) Cópia de programas shareware

Pré-Teste

4- Assinale com um X quais das características abaixo se aplicam as Redes Locais.

(a) Cobrem uma área geográfica limitada
(b) Velocidades da ordem de Kbps
(c) Baixa confiabilidade dos meios de transmissão
(d) Velocidades da ordem de Mbps
(e) Utiliza nós de comutação de pacotes
(f) Alto desempenho

Pré-Teste

5- Complete a coluna da direita de acordo com as definições da coluna de esquerda

(a) CSMA/CD ( ) IEEE 803.5
(b) Token-Ring ( ) IEEE 802.3
(c) Token-Bus ( ) IEEE 802.4
( ) Ouvir antes de falar
( ) Um "token" é passado entre as estaçõesformando um "anel lógico"
( ) Se "cair" uma estação toda a rede pára
( ) Não suporta redes muito carregadas

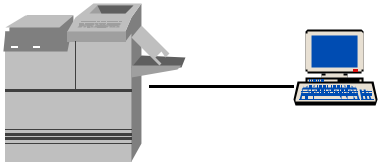
PARTE 1

REVISÃO DE CONCEITOS BÁSICOS

- HISTÓRICO
- ARQUITETURA DE REDES
- O MODELO DE REFERÊNCIA OSI da ISO

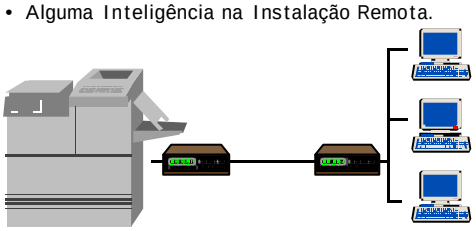
Histórico

- **DÉCADA DE 50**
  - **TELEPROCESSAMENTO**
    - Toda a Inteligência Centrada no Computador.
    - Utiliza a Infra-Estrutura já Existente para a Telefonia.



Histórico

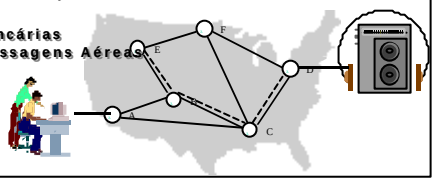
- **DÉCADA DE 60**
  - **TELEPROCESSAMENTO**
    - Compartilhamento da Linha de Comunicação.
    - Alguma Inteligência na Instalação Remota.



Histórico

- **DÉCADA DE 70**
  - **REDES DE COMPUTADORES**
    - Redes Destinadas Exclusivamente à Comunicação de Dados.
    - Redes Comutadas.
      - Comutação de Circuitos.
      - Comutação de Pacotes.

Aplicações Bancárias
Reserva de Passagens Aéreas



Histórico

- **DÉCADA DE 80**
  - **REDES DE COMPUTADORES**

MOTIVADOR

- Surgimento e Popularização dos Computadores de Uso Pessoal.
- Alto Custo dos Periféricos.

CARACTERÍSTICAS

- Cobre uma área geográfica limitada.
- Em geral pertence a uma mesma organização.
- Taxas de transferência muito alta.
- Meios de transmissão baratos.
- Taxas de erros muito baixas.

Histórico

- **FINAL DA DÉCADA DE 80 E DÉCADA DE 90**
  - **Novas Aplicações (COMPARTILHAMENTO DE INFORMAÇÕES, TEAMWORK, etc.).**
  - **Interligação com Redes de Longas Distância.**
- **MEADOS DA DÉCADA DE 90 ATÉ OS DIAS ATUAIS**

Conceitos Básicos

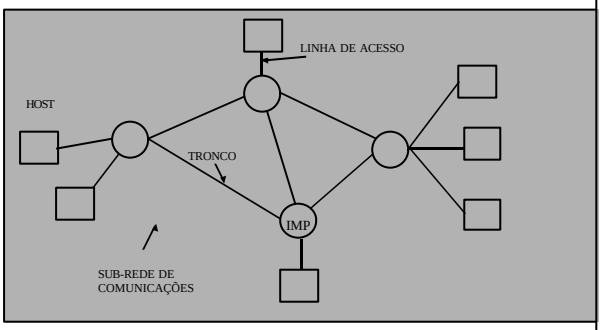
- CONCEITUAÇÃO DE REDES
  - Um Conjunto de Computadores Autônomos Interconectados Através de um Meio de Transmissão.
- OBJETIVOS
  - Compartilhamento de informações, programas e periféricos, não importando a localização física dos recursos e dos usuários.
  - Aumento de confiabilidade através de fontes alternativas de recursos.
  - Permitir o trabalho integrado e troca de informações entre as pessoas.

Conceitos Básicos

- HOSTS ou ESTAÇÕES
  - Computadores que rodam os programas de aplicação do usuário.
- COMMUNICATION SUBNET ou SUB-REDE DE COMUNICAÇÃO
  - Sistema cuja função é "transportar" as mensagens de uma estação a outra.
- IMP (Interface Message Processor) ou NÓS DE COMUTAÇÃO
  - Computadores dedicados à tarefa de conectar duas ou mais linhas, encaminhando as mensagens chegadas em uma para a outra. Os hosts são conectados a IMPs (uma ou várias) via linhas de acesso.
- TRONCOS ou CANAIS
  - Linhas de transmissão entre os IMPs.

Conceitos Básicos

- **ESTRUTURA DE REDES**



Conceitos Básicos

- TOPOLOGIAS
  - "Forma" pela qual as IMPs se interconectam para formar a Sub-Rede de Comunicação.
  - Em função do tipo de Canal, existem duas grandes classes de Sub-Redes:
    - As que utilizam canais PONTO-A-PONTO.
    - As que utilizam canais de ACESSO MÚLTIPLO, também chamados de canais de "BROADCAST", ou de DIFUSÃO.

Conceitos Básicos

- TOPOLOGIAS
  - **Sub-Redes Ponto-a-Ponto**
    - Cada canal conecta um par de IMPs.
    - Se duas IMPs não compartilham o mesmo canal, elas só podem se comunicar de maneira indireta através de outras IMPs.
  - **Exemplos:**
    - ESTRELA, ANEL, ÁRVORE, COMPLETA, IRREGULAR

Conceitos Básicos

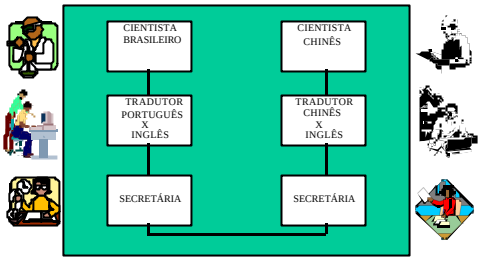
- TOPOLOGIAS
  - **Sub-Redes de Difusão**
    - Mensagens enviadas por qualquer IMP são recebidas por todos os outros IMPs.
    - Algo na mensagem deve especificar para quem a mensagem é destinada.
    - Mensagens recebidas, destinadas a outro IMP são ignoradas.
  - **Exemplos:**
    - **BARRAMENTO, ANEL, SATÉLITE**

Arquitetura de Redes

- **Conceitos**
  - As modernas redes de computadores são projetadas de maneira altamente estruturada.
  - HIERARQUIA DE PROTOCOLOS
  - A maioria das redes são organizadas como uma série de camadas (terminologia ISO) ou níveis (terminologia CCITT/ITU), cada um construído sobre seu predecessor.
  - OBJETIVO: Reduzir a complexidade de projeto. "Divida e Conquiste". - Júlio Cesar
  - FUNÇÃO: Oferecer serviços de comunicação aos níveis superiores, tornando transparente a forma como estes serviços são implementados.

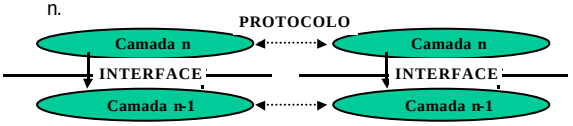
Arquitetura de Redes

- O conjunto de camadas e protocolos é chamado de ARQUITETURA DE REDES.
- Exemplo:



Arquitetura de Redes

- A camada n de uma máquina "conversa" com a camada n de outra máquina utilizando os serviços oferecidos pela camada n-1.
- As regras e convenções utilizadas nesta "conversação" são conhecidas como PROTOCOLO da camada n.
- Entre duas camadas adjacentes existe uma INTERFACE. A interface define que operações e serviços uma camada n-1 oferece para uma camada n.



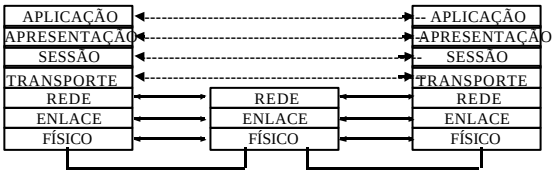
Modelo OSI/ISO

- O MODELO DE REFERÊNCIA OSI DA ISO
  - ISO - International Standards Organization
  - OSI - Open Systems Interconnections
- SISTEMAS ABERTOS
  - Sistemas que estão abertos para se comunicar com outros sistemas, independente do fabricante.
- MODELO DE 7 CAMADAS

Modelo OSI/ISO

- **PRINCÍPIOS**
  - **Uma camada deve ser criada quando um diferente nível de abstração é desejado.**
  - **Cada camada deve desempenhar uma função bem definida.**
  - **A função de cada camada deve ser escolhida visando a definição de padrões internacionais de protocolos.**
  - **A fronteira entre as camadas deve ser escolhida de forma a minimizar o fluxo de informações entre as interfaces.**
  - **O número de camadas deve ser grande o suficiente para que funções distintas possam ser executadas por camadas distintas e aos mesmo tempo pequena o suficiente para não prejudicar a compreensão.**

As Camadas do Modelo de Referência



As Funções de Cada Camada

- CAMADA 1 - NÍVEL FÍSICO
  - Trata dos aspectos físicos da transmissão de uma seqüência de bits, sem preocupação se eles foram entregues corretos ou não.
  - taxas de transmissão, tipo transmissão, tipo de conector, etc.
  - Exemplo: RS-232C, X.21, RS-485, etc.

As Funções de Cada Camada

- CAMADA 2 - NÍVEL DE ENLACE
  - O propósito desta camada é gerenciar uma ou mais conexões de enlace de dados entre entidades da camada de rede.
  - É composta por duas SUB-CAMADAS:
    - SUB-CAMADA DE CONTROLE DE ACESSO AO MEIO (MAC - Medium Access Control),
    - SUB-CAMADA DE CONTROLE LÓGICO DO ENLACE (LLC - Logical Link Control).
  - Exemplos: Ethernet, 802.3/802.2, 802.4/802.2, 802.5/802.2

As Funções de Cada Camada

- CAMADA 3 - NÍVEL DE REDE
  - Fornece a trajetória da conexão entre dois processos, possivelmente passando por nós intermediários.
  - Nesse nível são definidos:
    - Endereços e estratégias para roteamento e fragmentação de pacotes através de possíveis sub-redes até chegar à estação de destino.
  - Exemplos: IP, ISO8473

As Funções de Cada Camada

- CAMADA 4 - NÍVEL DE TRANSPORTE
  - Fornece serviços para a transferência confiável e transparente de dados fim-a-fim entre duas máquinas.
  - SEGURANÇA : garante a entrega da mensagem na máquina de destino. ("timeout" e retransmissões)
  - TRANSPARÊNCIA : o usuário não precisa ter conhecimento de como a ligação é feita.
  - Exemplos: TCP, ISO8072 e ISO8073

As Funções de Cada Camada

- CAMADA 5 - NÍVEL DE SESSÃO
  - Objetiva organizar e sincronizar o diálogo, e gerenciar a troca de dados entre entidades comunicantes.
  - O protocolo de sessão estabelece uma união lógica entre dois usuários, transfere informações confiavelmente entre eles, e termina a união quando assim instruída pelos usuários envolvidos.
  - Você já tentou fazer FTP de arquivos muito grandes?

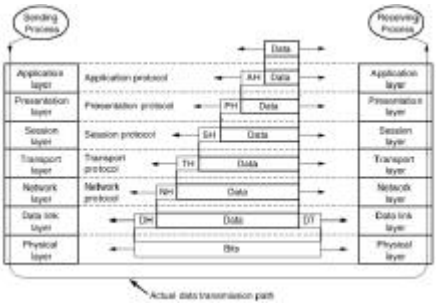
As Funções de Cada Camada

- CAMADA 6 - NÍVEL DE APRESENTAÇÃO
  - Ocupa-se da representação da informação trocada por sistemas abertos comunicantes.
  - Realiza serviços de :
    - compressão de textos, criptografia, conversão de código, etc.

As Funções de Cada Camada

- CAMADA 7 - NÍVEL DE APLICAÇÃO
  - É onde rodam os programas aplicativos dos usuários de uma rede de computadores.
  - Exemplos: FTAM, FTP, TELNET, MMS, etc.

Como o Modelo OSI é Usado



Exercícios

- Coloque nos espaços a seguir o número do nível do modelo OSI/ISO relacionado com a explicação ao lado.

( ) criar conexões entre máquina fonte e destino, independente do número de nós intermediários;
( ) roteamento de pacotes entre fonte e destino, mesmo que para isto tenha que passar por diversos nós intermediários no caminho;
( ) criptografia e compressão de dados;
( ) transmitir uma seqüência de bits através de um canal de comunicação;
( ) tarifação;

Exercícios

- Coloque nos espaços a seguir o número do nível do modelo OSI/ISO relacionado com a explicação ao lado.

( ) transmitir um quadro de dados entre duas máquinas, tratando problemas de quadros errados, perdidos ou duplicados;
( ) modificar a sintaxe da mensagem (mantendo a semântica) a fim de que possa ser entendido pelo receptor;
( ) controle de fluxo entre dois computadores;
( ) fornece ao usuário uma interface que permite acesso a diversos serviços;
( ) administrar e sincronizar diálogos entre dois processos;

Exercícios

- Coloque nos espaços a seguir o número do nível do modelo OSI/ISO relacionado com o nome do protocolo ao lado.

( ) SMTP: Simple Mail Transfer Protocol;
( ) Ethernet;
( ) TCP: Transfer Control Protocol;
( ) UDP: User Datagram Protocol;
( ) RS-232;
( ) IP: Internet Protocol;
( ) Token Ring;
( ) TP4;
( ) X-Windows;
( ) SQL: Structured Query Language.

PARTE 2

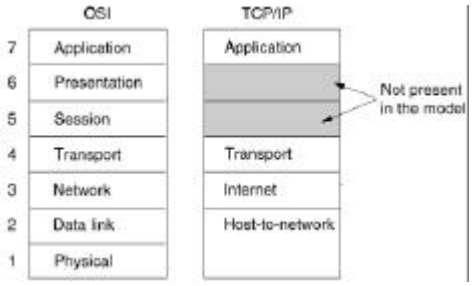
NÍVEL DE ENLACE

- REDES LOCAIS - ETHERNET
- PROTOCOLOS PARA ACESSO VIA PROVEDORES: SLIP & PPP

Introdução: Comunicação entre Processadores

Interprocessor distance	Processors located in same	Example
0.1 m	Circuit board	Data flow machine
1 m	System	Multicomputer
10 m	Room	Local area network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1,000 km	Continent	
10,000 km	Planet	The Internet

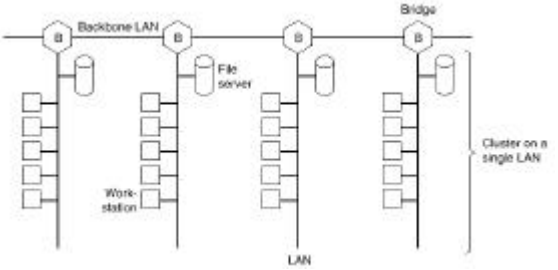
O Modelo TCP/IP



O Modelo TCP/IP

- O TCP/IP não segue o modelo de referência OSI da ISO.
- Ele especifica apenas os protocolos de nível 3, 4 e 7.
- Não se preocupa com que protocolo de enlace está operando.

Possível configuração de rede local

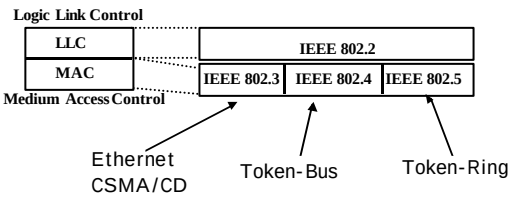


Protocolos de Redes Locais Introdução

- Redes Locais: Recomendação IEEE802
- Conjunto de normas para Redes Locais que diferenciam-se entre si pela utilização do meio físico (meio de transmissão).
- Compatíveis a nível de controle lógico do enlace.
- Adotadas pela ISO 8802.

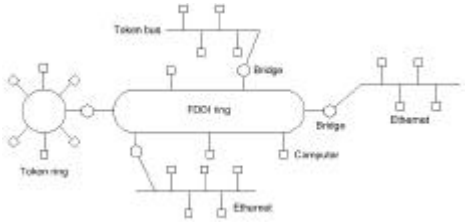
Introdução

- Redes Locais: Recomendação IEEE802



Introdução

- Possível configuração de uma Rede Local Corporativa:

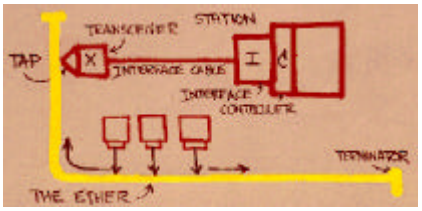


Introdução

- **ETHERNET » IEEE 802.3/802.2 » CSMA/CD**
- Rede Local (Local Area Network - LAN) mais utilizada no mundo inteiro, foi inventada por Robert Metcalfe da Xerox PARC em 1976.
- Padronizada em 1978
  - Intel Corporation,
  - Xerox Corporation, e
  - Digital Equipment Corporation

Introdução

- **ETHERNET » IEEE 802.3/802.2 » CSMA/CD**
  - http://wwwhost.ots.utexas.edu/ethernet/ethernet-home.html (boa referência)

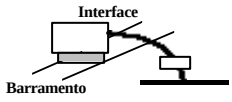


Características Funcionais

- **Disciplina de Acesso: CSMA/CD** - Carrier Sense Multiple Access with Colision Detection
  - Várias máquinas acessam (Multiple Access) o meio simultaneamente, e cada uma determina se o meio está livre, ou não, sentindo a presença de uma portadora (Carrier Sense)

Características Funcionais

- **Esquema de Funcionamento**



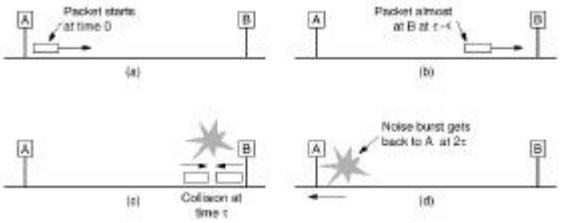
1. **A estação "escuta" o meio**
2. **Meio está livre?**
   sim: inicia transmissão
   não: espera ficar livre

- **Cada transmissão possui uma duração limitada**
- **Existe um tempo mínimo entre duas transmissões (slot time)**

slot time

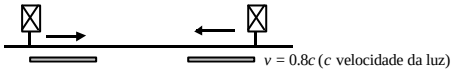
Características Funcionais

- **Esquema de Funcionamento**

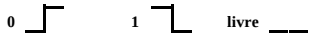


Características Funcionais

- **Collision Detection**
  - Colisão é a presença de duas transmissões na linha em um único intervalo de tempo.
  - É possível de ocorrer em função de atrasos de propagação de sinais na linha (cabo).



  - Transceiver tem condições de detectar a colisão através de violação de código (manchester, por exemplo).



Características Funcionais

- **Jamming**
  - É um reforço do sinal de colisão durante um intervalo de tempo para permitir que todas as estações (transceivers) tenham conhecimento da ocorrência da colisão.
  - Tempo de jamming: 32 bit times

Características Funcionais

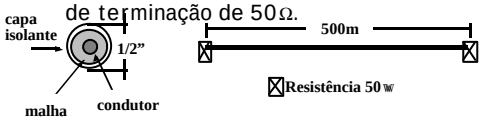
- **Backoff**
  - Solução da contenção, ou seja, quando for detectado uma colisão como determinar qual estação deverá iniciar a transmissão quando o meio ficar livre.
  - Cada estação gera um intervalo aleátorio de tempo para retentar o acesso. A cada nova colisão ocorrida (retentativa) a faixa de intervalo de tempo é dobrada.
    - 1ª vez: espera entre 0 e 1 intervalos de tempo
    - 2ª vez: espera entre 0, 1, 2 e 3 intervalos de tempo – e assim sucessivamente até a 10ª vez

Características Funcionais

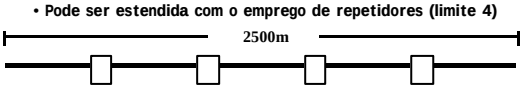
- **Uma rede ethernet é dita:**
  - **tecnologia de barramento**
    - todas as estações dividem um mesmo meio (canal) de comunicação
  - **broadcast**
    - todos transceivers recebem todas as transmissões
  - **best effort delivery**
    - não fornece informação ao transmissor que o sinal (pacote) enviado foi recebido pelo receptor
  - **controle de acesso distribuído**
    - não existe árbitro para acesso local

Características Físicas

- **Ethernet "Cabo Grosso" (thick ethernet)**
  - composta por um cabo coaxial (1/2") e comprimento máximo de 500m e resistores de terminação de 50Ω.

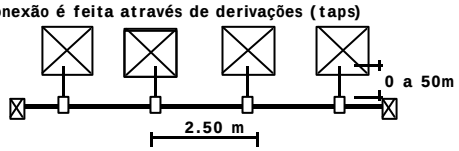


- **Pode ser estendida com o emprego de repetidores (limite 4)**

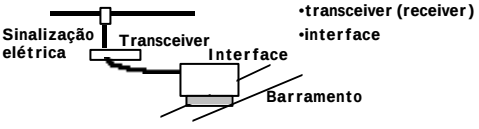


Características Físicas

- **Ethernet "Cabo Grosso" (thick ethernet)**
  - **Conexão é feita através de derivações (taps)**

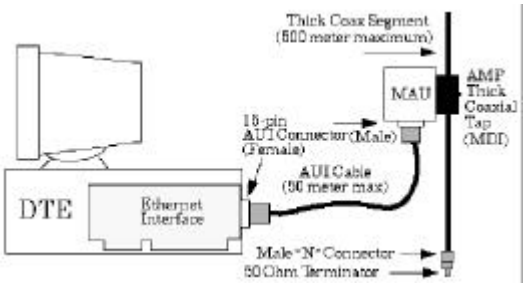


  - **Cada conexão possui dois componentes :**



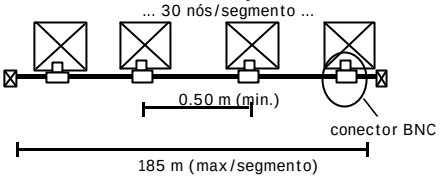
Características Físicas

- **Ethernet "Cabo Grosso" (thick ethernet)**



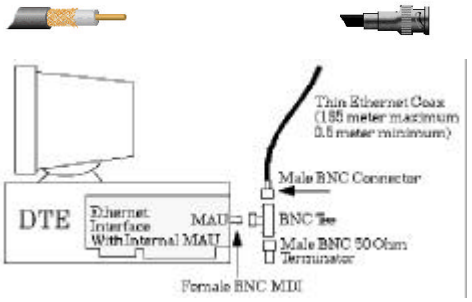
Características Físicas

- **Ethernet "Cabo Fino" (thin ethernet)**
  - Composta por um cabo coaxial RG 58 A/U e comprimento máximo de 185m, com resistores de terminação de 50Ω.



Características Físicas

- **Ethernet "Cabo Fino" (thin ethernet)**

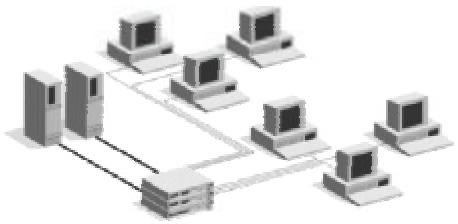


Características Físicas

- **Ethernet "Par Trançado" (twisted pair ethernet)**
  - **Cabeamento Estruturado**
    - UTP - Categoria 5
    - HUB
    - Distância máxima entre estação e hub: 100m
  - **Categorias de par-trançado não aterrado.**
    - Categoria 1 - Linha telefônica (apenas voz)
    - Categoria 2 - até 4 MBps (local talk)
    - Categoria 3 - até 10 MBps (ethernet)
    - Categoria 4 - até 20 MBps (token-ring)
    - Categoria 5 - até 100 MBps (fast ethernet)

Características Físicas

- **Ethernet "Par Trançado" (twisted pair ethernet)**



Variações Ethernet

- **Cabo: Coaxial**
  - Cabo Grasso: Thick Ethernet - 10Base-5
  - Cabo Fino: Thin Ethernet - 10Base-2
- **Par-trançado**
  - Twisted Pair Ethernet - 10Base-T
- **Fibra-ótica**
  - Fiber Optic Ethernet - 10Base-FL
- **FAST-ETHERNET**
  - 100Base-TX
  - 100Base-FX
  - 100baseT4

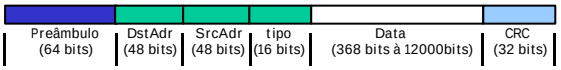
Variações Ethernet

Name	Cable	Max. segment	Nodes/seg.	Advantages
10Base5	Thick coax	500 m	100	Good for backbones
10Base2	Thin coax	200 m	30	Cheapest system
10Base-T	Twisted pair	100 m	1024	Easy maintenance
10Base-F	Fiber optics	2000 m	1024	Best between buildings

Tecnologias de Alta Velocidade

- FDDI – Token Ring a 100 Mbps
- Fast Ethernet
- ATM (sobre SONET - Synchronous Optical Networking Protocol)
- Gigabit Ethernet

Formato de um quadro Ethernet



Preâmbulo: sequência de 1 e 0 alternados (sincronização nível bit e quadro)
DstAdr: endereço ethernet do dispositivo destino
SrcAdr: endereço ethernet do dispositivo fonte
Tipo: identificação do tipo de dados (data) que o quadro possui (interpretação)
Data: informação a ser transmitida
CRC: detecção de erros (Cyclic Redundancy Check)

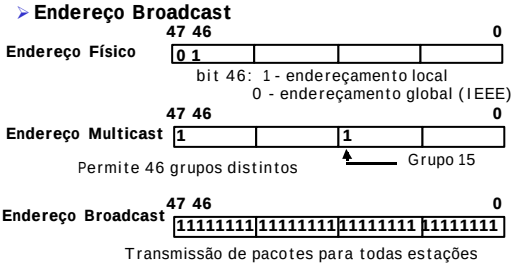
Endereçamento Ethernet

- Endereço Ethernet
  - Já que todos transceivers em uma rede ethernet "escutam" o barramento, é necessário criar mecanismos que permitam detectar qual transmissão pertence a uma determinada estação.
  - Cada estação (interface) conectado na ethernet é identificado por um número inteiro representado em 48 bits -> ENDEREÇO ETHERNET
  - Endereços Ethernet são UNICOS no mundo inteiro. O gerenciamento é feito pela IEEE (Institut for Electrical and Eletronic Enginners)

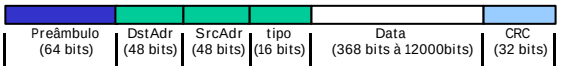
Endereço Ethernet = Endereço Hardware = Endereço Físico

Endereçamento Ethernet

- Interpretação do Endereço Ethernet
  - Endereço Físico
  - Endereço Multicast
  - Endereço Broadcast



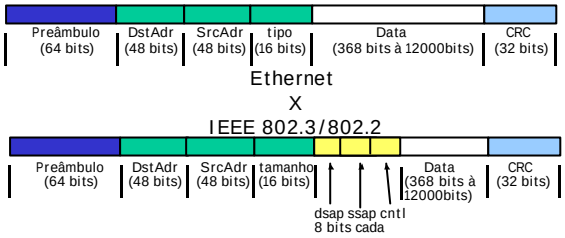
Formato de um quadro Ethernet



Preâmbulo: sequência de 1 e 0 alternados (sincronização nível bit e quadro)
DstAdr: endereço ethernet do dispositivo destino
SrcAdr: endereço ethernet do dispositivo fonte
Tipo: identificação do tipo de dados (data) que o quadro possui (interpretação)
Data: informação a ser transmitida
CRC: detecção de erros (Cyclic Redundancy Check)

Diferença entre Ethernet e IEEE 802.3/802.2

- No cabeçalho IEEE 802.3 o campo "tipo" é substituído pelo campo "tamanho".
- Existe ainda um cabeçalho 802.2



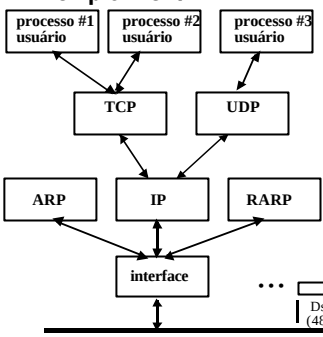
Ethernet

X

IEEE 802.3/802.2

Exemplo de Protocolo

- Exemplo TCP/IP



Função do campo "Tipo": Utilizado para determinar qual protocolo de software deve ser usado. Permite o uso de mais de um protocolo em um mesmo meio físico.

Campo Tipo identifica ARP ou RARP ou IP
0x0806 0x0800

Bridges

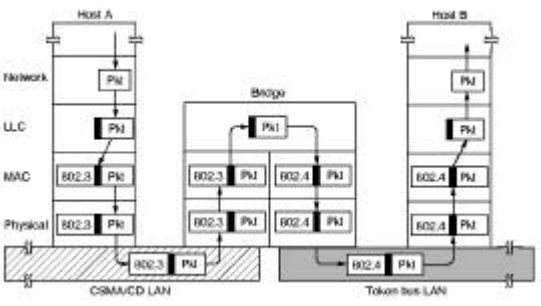
- **FUNÇÃO**
  - A principal função da Bridge é interconectar Sub-redes que apresentam ou não compatibilidade em relação a camada de Enlace.
    - **Interligando dois segmentos de rede Ethernet através de pontes vai diminuir o número de colisões da rede, diminuindo a carga total da rede e melhorando o desempenho das aplicações.**
    - **Interligando uma rede Ethernet a uma rede Token-Ring podemos construir redes locais corporativas, estendendo o domínio geográfico da rede.**

Bridges

- **Caracteristicas**
  - As Bridges possuem uma certa inteligência (baseada em microprocessador), armazenando o quadro e transmitindo para o outro segmento somente se o quadro for destinado a ele, e ignorando-o caso seja destinado ao mesmo segmento.
  - Do ponto de vista do usuário Final, as Bridges são transparentes, o usuário não necessita saber que ela existe.
  - A Bridge é vista como um equipamento "observador", nas redes, monitorando todo o pacote que circula em cada uma das redes à qual ela está associada.

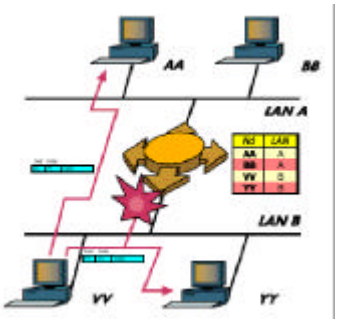
Bridges

- **Caracteristicas**



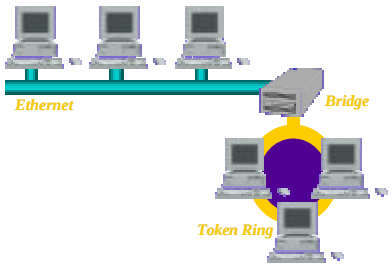
Bridges

- **Caracteristicas**



Bridges

- **Caracteristicas**

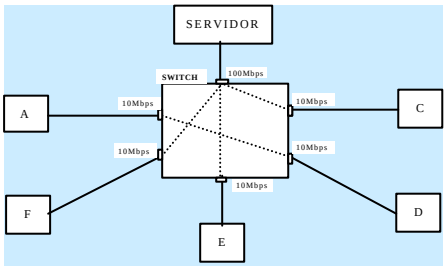


Switches

- **Função**
  - **A principal função dos Switches é eliminar as colisões, provocando aumento de desempenho da rede**
    - Os switches formam tabelas dinâmicas que mapeiam o posicionamento das estações da rede, em cada segmento. A partir dessas tabelas, os switches permitem criar caminhos virtuais entre dois ou mais segmentos de rede, de uma forma ágil e rápida.
    - Os switches são equipamentos que trabalham no nível 2 (Enlace) do modelo OSI, e permitem a interconexão entre máquinas diretamente, ou seja, simulando uma conexão ponto a ponto.

Switches

- **Características**



Exercícios

- Qual a conseqüência das colisões nas redes locais Ethernet?
- No interior do quadro de informações de dados das redes locais, existem dois campos: o endereço destino e o endereço fonte. Para que servem estes campos**?**
- Se a sua rede Ethernet está muito carregada (alta taxa de tráfego), o que pode acontecer? Como detectar esta situação? Como solucionar este problema?

E PARA ACESSAR A INTERNET ATRAVÉS DE PROVEDORES DE ACESSO?

PROTOCOLOS DE ENLACE PARA LINHAS SERIAIS

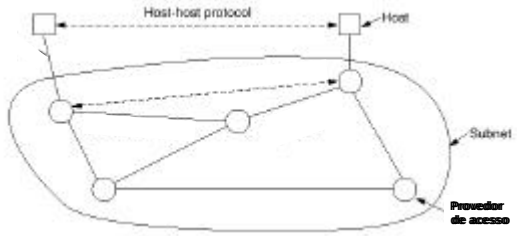
SLIP E PPP

Introdução

- **Provedor de Acesso:**
  - Empresa que através de um roteador conectado a rede Internet, disponibiliza o acesso de terceiros à Internet através de um **roteador**, mediante uma espécie de serviço de assinatura, que dá direito ao assinante a uma determinada quota de horas de acesso mensal.

Introdução

- **Acesso Host - Provedor de Acesso:**



Introdução

- **Provedor de Acesso:**
  - A conexão do usuário ao provedor é feita, tipicamente, através da rede telefônica discada e um modem padrão de canal de voz.
  - No enlace formado, entre o usuário e o provedor, deverá atuar um protocolo de nível de enlace, que deverá providenciar serviços como segmentação em quadros e seqüenciação, controle de erro e outras funções típicas do nível de enlace.
  - Dois protocolos em particular se tornaram muito populares entre os usuários de Internet: o SLIP e o PPP.

O Protocolo SLIP

- **Protocolo SLIP (Serial Line Interface Protocol):**
  - Desenvolvido por Rick Adams em 1984.
  - É o protocolo mais antigo e o mais simples, é descrito através RFC 1055. Algumas melhorias foram introduzidas mais tarde, que são descritas na RFC 1144.
  - O funcionamento básico do protocolo consiste em adicionar um flag aos próprios pacotes IP para configurá-los como um quadro.
  - A transparência do quadro é assegurada através de uma técnica de *caracter stuffing*, que funciona de forma semelhante ao *bit stuffing*.

O Protocolo SLIP

- **Protocolo SLIP (Serial Line Interface Protocol):**
  - **Está em desuso por possuir sérios problemas:**
    - O protocolo não implementa nenhum mecanismo de detecção e correção de erros.
    - O SLIP suporta somente IP.
    - Cada uma das pontas do enlace precisa saber antecipadamente o endereço IP um do outro.
    - SLIP não possui qualquer mecanismo de autenticação, ou seja, nenhum dos participantes sabe com quem esta falando.
    - SLIP é um protocolo sem aprovação do IETF.
  - **IETF definiu um novo protocolo de enlace: O PPP.**

O Protocolo PPP

- **Protocolo PPP (Point-to-Point Protocol):**
  - Desenvolvido por um grupo de pesquisadores, especialmente convocados pelo IETF.
  - Características especificadas na RFC 1661 posteriormente completadas através das RFC 1662 e 1663.
  - Suporta protocolos múltiplos, faz detecção e correção de erros, permite negociação de endereços de IP, faz autenticação.
  - O protocolo pode ser utilizado em linha privativa ou comutada em conexões usuário-roteador ou roteador-roteador.

O Protocolo PPP

- **Protocolo PPP (Point-to-Point Protocol):**
  - Método de delimitação dos quadros que de forma não ambígua sinaliza o começo e o fim de um quadro.
  - Engloba um protocolo de controle do enlace que executa entre outras funções de estabelecimento da conexão, permite negociação de opções (compactação do cabeçalho, por exemplo) além de funções de teste e supervisão. O protocolo é chamado de LCP (Link Control Protocol).

O Protocolo PPP

- **Protocolo PPP (Point-to-Point Protocol):**
  - PPP engloba um mecanismo que permite negociação de opções do nível de rede (o endereço IP, por exemplo), independente do protocolo de rede. O método utilizado para implementar esta função foi o de ter um NCP (Network Control Protocol) distinto, para cada tipo de protocolo de rede suportado.

O Protocolo PPP

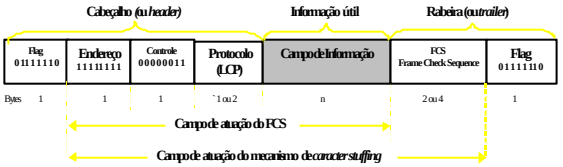
- **Protocolo PPP (Point-to-Point Protocol):**
  - 1.O PC chama o roteador do provedor via modem.
  - 2.Depois do modem estabelecer conexão física, o PC enviará uma série de pacotes LCP para negociar os parâmetros PPP a serem usados.
  - 3.Pacotes NCP serão trocados para configurar a camada de rede - atribui dinamicamente um endereço IP.
  - 4.Neste momento o PC passa a ser um Host Internet.

O Protocolo PPP

- **Protocolo PPP (Point-to-Point Protocol):**
  - 5.Ao final da transmissão o NCP é usado para liberar a conexão da rede.
  - 6.E o LPC é usado para liberar a conexão de enlace.
  - 7.Finalmente, o computador solicitará que o modem desligue o telefone, liberando a conexão física da camada.

O Protocolo PPP

- **Protocolo PPP (Point-to-Point Protocol):**



PARTE 3

O CONJUNTO DE PROTOCOLOS TCP/IP

O que vamos ver?

- **Introdução**
- **Endereçamento IP**
- **Sub-redes**
- **Protocolo IP**
- **Protocolos de Roteamento**
- **Protocolo ARP**

O que vamos ver?

- **Protocolo ICMP**
- **Protocolo TCP**
- **Protocolo UDP**

Introdução

- O que tem a ver TCP/IP com Internet?
- Enquanto os usuários esperavam o surgimento de produtos conformantes com os protocolos OSI/ISO, o conjunto de protocolos TCP/IP se tornou um padrão "de-facto" para interconexão de sistemas computacionais.
- Disponível quase que de forma padrão em máquinas UNIX, Computadores Pessoais, Mainframes, Supercomputadores, etc.
- Protocolos abertos e disponíveis.

Histórico

- Há aproximadamente 40 anos atrás, a RAND Corporation, uma das maiores empresas americanas envolvidas em estratégias para a Guerra Fria, se deparou com um estranho problema estratégico:
  - **Como as autoridades governamentais americanas poderiam continuar se comunicando após uma guerra nuclear?**

Histórico

- Não importa quão blindada ou protegida a rede fosse, seus comutadores e seu cabeamento sempre seriam vulneráveis ao impacto de bombas atômicas. Um ataque nuclear reduziria a sucata qualquer rede conhecida na época.
- Além disso, havia a questão de como a própria rede poderia ser comandada e controlada? Qualquer autoridade central, qualquer quartel general central seria um alvo óbvio e imediato para um míssil inimigo. O centro da rede seria o primeiro lugar a ser destruído.

Histórico

- A proposta da RAND:
- O princípio era simples. Se assumiria que a rede é não-confiável todo o tempo. Ela seria projetada tendo em mente a idéia de "receber-passar-adiante" de modo a transcender sua própria não-confiabilidade.
- Cada nó da rede seria igual em termos de status e função a todos os outros nós da rede.

Histórico

- As mensagens por sua vez seriam divididas em pacotes, cada pacote endereçado separadamente.
- Cada pacote começaria de um nó de origem e terminaria no nó destino final especificado.
- Cada pacote "viajaria" pela rede em uma base individual. A rota seguida por cada pacote através da rede não teria importância. Apenas os resultados finais teriam importância.

Histórico

- Em 1968 a Agência de Pesquisas e Projetos Avançados do Pentágono (ARPA) decidiu fundar um projeto baseado na proposta da RAND
- . Os nós da rede seriam supercomputadores muito rápidos. Eles eram máquinas extremamente raras e valiosas na época, e que apresentavam uma real necessidade de interconexão através de uma rede sólida e confiável, de modo a contribuir para os projetos nacionais de pesquisa e desenvolvimento.

Histórico

- Em dezembro de 1969 já existiam quatro nós nesta rede incipiente, que foi chamada de ARPANET.
- Os quatro computadores podiam transferir dados através de linhas de alta-velocidade dedicadas. Eles poderiam até mesmo ser programados remotamente pelos outros nós. Graças a ARPANET, cientistas e pesquisadores puderam compartilhar entre si recursos computacionais através de longas distâncias.

Histórico

- Já no segundo ano de operação da ARPANET, uma fato singular se tornou claro. Os usuários haviam transformado a rede para compartilhamento de recursos computacionais em um escritório de correios subsidiado pelo governo federal. O tráfego principal da ARPANET não era de submissão remota de processos, mas sim mensagens pessoais e de novidades. Os pesquisadores estavam utilizando a ARPANET para colaborar em projetos, para trocar comentários e até mesmo para difundir piadas e outros assuntos. O serviço de correio eletrônico oferecido era um sucesso.

Histórico

- Durante os anos 70, a ARPANET cresceu. Sua estrutura descentralizada tornava a expansão muito fácil. Ao contrário das redes de computadores corporativas, a ARPANET podia acomodar muitos tipos de máquinas. Uma vez que máquinas individuais pudessem falar segundo o protocolo estabelecido para esta rede nova e anárquica, suas marcas, seus conteúdos e mesmo quem eram seus donos, era irrelevante.

Histórico

- A medida que se passava a década de 80, muitos grupos sociais aderiram a esta rede. Era extremamente fácil ligar computadores à crescente rede-de-redes.
- A medida que a utilização do TCP/IP se tornou mais comum, redes inteiras se sentiram atraídas para esta interconexão, e desorganizadamente aderiam.

Histórico

- Uma vez que o software chamado TCP/IP era de domínio público, e a tecnologia básica era descentralizada e até mesmo anárquica por natureza, era difícil impedir as pessoas de se conectarem em um lugar ou outro desta super-rede.
- O ponto é que na verdade ninguém queria impedir as pessoas de se conectarem a este emaranhado complexo de redes, que acabou se tornando conhecido como Internet.

Histórico

- A ARPANET foi formalmente extinta em 1989.
- O uso dos padrões TCP/IP em computadores é hoje um fenômeno global, em apenas trinta anos, se passou de uma rede de apenas quatro computadores para milhões de nós pelos cinco continentes.
- A Internet é provavelmente o instrumento científico mais importante do final do século XX. O acesso poderoso e sofisticado que ela possibilita a dados especializados e troca de informações entre pesquisadores, acelerou enormemente a velocidade das pesquisas científicas em todo o mundo.

Histórico

- O ritmo de crescimento da Internet na década de 90 é espetacular. Poderia se dizer até mesmo "feroz". Ela está se espalhando mais rápido que os telefones celulares e as máquinas de fax. Em 1992 a Internet cresceu a uma taxa de 20% ao mês.
- A Internet é também uma pechincha. A Internet como um todo, ao contrário do sistema telefônico, não cobra por chamadas de longa-distância. E, ao contrário das grandes redes comerciais de computadores, ela não cobra por tempo de acesso.
- Cada grupo ou pessoa que acessa a Internet é responsável por sua própria máquina e seção de linha.

Introdução

- **Protocolo TCP/IP**
  - Protocolo: conjunto de regras que determinam como software e hardware de uma rede devem interagir para transmitir informações.
  - TCP/IP representa uma família de protocolos (protocol suite) centrado no protocolo IP (Internet Protocol)

Introdução

- **Protocolo TCP/IP**

TCP: Transmission Control Protocol

UDP: User Datagram Protocol

ARP: Address Resolution Protocol

RARP: Reverse Address Resolution Protocol

ICMP: Internet Control Message Protocol

IP: Internet Protocol

Família é denominada TCP/IP

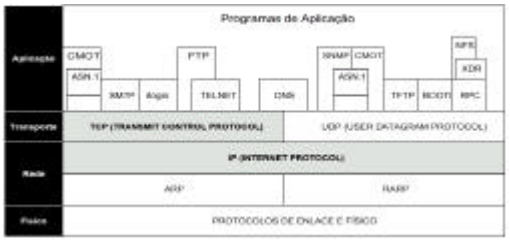
Introdução

- **Modelo Conceitual**

SERVIÇOS DE APLICAÇÃO	Correio Eletrônico, Transferência de Arquivos, Emulação de Terminais, etc...
SERVIÇOS DE TRANSPORTE CONFIÁVEL	Controle de erros, seqüenciamento, duplicação, fluxo.
SERVIÇOS DE REDE NÃO-ORIENTADOS À CONEXÃO	Roteamento de Pacotes, espaço de endereçamento único, não possui segurança da entrega

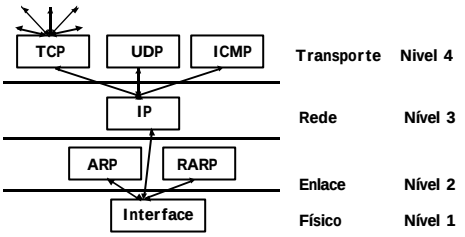
Introdução

- **Correspondência com os Níveis do Modelo de Referência OSI da ISO**



Introdução

- **Tratamento das Mensagens que Chegam ou Saem de uma Estação**



Introdução

- **Onde obter informações sobre os protocolos que compõem o TCP/IP?**
  - Estas informações podem ser obtidas nas RFCs (Request For Comments).
  - As RFCs são os documentos básicos que representam todos os trabalhos internos relacionados com a Internet.
  - É através destes documentos que se divulgam novos protocolos.
  - Assim, a Internet atua como um gigantesco tubo de ensaio para aprimoramento dos protocolos TCP/IP.

RFCs - Request For Comments

- **Onde Obter**
  - Esses documentos estão em constante desenvolvimento, e podem ser obtidos via FTP ou http nos seguintes locais:
  - http://www.cis.ohio-state.edu/htbin/rfc/INDEX.rfc.html
  - http://www.unicamp.br/pub/RFC
  - http://nis.nsf.net
  - http://venera.isi.edu
  - http://wuarchive.wustl.edu

RFCs - Request For Comments

- **Algumas importantes**
  - Algumas RFCs relevantes para o estudo de redes estão listadas a seguir, mas é importante acessar o índice das RFCs a fim de ver a lista completa.
    - **768 User Datagram Protocol (UDP)**
    - **791 Internet Protocol (IP)**
    - **792 Internet Control Message Protocol (ICMP)**
    - **793 Transmission Control Protocol (TCP)**
    - **826 Address Resolution Protocol (ARP)**
    - **854 Telnet Protocol (TELNET)**
    - **862 Echo Protocol (ECHO)**
    - **894 IP over Ethernet**

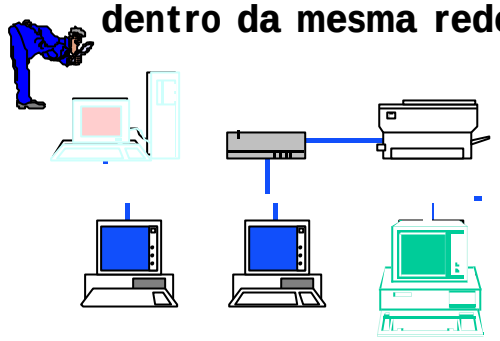
RFCs - Request For Comments

- **Algumas importantes**
  - **950 Internet Standard Subnetting Procedure**
  - **959 File Transfer Protocol (FTP)**
  - **1001, 1002 NetBIOS Service Protocols**
  - **1009 Requirements for Internet Gateways**
  - **1034, 1035 Domain Name System (DNS)**
  - **1112 Internet Gateway Multicast Protocol (IGMP)**
  - **1157 Simple Network Management Protocol (SNMP)**
  - **1518 An Architecture for IP Address Allocation with CIDR**
  - **1519 Classless Inter-Domain Routing (CIDR): An Address Assignment and Aggregation Strategy**
  - **1541 Dynamic Host Configuration Protocol (DHCP)**

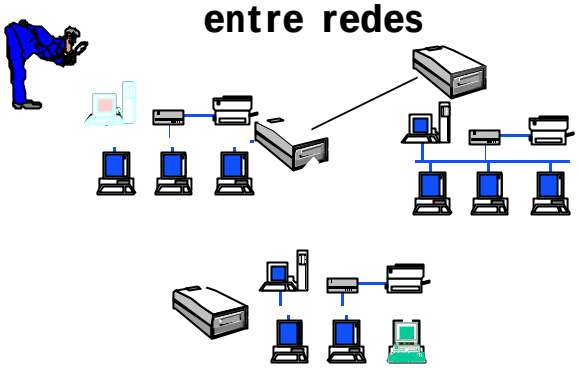
Nível de Rede

- **Função dos Roteadores**
  - Roteador é um equipamento responsável pela interligação entre redes atuando nas camadas 1,2 e 3 do modelo ISO/OSI. Permitindo que máquinas de uma dada rede comuniquem-se com máquinas de outra rede remota, como se as redes fossem uma só.

Pacotes que trafegam dentro da mesma rede



Pacotes que trafegam entre redes



Nível de Rede

- **O PROTOCOLO IP (Internet Protocol)**
  - A principal função do protocolo IP é o roteamento das mensagens a serem transmitidas pela rede.
  - O roteamento é baseado em um endereço único para cada máquina chamado **ENDEREÇO INTERNET ou ENDEREÇO IP**.
  - Provê um sistema de comunicação **não confiável e não orientado a conexões**.
  - O protocolo IP não oferece qualquer garantia de que o datagrama chegou sem erros à máquina destino.

Endereçamento IP

- Uma rede TCP/IP gerencia pacotes de acordo com o endereço IP que existe na mensagem.
- Pacotes:
  - trafegam dentro de uma mesma rede
  - trafegam de uma rede local a outra (routing)
- Para utilizar apropriadamente uma rede TCP/IP é necessário um endereço IP.

Nível de Rede

- **Endereçamento IP**
  - **Endereço IP é composto pelas seguintes informações:**
    - **endereço de rede** (atribuído pelo Administrador do Domínio da Raiz - no Brasil a FAPESP)
    - **endereço de sub-rede** (atribuído pelo administrador local)
    - **endereço (número) do host** (atribuído pelo administrador local)
  - O Endereço IP é como se fosse o endereço postal de uma pessoa, cujas informações são o nome da rua e o nome da pessoa.

Nível de Rede

- **Endereço IP**
  - O Endereço IP é composto por 32 bits divididos em 4 camps de 8 bits.
  - Cada campo é denominado de octeto e representado por um número decimal separado por um ponto.
  - Cada octeto pode conter valores de 0 a 255.
    - Exemplo:

      129.144.50.56

Pausa para um pouco de matemática

- **Sistema de numeração**
  - **Base 10: é a base que estamos acostumados**
    - 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, etc.
  - **Base 2: é a base de numeração utilizada nos computadores**
    - 1 bit: binary digit (dígito binário) - 0 ou 1
    - 0, 1, 10, 11, 100, 101, 110, 111, 1000, etc.
    - 1 byte ou 1 octeto: coleção de 8 bits.

Pausa para um pouco de matemática

- **Sistema de numeração**
  - **Base 16 - Hexa: é a base que utilizamos para "ler" um byte que esteja representado em binário.**
    - 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F.

Sistemas de Numeração

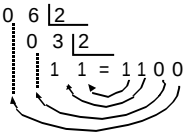
- **Conversão de Binário para Decimal**
  - Cada bit é multiplicado por 2 elevado na potência dada pela posição do bit dentro do numero (começando pela posição 0, da direita para a esquerda).
  - O resultado em decimal é a soma destes valores.
  - **Exemplo:**
    - **1010** = $1*2^3+0*2^2+1*2^1+0*2^0$ = $1*8+0*4+1*2+0*1 = 8+2 =$ **10**
    - **10011100** = $1*2^7+0*2^6+0*2^5+1*2^4+1*2^3+1*2^2+0*2^1+0*2^0 = 128+16+8+4 =$ **156**

Sistemas de Numeração

- **Conversão de Binário para Decimal**
  - $2^0 = 1$
  - $2^1 = 2$
  - $2^2 = 4$
  - $2^3 = 8$
  - $2^4 = 16$
  - $2^5 = 32$
  - $2^6 = 64$
  - $2^7 = 128$
  - $2^8 = 256$
  - $2^9 = 512$
  - $2^{10} = 1024$

Sistemas de Numeração

- **Conversão de Decimal para Binário**
  - O processo consiste em dividir recursivamente o número em decimal por 2, até que o número resultante seja igual a 1 ou 0. A partir daí o número em binário correspondente é obtido pelos restos obtidos durante o processo de divisão.
  - Exemplo:
  - 12 |2
    0 6 |2
    0 3 |2
    1 1 = 1 1 0 0



Sistemas de Numeração

- **Conversão de Binário para Hexa**
  - O processo consiste em dividir o byte em duas partes de 4 bits chamadas de "nibbles". A partir daí transformamos o nibble em seu correspondente hexadecimal.

0000 = 0 0001 = 1 0010 = 2 0011 = 3
0100 = 4 0101 = 5 0110 = 6 0111 = 7
1000 = 8 1001 = 9 1010 = A 1011 = B
1100 = C 1101 = D 1110 = E 1111 = F

  - Exemplo:
  - 10011100 = 1001 1100 = 9C

Álgebra Booleana

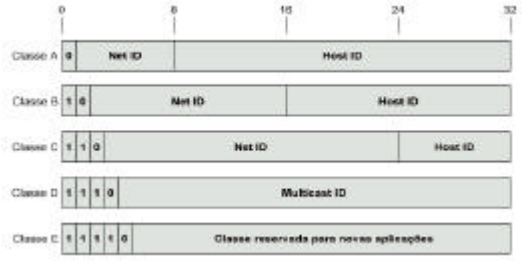
- **Operadores Lógicos e Números Binários**
  - E (AND) Lógico
    - 0 .AND. 0 = 0
    - 0 .AND. 1 = 0
    - 1 .AND. 0 = 0
    - 1 .AND. 1 = 1
  - OU (OR) Lógico
    - 0 .OR. 0 = 0
    - 0 .OR. 1 = 1
    - 1 .OR. 0 = 1
    - 1 .OR. 1 = 1
  - NÃO (NOT) Lógico
    - .NOT. 0 = 1
    - .NOT. 1 = 0
  - OU-EXCLUSIVO (XOR)
    - 0 .XOR. 0 = 0
    - 0 .XOR. 1 = 1
    - 1 .XOR. 0 = 1
    - 1 .XOR. 1 = 0

Endereçamento IP

- **Classes de Endereçamento IP**
  - O Endereçamento IP é dividido em 5 classes: A, B, C, D e E.
  - As máquinas conectadas à Internet vão possuir endereços correspondentes a uma das três primeiras classes de endereços.

Endereçamento IP

- **Classes de Endereçamento IP**



Endereçamento IP

- **Classes de Endereçamento IP**
  - **Classe A:**
    - Identificada pelo primeiro bit colocado a 0. Valor do primeiro octeto contido na faixa entre 0 e 127.
    - Possui um campo Net ID de 7 bits.
    - Podem existir no máximo 128 redes classe A.
    - Cada rede pode endereçar até 2^{24} (16 M) hosts.
    - Destinada a redes com grande números de estações.
    - Exemplo: MIT - endereço de rede=18

Endereçamento IP

- **Classes de Endereçamento IP**
  - **Classe B:**
    - Identificada pelos dois primeiros bits do endereço colocados em 1 e 0 respectivamente. Valor do primeiro octeto contido na faixa entre 128 e 191.
    - Possui um campo Net ID de 14 bits.
    - Podem existir no máximo 16384 redes classe B.
    - Cada rede pode endereçar até 2^{16} (64 K) hosts.
    - Destinada a redes consideradas de médio porte.
    - Exemplo: UFSC - endereço de rede=150.162

Endereçamento IP

- **Classes de Endereçamento IP**
  - **Classe C:**
    - Identificada pelos três primeiros bits do endereço colocados em 1, 1 e 0 respectivamente. Possui um campo Net ID de 21 bits. Valor do primeiro octeto contido na faixa entre 192 e 223.
    - Podem existir no máximo 2.097.152 redes classe C.
    - Cada rede pode endereçar até 2^{8}-2 (254) hosts.

Endereçamento IP

- **Classes de Endereçamento IP**
  - **Classe C:**
    - Os endereços de Host ID = 00000000 e 11111111 são destinados a broadcasting.
    - Destinada a redes consideradas de pequeno porte.
    - Exemplo: portadigital - endereço de rede=200.237.249

Endereçamento IP

- **Obtendo um Endereço IP**
  - **Solicitar ao administrador do domínio superior.**
    - No caso do Brasil, este administrador é a FAPESP.
    - Preencher um formulário padrão informando a identificação da instituição e qual a classe de rede desejada..

Endereçamento IP

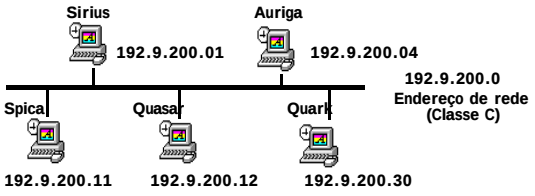
- **Criando Endereços IP para sua Rede**
  - O endereço de rede deve obrigatoriamente ser atribuído pelo administrador do domínio superior.
  - A número do host é atribuído pelo valor dos octetos restantes, e deve ser ÚNICO.
  - Exemplo:
    - Endereço classe A - 3 octetos para *host*
    - Endereço classe B - 2 octetos para *host*
    - Endereço classe C - 1 octeto para *host*
  - Cada octeto do endereço IP pode receber valores de 0 a 255, com a restrição que os octetos correspondentes ao número do host não seja com todos os bits em zero ou em um.

Endereçamento IP

- **Criando Endereços IP para sua Rede**
  - O endereço IP 127.x.y.z é um endereço reservado utilizado para loop-back local e auto-diagnóstico.
  - O endereço IP de uma rede e de um host não pode ter todos os bits em 1 (255).
    - **Todos os bits em 1 é interpretado como broadcast.**
  - O endereço IP de uma rede e de um host não pode ter todos os bits em 0.
    - **Todos os bits em 0 é interpretado como "esta rede".**

Endereçamento IP

- **Exemplo**



Exercício

- Coloque os seguintes números em binário, dizendo a que classe de rede eles pertencem:

a) 9.3.158.1_____
b) 100.8.5.4_____
c)143.54.8.11_____
d)200.248.3.1_____
e) 224.8.1.8_____
f) 247.5.4.3_____

Quem gerencia a numeração IP?

- IANA - Internet Assigned Numbers Authority (http://www.iana.org). Órgão encarregado de entregar endereços IP aos países do mundo. Designa um representante em cada país. No Brasil, é a FAPESP (Federação de Auxílio a Pesquisa do Estado de São Paulo - http://www.fapesp.br).
- Internic - www.internic.net
- Recentemente foram criados novos domínios, como .nom, .firm, e assim por diante. Esses novos "generic top levels domains" podem ser vistos na recomendação final do IAHD (International Ad Hoc Commitee), no endereço http://www.iahc.org/draft-iahc-recommend-00.html

Endereçamento IP

- **Resumo**
  - **Classe A:**
    - Computadores em uma rede classe A tem endereços da forma *N.a.b.c*, onde *N* é o número da rede e *a.b.c* o número do computador.
    - O bit mais significativo de N deve ser zero.
    - Isto permite a existência de 127 redes classe A, cada uma podendo conter 16.777.216 computadores. Naturalmente, tais redes não são práticas. Mesmo assim, muitas das instituições pioneiras na Internet possuem redes classe A.

Endereçamento IP

- **Resumo**
  - **Classe B:**
    - Os endereços são da forma *N.M.b.c*, onde *N.M* é o número da rede e *a.b* o número do computador
    - Os dois bits mais significativos de N devem ser 10.
    - Redes classe B são encontradas em grandes universidades e organizações comerciais de grande porte.

Endereçamento IP

- **Resumo**
  - **Classe C:**
    - Os endereços tem a forma *N.M,O.a*, sendo *N.M.O* o número da rede e *a* o número do computador.
    - Os três bits mais significativos de N devem ser 110.
    - Isto permite a existência de 254 computadores neste tipo de rede (os números 0 e 255 são reservados).

Endereçamento IP

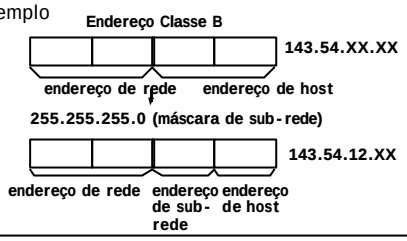
- **Resumo**
  - **Classe D:**
    - Os endereços tem a forma *N.M,O.a*, onde os quatro bits mais significativos de N devem ser 1110. Estes endereços não são de redes, mas sim de grupos de *multicast*.
  - **Classe E:**
    - Os endereços tem a forma *N.M.O.P*, sendo os quatro bits mais significativos de N iguais a 1111. Estes endereços são reservados para uso experimental.

SUB-REDES

- **Criando Sub-Redes**
  - Sub-redes são divisões lógicas e físicas de uma rede TCP/IP.
  - Em uma rede Classe B, não seria viável conectar todos os 65.000 hosts na mesma rede.
  - Pode-se então dividir os 16 bits de endereçamento de host em 8 bits para sub-rede e 8 bits para hosts em cada sub-rede.
  - **Esta divisão é transparente para todas as máquinas externas à sua rede.**
  - O roteamento dentro da rede é baseado em pares rede#,sub-rede#.

Endereçamento IP

- **Criando Sub-Redes**
  - O número de bits dentro de um endereço IP destinado ao número do host, mas utilizados para determinar a rede é determinado por uma **MÁSCARA DE SUB-REDE** (network mask).
  - Exemplo

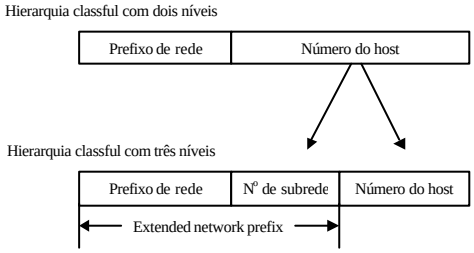


Endereçamento IP

- **Criando Sub-Redes**
  - RFC 950 (1985): definição de um processo padrão para dividir uma classe A, B ou C em pedaços menores, utilizando subredes.
  - Melhorias: Diminui tabelas de roteamento na Internet; administradores podem ter autonomia na criação desubredes internas à empresa (antes necessitavam requisitar outro número de rede).

Endereçamento IP

- **Criando Sub-Redes**



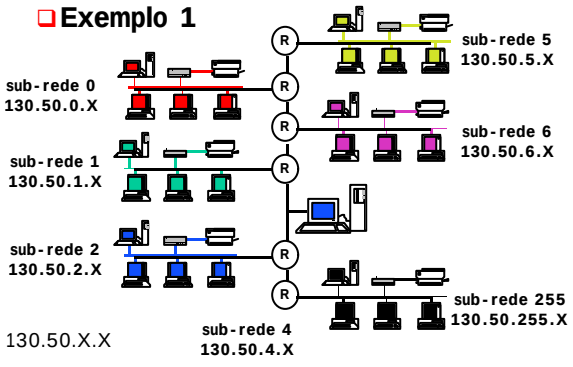
Endereçamento IP

- **Criando Sub-Redes**
  - O "extended network prefix" é identificado pela máscara desubrede, e forma a nova notação de endereçamento utilizado atualmente, o "/x". Por exemplo, um classe A tradicional é um /8. Um classe B é um /16 e um classe C é um /24.
  - Por exemplo, um endereço de rede 143.54.8.11 com máscara 255.255.255.0 pode ser expresso como 143.54.8.11/24. Isso facilita o entendimento, como mostra a tabela a seguir.

143.54.8.11	10001111.00110110.00001000.00001011
255.255.255.0	11111111.11111111.11111111.00000000
143.54.8.11/24	10001111.00110110.00001000.00001011

Endereçamento IP

- **Exemplo 1**



Endereçamento IP

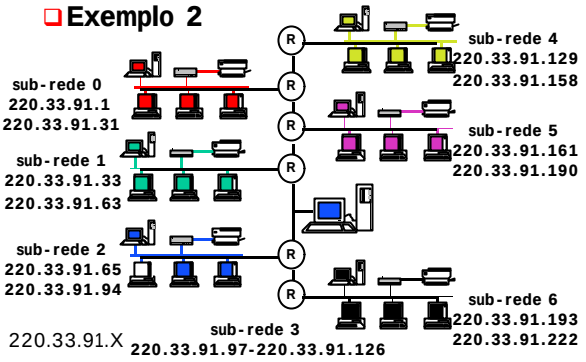
- **Exemplo 1**
  - Supondo uma rede classe B (130.50) com 256 sub-redes (máscara de sub-rede 255.255.255.0 ou em binário 11111111. 11111111. 11111111. 00000000).
  - Vamos supor que o roteador da sub-rede 5 recebe um pacote com o seguinte endereço:130.50.19.16 ou em binário 10000010. 00110010. 00010011. 00010000

Endereçamento IP

- **Exemplo 1**
  - fazendo o E Lógico (.AND.) com a máscara, 11111111. 11111111. 11111111. 00000000
    - resulta, 10000010. 00110010. 00010011. 00000000
    - que corresponde a : 130.50.19.0 Este endereço é procurado na tabela que indicará como chegar à sub-rede 19.

Endereçamento IP

- **Exemplo 2**



Endereçamento IP

- **Exemplo 2**
  - Supondo uma rede classe C (220.33.91) com 8 sub-redes (máscara de sub-rede 255.255.255.224 ou em binário 11111111. 11111111. 11111111. 11111100).
  - Vamos supor que o roteador da sub-rede 5 recebe um pacote com o seguinte endereço:220.33.91.102 ou em binário 11011100. 00100001. 01011011. 01100110

Endereçamento IP

- **Exemplo 2**
  - fazendo o E Lógico (.AND.) com a máscara, 11111111. 11111111. 11111111. 11100000
    - resulta, 11011100. 00100001. 01011011. 01100000
    - que corresponde a : 220.33.91.96. Este endereço é procurado na tabela que indicará como chegar à sub-rede 3.

Endereçamento VLSM e CIDR

- **VLSM (Variable Lenght Subnet Mask)**
  - VLSM: RFC 1009 (1987) e RFC 1716
  - Podendo dividir a rede em sub-redes de tamanho variável permite uma melhor utilização do espaço de endereços destinados à empresa.
  - Antes a empresa tinha que ficar com um número fixo de sub-redes de tamanho fixo.
  - Com VLSM, é possível ter redes com grande número dehosts e também com pequeno número de hosts.

Endereçamento VLSM e CIDR

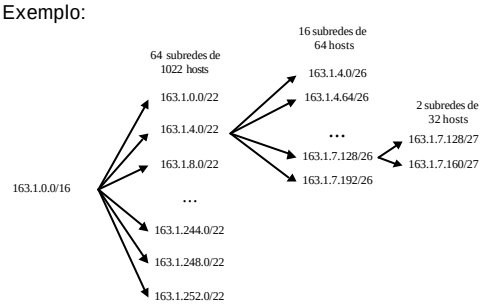
- **VLSM (Variable Lenght Subnet Mask)**
  - Exemplo:
    - Suponha que uma empresa razoavelmente grande tenha um classe B cheio (163.1.0.0/16), permitindo até 65.534 hosts.
    - Entretanto, essa empresa precisa de algumas sub-redes com aproximadamente 1.000 máquinas, e outras em setores com aproximadamente 30 máquinas.

Endereçamento VLSM e CIDR

- **VLSM (Variable Lenght Subnet Mask)**
  - Exemplo:
    - Se dividir igualmente o espaço de endereçamento (um /22), terá somente 64 subredes de 1022 hosts, o que provocará um desperdício em setores pequenos (aproximadamente 1.000 endereços desperdiçados).
    - Qual a solução? VLSM.

Endereçamento VLSM e CIDR

- **VLSM (Variable Lenght Subnet Mask)**
  - Exemplo:



Endereçamento VLSM e CIDR

- **CIDR (Classless InterDomain Routing):**
  - O CIDR é praticamente a mesma coisa que o VLSM, porém, envolve a Internet externa à empresa, a fim de facilitar o roteamento entre domínios.
  - Estes endereços, denominados deClassless InterDomain Routing, utilizam os k bits mais significativos para identificar a rede, e os 32-k bits restantes para identificar o computador. O método CDIR pode ser combinado com o esquema clássico, e foi definido como uma maneira de contornar a crescente falta de endereços IP.

Endereçamento VLSM e CIDR

- **Endereços CIDR:**
  - A idéia básica do plano é alocar um ou mais blocos de rede classe C para cada provedor de serviço da rede. Para toda organização que se conecte à Internet via provedor, são alocados subconjuntos de endereços deste provedor.
  - Hipoteticamente, suponha que um provedor A tenha 2048 redes classe C que começam com 192.24.0.0 e terminam com 192.31.255.0. Seja ainda um cliente C que deseja menos do que 2048 endereços de hosts. Então serão alocados os endereços 192.24.0.0 a 192.24.7.0.

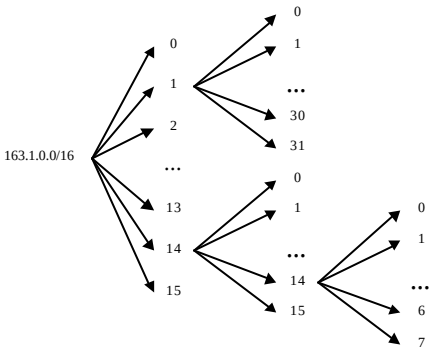
Endereçamento VLSM e CIDR

- **Endereços CIDR:**
  - Esta subalocação hierárquica de endereços implica que clientes com subconjunto de endereços de um provedor terão, obrigatoriamente, sua informação roteada pela infra-estrutura do roteador.

Exercícios

- Para a figura a seguir, definir
  - a) todas as sub-redes envolvidas, com máscaras de sub-rede e extended network prefix para cada uma
  - b) endereçamento de hosts,
  - c) endereço broadcast para as sub-redes 1-1, 3 e 14-14-1.

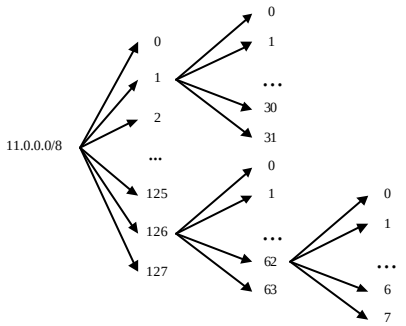
Exercícios



Exercícios

- Para a figura a seguir, definir
  - a) todas as sub-redes envolvidas, com máscaras de sub-rede e extended network prefix para cada uma
  - b) endereçamento de hosts, c)
  - endereço broadcast para as sub-redes 1-1, 3 e 6-14-1.

Exercícios



Endereços IP Reservados

- O seguintes endereços são reservados para redes privadas (Intranets) de modo que nenhuma máquina na INTERNET possuirá estes endereços.

Endereço	Classe de Endereçamento
10	A
128	B
192	C

Range de IPs Livres para Intranet

- 10.0.0.0 até 10.255.255.255 para Classe A
- 128.16.0.0 até 128.31.255.255 para Classe B
- 192.168.0.0 até 192.168.255.255 para Classe C

Exercício

- Uma organização recebeu o número de rede 156.1.1.0, e precisa definir 6 subredes. A maior subrede deve suportar 25 hosts. Defina o seguinte:
  - a) máscara de sub-rede
  - b) número de cada sub-rede
  - c) endereço broadcast de cada sub-rede
  - d) endereços de host para cada sub-rede

Correspondência Número X Nome

- **NÃO EXISTE CORRESPONDÊNCIA ENTRE NOMES E NÚMEROS IP**
- com - instituição comercial ou empresa (ex: apple.com - Apple Computers);
- edu - instituição educacional (ex: berkeley.edu - Universidade de Berkeley);
- gov - órgão do governo (ex: nasa.gov - NASA);
- mil - organização militar (ex: nic.ddn.mil - departamento de defesa dos EUA);
- net - *gateways* e *hosts* administrativos de uma rede (ex: uu.net);
- org - organizações privadas que não se enquadram nas outras categorias (ex: eff.org);

Correspondência Número X Nome

- países - cada país tem duas letras que o caracterizam (ex: br - Brasil, us - EUA, fr - França, de - Alemanha, au – Austrália, e assim por diante). Baseados na norma ISO 3166
  - net.br empresas de telecomunicações
  - g12.br entidades de ensino de primeiro e segundo grau
  - art.br artes: músicas, pintura, folclore, entre outros
  - esp.br clubes, esportes em geral
  - ind.br organizações industriais

Correspondência Número X Nome

- inf.br provedores deinformaçoes (rádios, TVs, Jornais, Revistas, Bibliotecas)
- psi.br provedores de serviço Internet
- rec.br entretenimento, diversão, jogos, etc.
- tmp.br eventos temporários, como feiras e exposições
- etc.br os que não se enquadram nas categorias citadas

O Protocolo IP

- **O Protocolo IP (Internet Protocol)**
  - **Roteamento IP**
    - O roteamento é baseado nos endereços de rede contidos nos endereços Internet.
    - Equipamentos roteadores interligam duas ou mais redes.

O Protocolo IP

- **O Protocolo IP (Internet Protocol)**
  - **Roteamento IP**
    - O roteamento é feito em cima de TABELAS DE ROTEAMENTO.
    - Se não encontrar o roteador na Tabela de Roteamento, manda para o DEFAULT GATEWAY.
    - Estações normais ("host") normalmente não possuem Tabela de Roteamento e mandam sempre para o Default Gateway.

O Protocolo IP

- **O Roteamento IP**
  - **Roteamento Direto**
    - Corresponde à entrega do datagrama para um destinatário pertencente à mesma rede física do remetente;
    - Basta que o host remetente compare o campo NetID do endereço IP do host destinatário com o NetID do seu próprio endereço.
    - É relativamente simples. Basta que o datagrama a ser enviado seja encapsulado no frame do nível físico, o endereço IP sendo mapeado no endereço físico do remetente.

O Protocolo IP

- **O Roteamento IP**
  - **Roteamento Indireto**
    - Utilizado para entregar o datagrama a um host destinatário em uma rede distinta à do remetente.
    - O host remetente encaminha o datagrama (por roteamento direto) até o gateway mais próximo.
    - Este, por sua vez, o encaminha a um outro gateway, de modo a que, de gateway em gateway, este seja entregue ao host destinatário.

O Protocolo IP

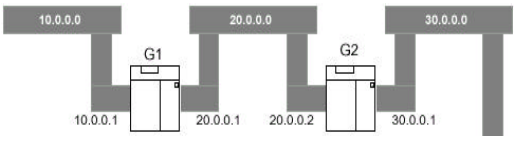
- **Roteamento Indireto**
  - Como o host remetente vai saber para que gateway encaminhar o datagrama?
  - Como o gateway vai saber qual é a melhor rota para que o datagrama chegue ao seu host destinatário?

O Protocolo IP

- **Roteamento Indireto**
  - **Tabelas de Roteamento**
    - A tarefa de roteamento realizada pelo protocolo IP é baseada na existência de Tabelas de Roteamento (IP Routing Table) implementadas em cada host e gateway. Estas tabelas contêm os endereços de possíveis destinatários e o caminho a tomar para que os datagramas cheguem até eles.

O Protocolo IP

- **Roteamento Indireto**
  - **Tabela é composta de dois campos:**
    - um campo N, que contém o NetID da rede considerada;
    - um campo G que contém o endereço IP completo do gateway daquela rede.



O Protocolo IP

- **Roteamento Indireto**

G1		G2	
NetID	Gateway	NetID	Gateway
10.0.0.0	Entrega direta	10.0.0.0	20.0.0.1
20.0.0.0	Entrega direta	20.0.0.0	Entrega direta
30.0.0.0	20.0.0.2	30.0.0.0	20.0.0.2
40.0.0.0	20.0.0.2	40.0.0.0	30.0.0.2
50.0.0.0	20.0.0.2	50.0.0.0	30.0.02

O Protocolo IP

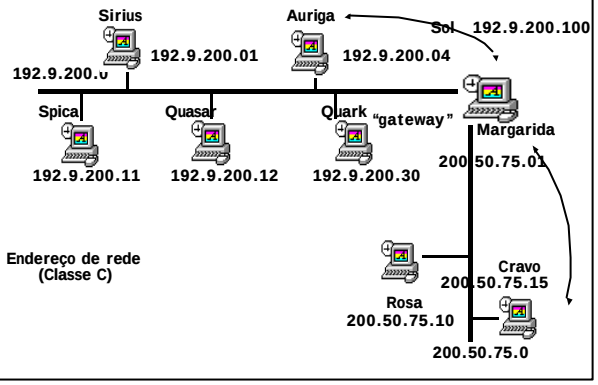
- **O Default Gateway**
  - Normalmente, nas redes interconectadas, é importante a definição de um Default Gateway, o qual é utilizado basicamente em duas situações:
    - quando não existe, numa tabela de roteamento, o mapeamento para um dado NetID; neste caso, o datagrama é encaminhado ao Gateway Default;
    - em redes pequenas, providas de apenas um gateway; este gateway assume o papel de Default Gateway para todos os hosts da rede, o que simplifica bastante o processo de envio dos datagramas.

O Protocolo IP

Algoritmo de Roteamento

- 1. extrair o endereço IP do host destinatário do datagrama;
- 2. verifica se o NetID do host endereço IP do host destinatário é igual ao NetID da rede conectada diretamente;
- 3. em caso positivo, envia o datagrama utilizando o roteamento direto;
- 4. se o datagrama especifica uma rota específica, rotear segundo esta especificação;
- 5. se o NetID não é igual ao da rede considerada, consultar a tabela de roteamento e encaminhar o datagrama para o gateway especificado;
- 6. se o NetID não constar na tabela, encaminhar o datagrama ao Gateway Default.

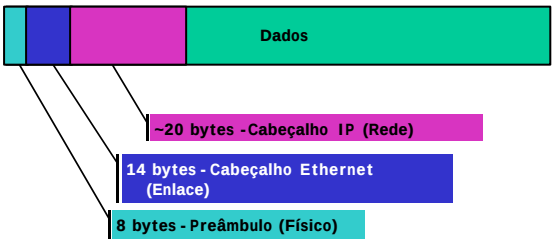
O Protocolo IP



O Protocolo IP

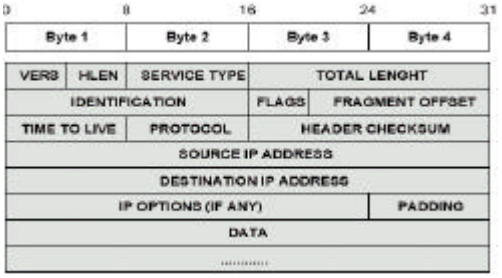
O Cabeçalho IP

- Exemplo de um pacote em rede local ethernet



O Protocolo IP

O Formato do Cabeçalho IP



O Protocolo IP

O Formato do Cabeçalho IP

- Vers
  - Este campo de 4 bits permite identificar a versão do protocolo IP que gerou o datagrama. Isto permite aos hosts responsáveis da interconexão manterem a compatibilidade com relação ao formato dos datagramas. Caso a versão do IP especificada neste campo não seja compatível com a instalada no host, o datagrama é descartado por ele para evitar leitura errada de campos. Versão atual: 4

O Protocolo IP

O Formato do Cabeçalho IP

- Hlen
  - Campo de 4 bits que especifica o tamanho do cabeçalho dodatagrama (em grupos de 4 bytes). Todos os campos do cabeçalho apresentam tamanho fixo, com exceção dos campos OPTIONS e PADDING. O cabeçalho típico (sem levar em conta os dois campos citados anteriormente) é composto de 20 bytes (ou 5 x 32 bytes). Portanto, o tamanho do cabeçalho seria expresso como 5 neste campo.

O Protocolo IP

O Formato do Cabeçalho IP

- Total Length
  - Campo de 16 bits especificando o tamanho total do datagrama IP (considerando o cabeçalho e os dados). Isto significa que o tamanho máximo de um datagrama poderá ser de 2^{16} ou 65.536 bytes.
- Service Type
  - Especifica, em 8 bits, o tipo do serviço oferecido para a transmissão do datagrama. Basicamente, permite aos hosts definirem de que forma deverá ser encaminhado o datagrama (baixo "delay", alta confiabilidade, grande banda passante, etc).

O Protocolo IP

O Formato do Cabeçalho IP

- Time to Live
  - Este campo de 8 bits funciona como um mecanismo de controle de congestionamento. Ao ser enviado pelo remetente, este campo é preenchido com um dado valor que é decrementado a cada vez que passa por um host. Este valor representa um "tempo máximo" de circulação do datagrama na rede. Ao passar por um host, se este campo assume o valor "0", o datagrama é descartado imediatamente. Nem sempre definir o valor a ser atribuído ao campo Time to Live é uma tarefa simples, principalmente no caso de redes grandes.

O Protocolo IP

O Formato do Cabeçalho IP

- Identification, Fragment Offset e Flags
  - Estes três campos estão associados ao controle da fragmentação e restauração de datagramas.
  - O campo Identification, de 16 bits, contém um número de identificação do datagrama que é copiado em todos os fragmentos do mesmo datagrama. Isto garante ao host destinatário a informação de quais fragmentos fazem parte do mesmo datagrama.

O Protocolo IP

O Formato do Cabeçalho IP

- Identification, Fragment Offset e Flags
  - O campo Fragment Offset é um campo de 13 bits que permite situar a posição do fragmento no datagrama.
  - O campo Flags, composto de 3 bits, onde cada bit tem a função de sinalizar um aspecto específico. O primeiro bit de flag indica se o datagrama está fragmentado (0) ou não (1). Os dois outros bits de flag são utilizados na restauração do datagrama. O bit 2 indica que um dado fragmento corresponde ao meio do datagrama enquanto o bit 3 informa que aquele fragmento é o último do datagrama.

O Protocolo IP

O Formato do Cabeçalho IP

- Protocol
  - Este campo de 8 bits permite especificar o protocolo utilizado a nível superior (no Nível de Transporte) que gerou o conteúdo do campo Data do datagrama IP (por exemplo, TCP ou UDP).
- Header Checksum
  - Este campo é utilizado para garantir a integridade dos campos do cabeçalho do datagrama.

O Protocolo IP

O Formato do Cabeçalho IP

- Source IP e Destination IP
  - Endereços IP do remetente e do destinatário do datagrama (representado em 32 bits ou 4 bytes).
- IP Options
  - Campo opcional de tamanho variável que permite indicar eventuais opções de operação do protocolo.

Opção	Descrição
Record Route	permite marcar no datagrama a sua rota
Loose Source Routing	utilizado para que o remetente defina a rota do datagrama
Strict Source Routing	outra forma de definição de rota (mais restrita)
Timestamp	permite registrar o instante de tratamento do datagrama

O Protocolo ARP

- **O Protocolo ARP (Address Resolution Protocol) - Somente para IP operando em rede local ethernet.**
  - Como já vimos, os endereços das estações Ethernet são codificados em 48 bits, definidos pelo fabricante.
  - Existe a incompatibilidade entre os 32 bits utilizados pelo IP e os 48 bits utilizados pela Ethernet.
  - Além disso, quando uma falha de hardware ocorre (problema na placa), a interface é substituída, modificando o endereço Ethernet da máquina considerada.

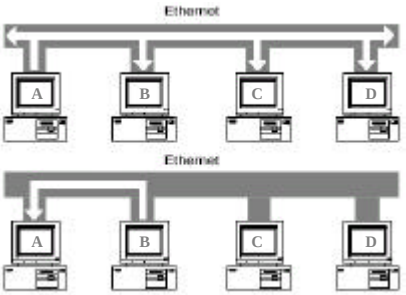
O Protocolo ARP

- COMO FAZER PARA DESCOBRIR O ENDEREÇO ETHERNET DA MÁQUINA DESTNO, SE POSSUO APENAS O ENDEREÇO IP DELA?

O Protocolo ARP

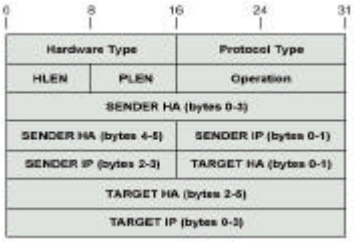
- **O Protocolo ARP (Address Resolution Protocol)**
  - A forma encontrada para solucionar este problema veio através das facilidades de broadcasting das redes Ethernet. O protocolo ARP foi então criado para manipular este tipo de mapeamento.
  - O protocolo ARP mapeia endereços IP para endereços físicos.
    - A deseja mandar uma mensagem para B.
    - A manda uma mensagem em "broadcast": "qual é o endereço físico de quem tem o endereço Internet igual a IB?".
    - B responde: "o endereço físico FB corresponde ao endereço Internet IB".

O Protocolo ARP



O Protocolo ARP

- **O cabeçalho ARP**



O Protocolo ARP

- **O cabeçalho ARP**

Campo	Função
Hardware Type	tipo de hardware utilizado na rede (16 bits)
Protocol Type	tipo de protocolo adotado no nível de Rede (16 bits)
HLEN	tamanho dos campos Sender HA e Target HA (8 bits)
PLEN	tamanho dos campos Sender IP e Target IP (8 bits)
Operation	indica se é um pedido/resposta ARP ou RARP (16 bits)
Sender HA	endereço físico do host remetente (48 bits)
Sender IP	endereço IP do host remetente (32 bits)
Target HA	endereço físico do host destinatário (48 bits)
Target IP	endereço IP do host destinatário (32 bits)

O Protocolo RARP

- **O Protocolo RARP (Reverse Address Resolution Protocol)**
  - O protocolo ARP foi definido considerando que todos os hosts conectados à rede conhecem seus endereços IP, o que não é necessariamente verdadeiro para todas as situações.
  - Normalmente, os endereços IP de um host é armazenado em disco, de modo a que este seja recuperado durante o boot da máquina. Sendo assim, como fica a situação de uma máquina desprovida de disco?

O Protocolo RARP

- **O Protocolo RARP (Reverse Address Resolution Protocol)**
  - O protocolo RARP foi definido para atender a esta situação específica. A operação deste protocolo baseia-se igualmente na facilidade de broadcasting da rede e utiliza o mesmo cabeçalho, sendo que um menor número de informações é preenchido neste, pelo fato do host ignorar seus endereços IP.
  - O datagrama de broadcasting é então respondido por hosts especiais denominados servidores RARP, os quais preenchem os conteúdos "vazios" do cabeçalho RARP.

Algoritmos de Roteamento

- **Tipos de Roteamento:**
  - Estático:
    - Não troca informações de roteamento com outros roteadores, utilizando apenas uma tabela de roteamento interna pré-programada.
  - Dinâmico:
    - Aprende sobre alcançabilidade de outras redes utilizando algum dos muitos protocolos de roteamento, tais como RIP (Routing Internet Protocol) , OSPF (Open Shortest Path First), etc.

Algoritmos de Roteamento

- **Algoritmos de Roteamento Dinâmico**
  - Roteamento com vetor distância
    - O roteamento com vetor de distância opera fazendo com que cada roteador mantenha uma tabela (ou seja, um vetor) que fornece a melhor distância conhecida a cada destino e determina qual linha deve ser utilizada para se chegar lá. Essas tabelas são atualizadas através da troca de informações com os vizinhos.
    - Também chamado de algoritmo de roteamento de Bellman-Ford distribuído e algoritmo de Ford-Fulkerson.

Algoritmos de Roteamento

- **Algoritmos de Roteamento Dinâmico**
  - Roteamento por estado de enlace
    - Cada roteador deve fazer o seguinte:
      1. Descobrir seus vizinhos e aprender seus endereços de rede.
      2. Medir o retardo ou o custo para cada um de seus vizinhos.
      3. Criar um pacote que diga tudo o que acaba de ser aprendido.
      4. Enviar esse pacote a todos os outros roteadores.
      5. Calcular o caminho mais curto para cada um dos outros roteadores.

Algoritmos de Roteamento

- **Algoritmos de Roteamento Dinâmico**
  - Roteamento Hierárquico
    - À medida que as redes aumentam de tamanho, as tabelas de roteamento do roteador crescem proporcionalmente.
    - Não somente a memória do roteador é consumida por tabelas cada vez maiores, como também é necessário mais tempo de CPU para percorrê-las e mais largura de banda para enviar relatórios de status sobre elas.
    - Em um determinado momento, a rede pode crescer até o ponto em que não mais é viável todos os roteadores terem uma entrada para todos os outros roteadores.

Algoritmos de Roteamento

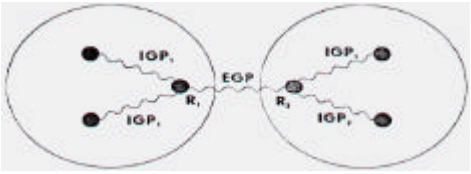
- **Algoritmos de Roteamento Dinâmico**
  - Roteamento Hierárquico
    - Portanto, o roteamento terá de ser feito hierarquicamente, como na rede telefônica.
    - Os roteadores são divididos em regiões, com cada roteador conhecendo todos os detalhes sobre como rotear pacotes para destinos dentro de sua própria região, mas sem conhecer coisa alguma sobre a estrutura interna de outras regiões.
    - Quando diferentes redes são interconectadas, é natural que cada uma seja vista como uma região separada a fim de liberar os roteadores de uma rede da necessidade de conhecerem a estrutura topológica das outras.

Algoritmos de Roteamento

- **Protocolo entre Roteadores da mesma região (IGP – Interior Gateway Protocol)**
  - Dois roteadores sob o controle de um único gerenciador executam um IGP, para promover o intercâmbio de informações sobre o roteamento. Dois roteadores de um sistema autônomo são considerados internos entre si.
  - Para manter precisas as informações sobre acessibilidade da rede, os roteadores internos comunicam-se entre si, trocando dados sobre a acessibilidade da rede.
  - Quando as informações de acessibilidade de todo o sistema autônomo estiverem reunidas, um dos roteadores do sistema pode anunciá-las a outro sistema igual ao EGP

Algoritmos de Roteamento

- **Protocolo entre Roteadores da mesma região (IGP – Interior Gateway Protocol)**



Algoritmos de Roteamento

- **Protocolo entre Roteadores de regiões diferentes (EGP - Exterior Gateway Protocol)**
  - Um sistema autônomo (SA) usa o EGP para anunciar rotas à outros sistemas autônomos.
  - Dois roteadores pertencentes a SA diferentes que trocam informações sobre roteamento são considerados vizinhos externos e, vizinhos internos se pertencerem ao mesmo SA. O protocolo que os vizinho externos usam para anunciar acessibilidade a outros SA chama-se EGP.

Algoritmos de Roteamento

- **Protocolo entre Roteadores de regiões diferentes (EGP - Exterior Gateway Protocol)**

Algoritmos de Roteamento

- **O EGP suporta três funções básicas:**
  - **Aquisição de vizinho (par).**
    - Permite que um roteador solicite a um roteador de outro SA comunicar informações de acessibilidade.
    - O roteador envia mensagens de aquisição de vizinhos para estabelecer uma comunicação do EGP com outro roteador. O EGP não especifica a razão ou forma como um roteador escolhe outro roteador como vizinho.
    - A mensagem contêm o intervalo de tempo para testar se o vizinho está vivo (intervalo hello), o intervalo de consulta (polling interval) para atualizações do roteamento.

Algoritmos de Roteamento

- **O EGP suporta três funções básicas:**
  - **Teste de acessibilidade do vizinho.**
    - O roteador testa continuamente se os vizinhos EGPs estão respondendo.
  - **Mensagem de atualização de roteamento.**
    - Os vizinhos EGPs trocam periodicamente informações de acessibilidade da rede, enviado mensagens de atualização do roteamento.
    - Um roteador externo envia uma mensagem de atualização de roteamento para transmitir informações sobre redes acessíveis ao seu vizinho.

Algoritmos de Roteamento

- **RIP (Routing Information Protocol)**
  - Este protocolo foi inicialmente desenvolvido como um componente do código de rede do UNIX BSD, amplamente inspirado pelo XNS-RIP (protocolo da Xerox).
  - É um protocolo extremamente simples, da família dos algoritmos de roteamento vetor-distância
  - Parte do princípio que toda entidade (roteador ou host) que participa do protocolo de roteamento, mantém uma tabela com informação sobre todos os demais nós da sua rede.
  - O RIP é destinado às redes baseadas no protocolo IP e UDP, e foi projetado para redes razoavelmente homogêneas de tamanho médio.

Algoritmos de Roteamento

- **RIP (Routing Information Protocol)**
  - Os pacotes RIP são transmitidos "em cima" de UDP e IP, usando a porta 520 do UDP tanto para transmissão quanto para recepção.
  - Se uma rota não é atualizada dentro de 180 segundos, sua distância é colocada em infinito e a entrada será mais tarde removida das tabelas de roteamento.

Algoritmos de Roteamento

- **RIP (Routing Information Protocol)**
  - Os roteadores Rip trocam o endereço de rede que cada roteador pode alcançar.
  - Ele utiliza um contador de nós roteadores (hop count) na sua tabela de roteamento para determinar adistância entre redes.
  - Redes com hop count maior que 16 são consideradas inatingíveis.
  - Se existirem várias rotas para um host na tabela de roteamento, um roteador RIP sempre utilizará a rota com menor número de nós.

Algoritmos de Roteamento

- **RIP (Routing Information Protocol)** -Vantagens e Desvantagens do RIP
  - Vantagens:
    - Em redes pequenas não despende muita largura de banda e tempo de configuração e gerenciamento;
    - Fácil implementação;

Algoritmos de Roteamento

- **RIP (Routing Information Protocol)** -Vantagens e Desvantagens do RIP
  - Desvantagens:
    - Cada roteador mantém uma tabela completa de toda a rede e rotas para todos os host conhecidos.
    - As tabelas de roteamento podem se tornar extremamente grandes.
    - O tamanho máximo de um pacote Rip é de 512 bytes, de modo que grandes tabelas de roteamento devem ser transmitidas como múltiplos pacotes, o que pode levar a grandes tráfegos.

Algoritmos de Roteamento

- **RIP (Routing Information Protocol)** -Vantagens e Desvantagens do RIP
  - Desvantagens:
    - Roteadores RIP enviam o conteúdo de suas tabelas através de quadros em broadcast a cada 30 segundos.
    - Convergência lenta quando ocorre um rearranjo na topologia da rede em redes de tamanho médio ou grande;
    - Existência de loops e contagem ao infinito;
    - Limitações do número saltos por caminho (15);
    - Limitação de métrica.

Algoritmos de Roteamento

- OSPF (Open Shortest Path First)
  - O OSPF é um protocolo de roteamento dinâmico.
  - O protocolo rapidamente detecta mudanças no SA(como falhas na interface de roteamento) e calcula novas rotas, livres de loops, após o período de convergência. Este período de convergência é pequeno e envolve o mínimo de tráfego de roteamento.

Algoritmos de Roteamento

- OSPF (Open Shortest Path First)
  - O OSPF permite conjuntos de redes serem agrupados.
  - Este grupo é chamado de área.
  - A topologia de uma área não e vista pelo resto do SA.
  - Esta informação ocultada, permite uma redução significativa no tráfego de roteamento.
  - Da mesma forma, o roteamento de uma área é determinado apenas pela topologia da área, dando proteção a área de dados de roteamentos errados.

Algoritmos de Roteamento

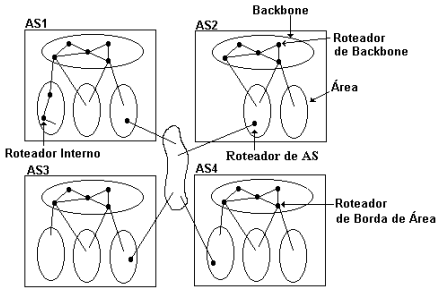
- OSPF (Open Shortest Path First)
  - O protocolo OSPF permite uma configuracão flexível de sub-redes IP.
  - Cada rota distribuída pelo OSPF possui um destino e uma máscara.
  - Duas sub-redes diferentes em um mesmo número IP de rede pode ter diferentes tamanhos (máscaras). Isto é comumente referenciado como tamanho variável de sub-redes. Um pacote é roteado para melhor combinação.

Algoritmos de Roteamento

- OSPF (Open Shortest Path First)
  - Toda troca do protocolo OSPF é autenticada.
  - Isto significa que apenas rotas confiáveis podem participar do roteamento de um sistema autônomo.
  - Uma variedade de esquemas de autenticação pode ser usado. Um esquema simples de autenticação é configurado para cada área. Isto permite algumas áreas usar autenticação mais restrita que outras.

Algoritmos de Roteamento

- OSPF (Open Shortest Path First)



Algoritmos de Roteamento

- OSPF (Open Shortest Path First)
- Por que OSPF ?
  - Suporte a subnetmask de tamanho variável - Variable-lenght subnet mask (VLSM).
  - Atualização de rotas sem os 30 segundos de "hold-down" requeridos pelo RIP.
  - Otimização de banda.
  - Até 255 segmentos entre roteadores.
  - Atualização segura de rotas através de autenticação.

Algoritmos de Roteamento

- OSPF (Open Shortest Path First)
- Quando usar o OSPF
  - Quando um roteador ou servidor de comunicação deve acomodar diferentes tamanhos de redes TCP/IP.
  - Quando as mudanças no roteamento deve se propagar rapidamente.
  - Quando se faz necessário mais de 15 saltos entre roteadores.
  - Quando a divulgação das rotas deve ser feita de modo seguro, para prevenir contra instabilidade da rede ou ataques de hackers.

Algoritmos de Roteamento

- Dependendo do tamanho da rede, diferentes protocolos de roteamento devem ser usados
- Internamente a um sistema autônomo, os protocolos de roteamento interno são usados.
  - O mais conhecido é o RIP (*Routing Information Protocol)*, implementado pelo *daemon routed*, da Berkeley (BSD).
- Para roteamento externo, são necessários protocolos como o EGP (*External Gateway Protocol)*, ou o BGP *(Border Gateway Protocol)*.
  - Estes, bem como o RIP, estão implementados no *daemon gated*, da Universidade de Cornell.

Algoritmos de Roteamento

- OBS: Como *gated* suporta RIP, é preferível seu uso frente ao *routed*. Além disso, é necessário rodar o *daemon* em todas as máquinas da rede.
- **Funcionamento do RIP**
  - Atualização a cada 30s (RNP n.1v.1)
- **Funcionamento do OSPF**
  - Atualização total a cada 10min (RNP n.1v.1), mas pequenas atualizações em menos tempo com “hello packets”.

Problemas com o crescimento da Internet

- **Eventual exaustão do endereçamento IPv4**
- **Habilidade para rotear tráfego em um número crescente de redes (tabelas de roteamento)**
  - **IPv4:** endereços de 32 bits (2^{32} = 4.294.967.296) endereços disponíveis. Parece bastante, mas ele é mal distribuído na visão classful de endereços.
    - O CIDR foi uma forma paliativa de resolver este problema.

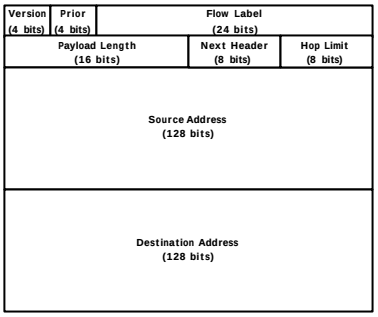
Forma de Representação dos Endereços IPv6

- x:x:x:x:x:x:x:x, onde os "x" são números hexadecimais, ou seja, o endereço é dividido em oito partes de 16 bits, com por exemplo: 1080:0:0:0:8:800:200C:417A
- Utilizando a notação :: para substituir uma seqüência de zeros (uma única vez no endereço). Por exemplo:
  Unicast: 1080:0:0:0:8:800:200C:417A. - > 1080::8:800:200C:417A
  Multicast: FF01:0:0:0:0:0:0:43 -> FF01::43
  Loopback: 0:0:0:0:0:0:0:1 -> ::1
  Unspecified: 0:0:0:0:0:0:0:0 -> ::

Forma de Representação dos Endereços IPv6

- Para usar na transição de IPv4 e IPv6: x:x:x:x:x:x:d:d:d:d, onde os "x" são números hexadecimais (16 bits) e os "d" são valores decimais de 8 bits, referentes à representação padrão do IPv4.
- Por exemplo: 0:0:0:0:0:0:192.168.20.30, ou, na forma abreviada: ::192.168.20.30

Formato do cabeçalho IPv6



Formato do cabeçalho IPv6

- **Version -** 4 bits com a versão do IP utilizado (6).
- **Prior -** Diz o nível de prioridade (4 bits). Permite que uma origem especifique a prioridade de entrega para determinados pacotes em relação a outros pacotes da mesma origem.
- **Flow Label -** Campo de 24 bits, relacionado com a qualidade de serviço do pacote.
- **Payload Length -** Inteiro sem sinal (16 bits). Tamanho do *payload*, isto é, o resto do pacote que segue o cabeçalho IPng em octetos.

Formato do cabeçalho IPv6

- **Next Header -** Campo de 8 bits. Identifica o tipo de cabeçalho que segue o cabeçalho IPng. Usar o mesmo valor do protocolo IPv4.
- **Hop Limit -** Inteiro sem sinal (8 bits). Decrementado de 1 a cada *node* que passa o pacote. O pacote é descartado caso o *hop limit* seja igual a zero. Semelhante ao TTL no Ipv4.
- **Source Address e Destination Address -** Campos de 128 bits com os endereços fonte e destino do pacote.

Exercícios

- A)Fazer esquematicamente o espaço de endereçamento IPv4 para as classes A, B, C, D e E, desenhando o resultado.
- B) Especificar número dehosts e redes máximo para cada classe.
- C) Especificar quanto porcento do espaço de endereçamento é usado para cada classe.
- D) Especificar o range de endereços na terminologia de ponto decimal para cada classe

IP sobre ATM

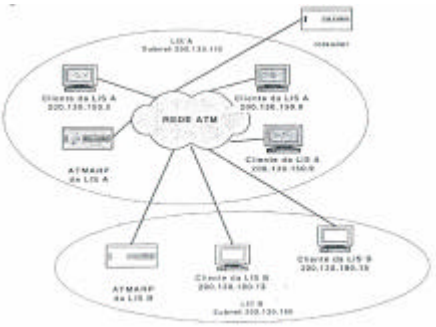
- Proposta do IETF (Internet Engineering Task Force) descrita na RFC 1577.
- ATM (Asynchronous Transfer Mode) - Modo de transferência assíncrono
  - Utiliza células fixas de 53 bytes (cabeçalho: 5 bytes)
  - Transporta voz, som, imagem
  - Camada Física: transporte das células na rede. Geralmente é usada fibra ótica (OSI 1 e 2).
  - Camada ATM: trata do encaminhamento ponto a ponto das células - geração/extração do cabeçalho das células (OSI 2 e 3).
  - Camada AAL (adaptação): detecção de perda e inserção de células, segmentação e remontagem (OSI 3 e 4).

IP sobre ATM

- **Modelo**
  - Modelo composto por uma ou mais LIS (Logical IP Subnets)
  - LIS: conjunto de estações ou roteadores pertencentes a uma mesma sub-rede IP
  - Os membros da LIS devem estar conectados diretamente à rede ATM e ter o mesmo endereço de sub-rede (mesma máscara)
  - Os membros de fora de uma LIS somente são acessados através de roteadores
  - Cada LIS tem seu próprio servidor ATMARP

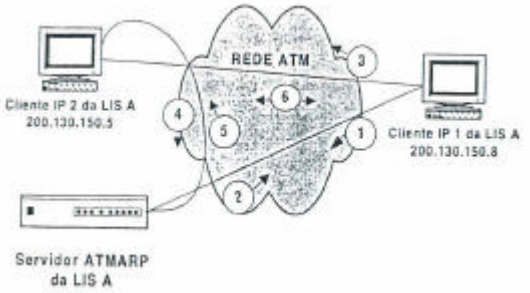
IP sobre ATM

- **Modelo**



IP sobre ATM

- **Modelo**



O Protocolo ICMP

- **O Protocolo ICMP (Internet Control Messages Protocol)**
  - **Roda "em cima" do IP**
  - **MENSAGENS DE ERRO E CONTROLE DA INTERNET**
  - **Exemplos de Serviços:**
    - Echo Request / Reply **(ping)**
    - Unreachable Destinations
    - Datagram Flow Control
    - Circular or Excessively Long Routes
    - Obtaining a Subnet Mask
    - etc.

Exercícios

- O que aconteceria numa rede TCP/IP se uma placa de rede local ethernet da rede queima e tem de ser substituída?
- O que é um default-gateway?
- Como o protocolo IP trata mensagens que eventualmente se perdem na rede e não consegue ser entregues ao host de destino?
- Para que serve o protocolo ARP? De um exemplo em que não seria necessária a utilização do protocolo ARP.

Exercícios

- Sabe-se que o endereçamento IP versão 4 reserva 4 bytes para o endereço IP. Isto possibilitaria endereçar 232-1 (4.294.967.295) endereços diferentes (comparativamente, a população da Terra é de 6.000.000.000). Porque então se diz que os endereços IP estão praticamente "esgotados"?
- Quais as informações que podem ser obtidas de um endereço IP?
- O que aconteceria se duas estações em uma mesma rede fossem configuradas acidentalmente com o mesmo endereço IP?

Exercícios

- Qual seria o valor da "mascara de sub-rede" em uma rede classe C que possuisse 8 sub-redes? Quantos "hosts" seria possível endereçar em cada sub-rede?
- Supondo que não existe o conceito de "máscara de sub-rede", o que você sugeriria que se fizesse no default-gateway para implementar fisicamente sub-redes?

Exercícios

- Após monitorar o tráfego IP em uma rede local ehernet por 10 minutos, você percebe que todos os quadros destinados à uma máquina X (cujo endereço ethernet é 'HX'), possuem no cabeçalho IP o "endereço IP destino" igual ao endereço IP da máquina X, enquanto todos os quadros destinados a uma máquina Y (cujo endereço etherner é 'HY'), possuem no cabeçalho IP o "endereço IP destino" um endereço diferente do endereço IP da máquina Y. Explique o que está acontecendo.

Nível de Transporte

- **O Protocolo TCP (Transmission Control Protocol)**
  - A principal função do protocolo TCP é a comunicação confiável de dados entre duas máquinas da rede.
  - Quando dados são roteados através de uma rede, eles podem ser duplicados, perdidos, entregues fora de ordem, ou demorar muito para serem entregues.
  - O TCP provê também a capacidade de multiplexação/demultiplexação das mensagens entre as aplicações.

Nível de Transporte

- **O Protocolo TCP (Transmission Control Protocol)**
  - Provê um sistema de comunicação CONFIÁVEL e ORIENTADO A CONEXÕES.

O Protocolo TCP - Principais Características

- **A conexão TCP sempre é duplex e ponto-a-ponto.**
  - Ponto-a-ponto significa que existe somente dois pontos finais (TSAP = *socket + port number*).
  - TCP portanto não suporta *broadcast ou multicast*.

O Protocolo TCP - Principais Características

- Uma conexão TCP é essencialmente um fluxo de bytes, ou seja, a unidade de transferência não é uma mensagem mas sim o byte.
- O significado dos dados no TCP é restrito ao byte, não conhece bloco ou qualquer outra estrutura.
- A cada byte está associado um número de sequenciação constituído de 32 bits.

O Protocolo TCP - Principais Características

- O TCP tem como mandar dados segundo um esquema de prioridade chamado urgent data que permite rapidamente passar dados altamente prioritários para a aplicação.
- É possível ao TCP abortar uma conexão.
- É função do TCP ordenar em seqüência correta os bytes e repassá-los para a interface de aplicação.

O Protocolo TCP - Principais Características

- **Tratamento dos Tamanhos dos Segmentos**
  - Diferentes tamanhos de blocos de dados podem ser manipulados no contexto das aplicações. Esta diversidade de tamanhos deve ser gerenciada pelo protocolo TCP.
  - O tratamento dos diferentes blocos de dados das aplicações é realizado basicamente em duas situações típicas:

O Protocolo TCP - Principais Características

- **Tratamento dos Tamanhos dos Segmentos - continuação**
  1 - no caso de blocos de dados muito grandes, o TCP deve fragmentá-los.
  2 - no caso de blocos de dados extremamente pequenos, o procedimento é inverso...o TCP bufferiza estes blocos e os envia em grupos encapsulados num mesmo segmento de nível inferior.
- **Este processo é transparente para o usuário.**

O Protocolo TCP - Principais Características

- **A Garantia da Integridade dos Dados**
  - É implementado um algoritmo de detecção de erros denominado "Checksum", o qual verifica não apenas a integridade do header (como no caso do IP), mas também dos dados transmitidos.
  - Para evitar duplicação de mensagens, o TCP gera um número de seqüência o qual é controlado pelos elementos envolvidos na comunicação. A confirmação das mensagens também utiliza este seqüenciamento.

O Protocolo TCP - Principais Características

- A Garantia da Integridade dos Dados - continuação
  - **Conta** bytes **para o sequenciamento:**
    - os dados que estou enviando começam no byte número X.
    - o próximo byte que eu espero receber é o de número Y.
  - **"**Positive acknowlegment**" com reconhecimento embutido em pacotes de dados (**"ack piggybacking**").**

O Protocolo TCP - Principais Características

- **Diálogo "Full-Duplex"**
  - O TCP permite a realização dos diálogos segundo um esquema de comunicação bidirecional simultânea (ou Full Duplex).
- **Término Ordenado de Conexões**
  - Neste caso, uma aplicação A que termine o envio de dados para uma aplicação B pode encerrar sua transmissão mas continuar a receber dados da outra aplicação até que esta encerre também a sua transmissão.
  - Não importa quem iniciou a conexão.

O Protocolo TCP - Principais Características

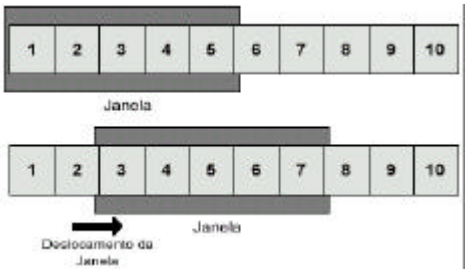
- **Protocolo Sliding Window - Janelas Deslizantes**
  - O TCP implementa um protocolo de transmissão denominado Sliding Window (ou Janela Deslizante, em Português) o qual propicia o envio de vários segmentos de dados encapsulados em seus datagramas IP, sem a necessidade de confirmação imediata da sua recepção.
  - Uma mesma confirmação pode ser utilizada para notificar a chegada de vários destes segmentos.

O Protocolo TCP

- Protocolo **Sliding Window - Janelas Deslizantes**

O Protocolo TCP

- Protocolo **Sliding Window - Janelas Deslizantes**

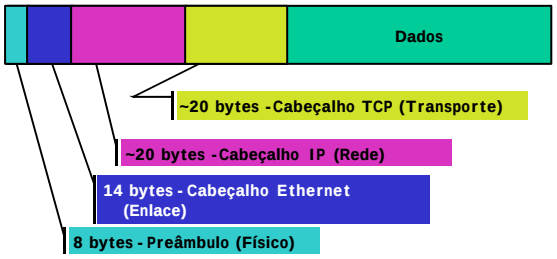


O Protocolo TCP - Principais Características

- **Janela de Tamanho Variável**
  - Permite um controle d fluxo fim-a-fim, de modo que máquina mais rápidas não "entupam" os buffers de máquinas mais lentas.
- **Timeout Adaptativo**
  - Permite que o protocolo se auto-ajuste quanto ao intervalo para retransmissão de mensagens.

O Protocolo TCP

- **O Cabeçalho TCP**



O Protocolo TCP

- **O Formato do Cabeçalho TCP**

SOURCE PORT			DESTINATION PORT
SEQUENCE NUMBER			
ACKNOWLEDGEMENT NUMBER			
HLEN	RESERVED	CODE BITS	WINDOW
CHECKSUM			URGENT POINTER
OPTIONS (IF ANY)			PADDING
DATA			

O Formato do Cabeçalho TCP

- **Source Port e Destination Port**
  - São campos de 16 bits que indicam os Ports das aplicações associadas a um dado canal virtual (Port Fonte e Port Destino) que serão associados aos endereços IP para definir o endereço do canal.
- **Sequence Number**
  - Campo de 32 bits utilizado para implementar a garantia de entrega do TCP (indica o número do primeiro byte de dados que a mensagem está transmitindo).

O Formato do Cabeçalho TCP

- **Acknowledgement Number**
  - Composto de 32 bits, este campo indica o número do primeiro byte da próxima mensagem a ser recebida. (até este número - 1 os bytes foram bem recebidos).
- **Hlen**
  - Especifica o tamanho (em 4 bits) do cabeçalho do bloco TCP.
- **Reserved**
  - Este campo de 6 bits é reservado para futuras implementações do TCP.

O Formato do Cabeçalho TCP

- **Code Bits**
  - Campo de 6 bits, utilizado para indicar a função da mensagem TCP. Este campo define um bit para cada função especificada no protocolo.

Bit	Nome	Indicação
1	URG	necessidade de leitura do campo Urgent Pointer
2	ACK	envio de confirmação válida no cabeçalho
3	PSH	autoriza envio dos dados à aplicação
4	RST	solicitação de retomada de conexão
5	SYN	solicitação de conexão a outra entidade TCP
6	FIN	solicitação de desconexão

O Formato do Cabeçalho TCP

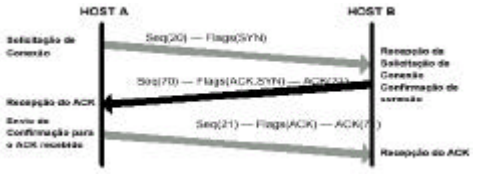
- **Window**
  - Campo de 16 bits especifica o tamanho da janela que o transmissor da mensagem está apto a receber (sliding window).
- **Checksum**
  - Campo de 16 bits utilizado para a detecção de erros de transmissão. Abrange o cabeçalho e a área de dados.
- **Urgent Pointer**
  - Campo de 16 bits que sinaliza a uma aplicação a informação de uma informação urgente presente na mensagem, indicando a posição desta informação na mensagem.

O Formato do Cabeçalho TCP

- **Options**
  - Campo de tamanho variável que permite a implementação de algumas opções de operação do protocolo, particularmente a opção MSS (Maximum Segment Size), que é uma opção que permite definir um tamanho máximo para os segmentos TCP.
- **Padding**
  - Este campo é utilizado para complementar o campo Options, que deve ser composto de 32 bits ou múltiplos deste valor.

O Protocolo TCP - Operação

- **Estabelecimento de uma Conexão TCP**
  - O estabelecimento de conexão é baseado numa técnica denominada “Aperto de Mão Triplo” (Triple Handshaking).
  - O processo pode ser inicializado por qualquer uma das partes envolvidas.



Operação do TCP

- **A Troca de Dados no TCP**
  - Estabelecida a conexão, os dados irão transitar num esquema de comunicação "Full-Duplex".
  - Durante a troca de dados, os números de seqüência vão se alterando de modo a manter um sincronismo entre os elementos envolvidos na comunicação.
  - O campo Acknowledgement Number de um segmento TCP de confirmação sempre indica o próximo segmento esperado pelo destinatário.

Operação do TCP

- **Fechamento de Conexões**
  - Fechamento bem ordenado de conexões.
  - As conexões TCP são finalizadas comumente a partir de uma operação "Close", emitida por um programa de aplicação. O TCP vai então gerar um pacote com o code bit de FIN setado indicando que o seu lado do canal não tem mais nada para transmitir.
  - No entanto o canal do lado do outro host permanece aberto até que ele também resolva encerrar as suas transmissões.

Operação do TCP

- **Reset do Protocolo TCP**
  - Fechamento abrupto de conexões.
  - Quando o processo de desconexão for caracterizado pela ocorrência de uma falha, o aplicativo pode utilizar o serviço "Reset", o qual permite abortar a conexão. Neste caso, o segmento TCP que vai caracterizar este serviço vai ter o bit RST do seu campo CodeBits setado. O receptor do segmento vai liberar imediatamente o canal virtual.

Operação do TCP

- **Endereçamento de Aplicações**
  - **Estabelecimento de Canais Virtuais**
  - Dado que o protocolo implementado no TCP deve fornecer um serviço de Transporte "Fim a Fim" para as aplicações, este executa um mecanismo baseado no estabelecimento simultâneo de vários canais (ou "pipes") utilizando a técnica de circuito virtual.
  - Segundo esta técnica, é estabelecido um canal lógico entre as aplicações fonte e destino, através do qual será realizado o diálogo segundo o esquema "Full Duplex".
  - Terminada a transmissão, o canal é automaticamente cancelado.

Operação do TCP

- **Endereçamento de Aplicações**
  - **Estabelecimento de Canais Virtuais**
  - Devido à possibilidade de existência de vários destes canais, cada aplicação recebe um número lógico de identificação denominado "Port". O endereço de um "Port" é entregue a uma dada aplicação apenas quando esta vai iniciar um canal.
  - Sendo assim, um endereço de canal virtual TCP corresponde não apenas a um endereço IP, mas a este somado ao número do Port utilizado para o canal virtual.

Operação do TCP

- **Endereçamento de Aplicações**
  - Número de 16 bits (source / destination port)
  - Possibilita a multiplexação/demultiplexação pelo TCP.
  - Servidores de aplicação possuem número de porta bem-conhecido ("well-known ports"). O protocolo TCP reserva um conjunto de Ports a algumas aplicações já conhecidas, sendo que, por convenção, o número de Ports alocados previamente não devem ser superiores a 256. A maioria deles fica disponível ao sistema operacional para alocá-los segundo as necessidades das aplicações.

Operação do TCP

- **Endereçamento de Aplicações**

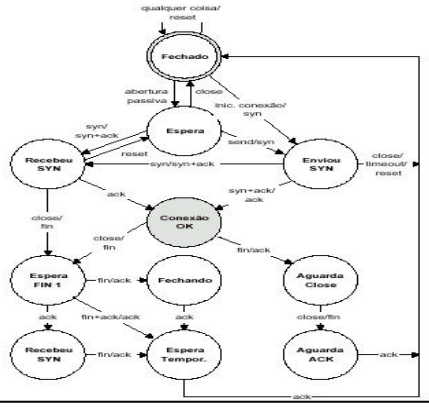
Port	Pal. Chave	Descrição
20	FTP-DATA	Dados do protocolo FTP
21	FTP	File Transfer Protocol (protocolo FTP)
23	TELNET	Conexão remota via terminal
25	SMTP	Simple Mail Transport Protocol (correio eletrônico)
79	FINGER	finger

O Protocolo TCP

- **Endereçamento de Aplicações**

Serviço	Protocolo	Porta
Systat	TCP	11
File Transfer (FTP)	TCP	20, 21
Telnet	TCP	23
Simple Mail Transfer (SMTP)	TCP	25
Access Control (TACAS)	UDP	49
Domain Name (DNS)	TCP, UDP	53
Trivial Transfer (TFTP)	UDP	69
Finger	TCP	79
HyperText Transfer (HTTP)	TCP	80
Post Office (POP)	TCP	109,110
Portmapper	TCP, UDP	111
Identification (auth)	TCP	113
Network News (NNTP)	TCP	119
Network Time	UDP	123
Simple Management (SNMP)	UDP	161,162
Remote Exec (rexec)	TCP	512
Remote login (rlogin)	TCP	513
Remote shell (rsh)	TCP	514
Routing (RIP)	UDP	520
X Window	TCP	6000-6063

O Protocolo TCP



O Protocolo UDP

- **O Protocolo UDP (User Datagram Protocol)**
  - Provê um serviço de transmissão NÃO-CONFIÁVEL e NÃO-ORIENTADADO A CONEXÕES. IDEAL PARA REDES LOCAIS.
  - Não utiliza mensagens de reconhecimento.
  - Não ordena mensagens que chegam.
  - Não possui mecanismo de controle de fluxo.
  - Extremamente simples.
  - Possui um checksum que engloba o cabeçalho e a área de dados.
  - Possibilita, através do uso de "ports", endereçar diferentes processos de aplicação.

O Protocolo UDP

- **O Protocolo UDP (User Datagram Protocol)**
  - Foi definido para ser utilizado por aplicações que não gerem um volume muito alto de dados na INTERNET.
  - Alguns protocolos definidos no Nível de Aplicação da arquitetura INTERNET (como por exemplo, o SNMP, o BOOTP e o TFTP) utilizam este protocolo.

O Protocolo UDP

- **O Formato do Cabeçalho UDP**

UDP Source Port	UDP Destination Port
UDP Message Length	UDP Checksum
DATA	
...	

O Protocolo UDP

- **O Formato do Cabeçalho UDP**
  - **UDP Source Port e Destination Port**
    - São dois campos de 16 bits que identificam o número do Port alocado para as aplicações origem e destinatária.
  - **UDP Message Length**
    - Campo de 16 bits, especifica o tamanho total do datagrama UDP (cabeçalho + dados).
  - **UDP Checksum**
    - Este campo transporta o Checksum. O Checksum é calculado levando em conta o cabeçalho e a área de dados.

Comparação OSI e TCP/IP

- **Pontos em comum entre os modelos OSI e TCP/IP**
  - Ambos são baseados em uma pilha (Stack) de protocolos independentes.
  - A funcionalidade das camadas é de modo geral similar. Por exemplo, em ambos os modelos as camadas de Transporte tem como objetivo fornecer um serviço de transporte fim a fim independente da rede aos processos que desejam se comunicar.
  - Em ambos, as camadas superiores, acima do Transporte, estão voltadas para as aplicações de usuário.

Comparação OSI e TCP/IP

- **Diferenças entre os modelos OSI e TCP/IP**
  - **Modelo OSI:** A conceituação do modelo OSI está centrada em torno de 3 conceitos fundamentais:
    - Serviços: Define o que a camada faz, não como as entidades acima a acessam ou como a camada funciona
    - Interfaces: Define como os processos acima acessam a camada. (também não diz como funciona a camada)
    - Protocolos: Os protocolos *peer to peer* usados na camada são próprios da camada. Podem ser quaisquer desde que realizem os serviços e funções da camada. Mudanças nos protocolos não afetam os níveis superiores.

Comparação OSI e TCP/IP

- **Diferenças entre os modelos OSI e TCP/IP**
  - **Modelo TCP/IP:** não distingue claramente entre;
    - Serviços
    - Interface e
    - Protocolo
  - Ultimamente tenta-se retroagir em relação a isto para tornar o modelo mais parecido com o modelo OSI. Por exemplo os únicos serviços oferecidos pela camada internet são: Send IP packet e Receive IP packet

Porque Entrar na Internet?

- Pelo mercado que se abre
- Para fazer contatos
- Para anunciar seu negócio interativamente
- Para prestar serviços aos clientes
- Para atrair a atenção do público
- Para publicar informação estratégica
- Para vender produtos ou serviços
- Para disseminar fotografias, som ou filmes
- Para alcançar um segmento de mercado altamente desejável

Porque Entrar na Internet?

- Para responder a perguntas mais freqüentes
- Para estar em contato direto com os vendedores
- Para alcançar mercados internacionais
- Para oferecer serviços 24 horas por dia
- Para tornar informação volátil disponível
- Para estimular o intercâmbio com clientes
- Para prover novos produtos e serviços
- Para impactar os meios de comunicação
- Para atingir o mercado educacional e juvenil
- Para alcançar mercados especializados
- Para atender seu próprio mercado local

Exercícios

- Como o TCP trata duplicação de mensagens?
- Como o TCP trata perda de pacotes?
- Como é feito o controle de fluxo entre máquinas de diferentes velocidades utilizando TCP?
- O que significa a filosofia "positive acknowlegdment with retransmission"?
- Uma conexão de transporte TCP é dita "full-duplex". Explique porque.
- No que consiste o mecanismo de "ackpiggybacking" utilizado pelo TCP e porque ele melhora o desempenho do protocolo?
- É necessário ao usuário configurar o tempo de "timeout" de uma conexão TCP? Porque?

Exercícios

- O que significa o conceito de "well known port"? Como este conceito o afetaria se você desejasse fazer uma aplicação que executasse diretamente "em cima" do protocolo TCP, comparando com a possibilidade de desenvolver a mesma aplicação em Java ou CGI.

PARTE 4

FERRAMENTAS E APLICAÇÕES

O que vamos ver?

- **Modelo Cliente-Servidor**
- **Domínios**
- **Protocolos de Aplicação**
- **Administração**
- **Diagnóstico de Redes**

O Modelo Cliente X Servidor

- **Introdução**
  - Os protocolos de aplicação que se utilizam do TCP/IP seguem o modelo cliente/servidor.
- **O Modelo Cliente X Servidor**
  - Servidor está sempre esperando em um número de porta bem conhecido.
  - O cliente possui número de porta variável, escolhida normalmente de forma aleatória.
  - O servidor aceita requisições e executa os serviços solicitados.
  - Cliente envia requisições e espera pela resposta.

O Modelo Cliente X Servidor

- **Funções do Cliente:**

1. Criar uma conexão TCP com o servidor;
2. Receber dados de entrada do usuário de uma maneira conveniente;
3. Reformatar os dados de entrada para algum formato padrão e enviá-lo para o servidor;
4. Receber dados de saída do servidor em algum formato padrão;
5. Reformatar os dados de saída para mostrá-los ao usuário.

O Modelo Cliente X Servidor

- **Funções do Servidor:**
  - O software servidor é executado na máquina que entrega o serviço, se o servidor não está rodando, o serviço fica indisponível.
  - Nos sistemas UNIX, servidores são freqüentemente referenciados como *daemons,* processos que rodam em "background".
  - Um protocolo de aplicação geralmente permite ao cliente e servidor fazer diferenciações entre dados destinados ao usuário, e mensagens que o cliente e o servidor utilizam para comunicar entre si.

O Modelo Cliente X Servidor

- **Funções do Servidor:**

1. Informa aos softwares de rede que está apto à receber conexões;
2. Espera que uma solicitação de serviço em um formato padrão ocorra;
3. Atende a solicitação;
4. Envia o resultado de volta ao cliente em um formato padrão;
5. Permanece em espera.

O Sistema de Nomes do Domínio

- **Histórico**
  - Inicialmente só se usavam números para identificar os computadores da rede. Era difícil decorar os endereços, usá-los e divulgá-los.
  - Hoje todas as aplicações da INTERNET permitem que os servidores sejam identificados por nomes ao invés de endereços numéricos.
  - Deve-se garantir que dois computadores ligados a INTERNET não possuam o mesmo nome.
  - É preciso também definir um modo de converter nomes em endereços numéricos, uma vez que os computadores definitivamente preferem os números.

O Sistema de Nomes

- **Histórico**
  - No início, o NIC (Network Information Center) fez um registro de nomes e endereços. Este arquivo, chamado arquivo de *hosts*, era regularmente distribuído a todas as máquinas da rede.
  - À medida que a INTERNET foi crescendo, o controle deste arquivo foi tornando-se proporcionalmente mais complexo. Também muito tempo de rede era gasto para distribuir este grande arquivo para todas as máquinas na rede.

O Sistema de Nomes

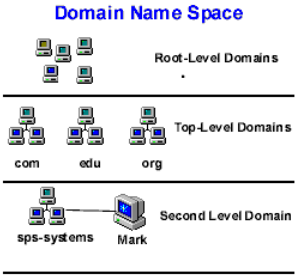
- **O DNS - Sistema de Nomes de Domínio**
  - Um sistema on-line era necessário para enfrentar esta grande taxa de mudanças. Este sistema é chamado de DNS (Domain Name System).
  - O Sistema de Nomes de Domínio é um método para administrar nomes dando diferentes grupos de responsabilidade para subconjuntos de nomes.

O Sistema de Nomes

- **O DNS - Sistema de Nomes de Domínio**
  - Cada nível neste sistema é chamado de um *domínio.* Os domínios são separados por pontos. Por exemplo:
    - inf.ufsc.br
    - npd.ufsc.br
    - ux.cso.uiuc.edu
    - nic.ddn.mil
    - yoyodyne.com

O Sistema de Nomes

- **O DNS - Sistema de Nomes de Domínio**



O Sistema de Nomes

- **O DNS - Sistema de Nomes de Domínio**
  - Nível Raiz: Domínios definem diferentes níveis de autoridade numa estrutura hierárquica.O topo da hierarquia é chamada de nível raiz.
  - Primeiro Nível (Top-level): Domínios .com, .edu, .org, .net, .gov, .mil e códigos de duas letras de países.
  - Segundo Nível: Domínios que podem conter tanto hosts como outros domínios chamados "sub-domínios".
  - Nomes de hosts são adicionados à esquerda no início do domínio, formando o "FULLY QUALIFIED DOMAIN NAME".

O Sistema de Nomes

- **O DNS - Sistema de Nomes de Domínio**
  - No Brasil, por determinação do Conselho Gestor (CG) da Intenet no Brasil, o órgão responsável pelo registro e manutenção dos domínios sob a terminação .br é a Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP). Todas as informações pertinentes à registro e alteração de domínios podem ser encontradas em **http://www.registro.br**.

O Sistema de Nomes

- **O DNS - Sistema de Nomes de Domínio**
  - Antes de solicitar o registro propriamente dito, é preciso se cadastrar na página www.registro.br, preenchendo um formulário on-line.
  - Em seguida, é necessário certificar-se de que o nome pretendido está disponível.
  - A partir daí o solicitante tem 10 dias para procurar um provedor de acesso para que o mesmo forneça o endereço IP onde o domínio ficará hospedado.
  - Cada registro implica o pagamento de 2 taxas de R$50, sendo uma no ato de registro e outra anual para manutenção.

O Sistema de Nomes

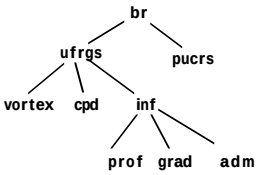
- **O DNS - Sistema de Nomes de Domínio**
  - Pode existir um número variável de domínios dentro do nome, mas é usual existirem 5 ou menos. À medida que se avança da esquerda para a direita através do domínio, o número de nomes contidos no grupo aumenta.
  - Cada grupo pode criar ou modificar qualquer configuração dentro dele. Seuiuc decidir criar outro grupo chamado ncsa, poderia ser feito sem pedir permissão a ninguém.

O Sistema de Nomes

- **O DNS - Sistema de Nomes de Domínio**
  - Tudo o que se tem a fazer é adicionar o novo nome para sua participação na base de dados mundial. Similarmente, cso pode comprar um novo computador, associar um nome e adicioná-lo a rede sem pedir permissão a ninguém. Se qualquer grupo do edu fizer uso das regras e certificar-se que os nomes que eles associaram são únicos, então dois sistemas, de qualquer lugar da INTERNET, não terão o mesmo nome. Você pode ter duas máquinas chamadas fred, mas apenas se elas estiverem em domínios diferentes (por exemplo, fred.cso.uiuc.edu e fred.ora.com).

O Sistema de Nomes

- **O DNS - Sistema de Nomes de Domínio**
  - **Exemplo:**



vortex.ufrgs.br
inf.ufrgs.br
bio.ufrgs.br
prof.inf.ufrgs.br

Consulta ao DNS

- Para converter um nome em um endereço numérico o computador começa a pedir ajuda aos servidores DNS, começando pela esquerda.
- Primeiro ele pergunta ao servidor local para que este consulte o endereço. Neste ponto existem três possibilidades:
  - o servidor local conhece o endereço, porque o endereço está na parte do servidor local da base de dados mundiais.
  - o servidor local conhece o endereço porque alguém já pediu pelo mesmo endereço recentemente.
  - O servidor local não conhece o endereço, mas sabe como encontrá-lo.

Consulta ao DNS

- Como o servidor local encontra o endereço? O seu software sabe como contactar um servidor raiz ou *root*.
- Este é o servidor que conhece o endereço de servidores de nomes para a zona mais à direita do nome.
- Ele pergunta ao servidor root pelo endereço do computador responsável pela zona à direita.

Consulta ao DNS

- Tendo essa informação ele contacta aquele servidor e pede à ele o endereço do servidor à esquerda. O seu software contacta então com aquele servidor e pede pelo endereço do servidor à esquerda.
- Finalmente ele contacta aquela máquina e pega o endereço do host que era o alvo da aplicação.

Consulta ao DNS

- **Exemplo Didático**
  - Tomemos como exemplo um servidor recém instalado que somente conhece o servidor raiz e tem que resolver uma consulta para encontrar o número IP do servidor www.embratel.net.br.
  - O servidor envia uma consulta para o primeiro Servidor Raiz de sua lista e recebe a informação que quem atende o domínio .br são os servidores:

NS.DNS.br internet address = 143.108.23.2
NS1.DNS.br internet address = 200.255.253.234
NS2.DNS.br internet address = 200.19.119.99
NS3.NIC.FR internet address = 192.134.0.49

Consulta ao DNS

- **Exemplo Didático**
  - Ele envia então uma consulta para o primeiro servidor dessa lista e recebe a informação que quem atende o domínio .net.br são os servidores:

NS.DNS.BR internet address = 143.108.23.2
NS2.DNS.BR internet address = 200.19.119.99
NS1.DNS.BR internet address = 200.255.253.234

Consulta ao DNS

- **Exemplo Didático**
  - Ele envia então outra consulta e recebe a informação de que o domínio .embratel.net.br é atendido por:

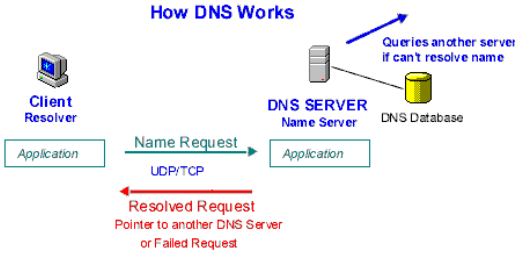
NS2.embratelnet.br internet address=200.245.255.33
NS.embratel.net.br internet address=200.255.253.241

  - Finalmente ele envia a consulta para o primeiro desses e recebe o número IP de www.embratel.net.br como resposta:

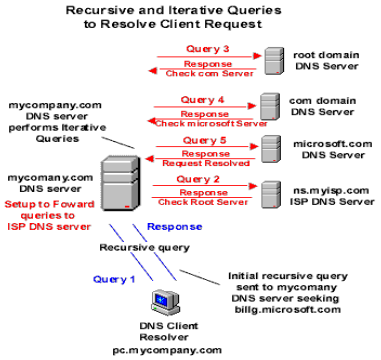
Name: rjo02.embratel.net.br
Address: 200.255.253.238
Aliases: www.embratelnet.br

Consulta ao DNS

- **Exemplo Didático**



Consulta ao DNS



Transferência de Arquivos

- **O FTP - File Transfer Protocol**
  - FTP é o nome dado ao programa que implementa o protocolo FTP : *File Transfer Protocol*. Como o nome indica, a tarefa do protocolo é mover arquivos de um computador para outro.
  - Não importa onde os computadores estão, como eles estão conectados, ou qual sistema operacional eles estão usando.
  - FTP foi implementado em um grande número de bases de dados. Pode-se encontrar nestas bases de dados desde receitas a programas ou importantes documentos.

Transferência de Arquivos

- **O FTP - File Transfer Protocol**
  - Permite a um usuário:
    1. conectar-se a uma máquina remota
    2. identificar-se
    3. listar os diretórios da máquina remota
    4. copiar arquivos de/para a máquina remota
    5. executar alguns comandos simples (ex.: solicitar help).

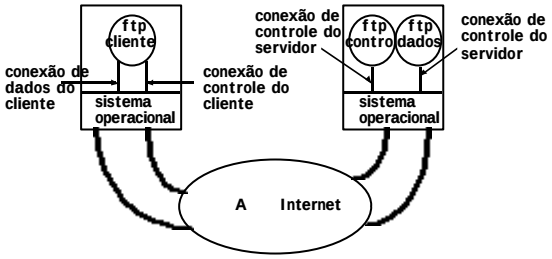
Transferência de Arquivos

- **O FTP - File Transfer Protocol**
  - **Sumário dos comandos:**

Comando	Função
ascii	modo de transferência ASCII
binary	modo de transferência binário
bye	finaliza sessão ftp
cd *[diretório-remoto]*	troca o diretório remoto de trabalho
close	finaliza uma sessão ftp
dir *[diretório]*	lista completa do diretório
help *[comando]*	imprime informações sobre o comando
lcd *[diretório]*	troca o diretório local de trabalho
ls *[diretório]*	lista simplificada do diretório
mget *lista-de-arquivos*	"pega" múltiplos arquivos
mput *lista-de-arquivos*	"coloca" múltiplos arquivos
open *nome-da-máquina*	conecta-se uma máquina remota
pwd	imprime o diretório corrente
quit	finaliza todas as conexões e termina o ftp
user *nome-do-usuário*	envia o nome de usuário à máquina remota

Transferência de Arquivos

- **O FTP - File Transfer Protocol**
  - **Conexões TCP**



Emulação de Terminal

- **O Telnet**
  - Telnet é usado para permitir um usuário logar em outros computadores na INTERNET. Também é usado para ter acesso a uma grande variedade de serviços públicos, incluindo catálogos de bibliotecas e outros tipos de bases de dados.
  - A conexão pode ser para uma máquina na mesma sala, no mesmo campus, ou em um computador em um lugar qualquer do mundo.
  - A partir do momento que o usuário está conectado, é como se o seu teclado e seu terminal de vídeo estivesse conectado diretamente ao computador remoto. A sua máquina passa a emular um terminal da máquina remota.

Correio Eletrônico

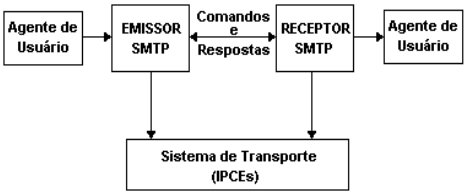
- **O Correio Eletrônico**
  - Correio eletrônico difere de outras aplicações (como ftp e telnet) porque não é necessariamente um serviço fim-a-fim -- o remetente e o destinatário não precisam estar ambos na INTERNET para fazer a comunicação.
  - Correspondência é passada de uma máquina para outra até finalmente chegar no destino.
  - Semelhante ao serviço postal convencional.

Correio Eletrônico

- **O SMTP: (Simple Mail Transfer Protocol)**
  - Possui basicamente três entidades: Agente do Usuário, Emissor-SMTP e Receptor-SMTP.
  - É orientado a conexão, sendo transmitido sobre TCP.
  - A comunicação entre Emissor-SMTP e Receptor-SMTP é feita através de comandos formados por sequências de caracteres no padrão ASCII.
  - Apenas alguns dos comandos tem implementação obrigatória em um servidor básico: HELO, MAIL, RCPT, DATA,NOOP,QUIT e RSET

Correio Eletrônico

- **O SMTP: (Simple Mail Transfer Protocol)**



Servidor de Arquivos

- **O NFS: (Network File System)**
  - Sistema operacional de rede desenvolvido pela Sun Microsystem's (1984).
  - Desenvolvido para ser usado em ambientes UNIX, mas atualmente suporta ambientes heterogêneos
  - Tornou-se padrão de gerenciamento para sistemas de arquivos distribuídos.
  - OBJETIVO:
    - Fornecer transparência de localidade de arquivos e hierarquias;
    - Permitir que usuários compartilhem arquivos na rede.

Servidor de Arquivos

- **O NFS: (Network File System)**
  - **CARACTERÍSTICAS:**
    - Independência de Sistema Operacional;
    - Acesso transparente;
    - Conserva a semântica do UNIX para acesso a arquivos;
    - Observa o paradigma Cliente X Servidor;
      - Servidor NFS oferece seu sistema de arquivos a outras máquinas (export)
      - Cliente NFS utiliza sistema de arquivos de outras máquinas (mount ou import)
    - Utiliza RPC (Remote Procedure Call).

Servidor de Arquivos

- **O NFS: (Network File System)**
  - Uma máquina pode ser:
    - Cliente e servidor (máquinas com disco)
    - Cliente (máquinas sem disco - diskless)
    - Servidor (máquinas com disco)
  - Um servidor pode servir vários clientes;
  - Um cliente pode acessar vários servidores.

Servidor de Arquivos

- **O NFS: (Network File System)**
  - Uma máquina pode ser:
    - Cliente e servidor (máquinas com disco)
    - Cliente (máquinas sem disco - diskless)
    - Servidor (máquinas com disco)
  - Um servidor pode servir vários clientes;
  - Um cliente pode acessar vários servidores.

Aplicações e Idéias para sua Dissertação

- **O QUE PODEMOS FAZER COM A INTERNET.**
- **Colaboração**
  - Interação entre indivíduos ou grupos de indivíduos remotamente localizados entre si, para cooperar em alguma atividade específica
  - Exemplos:
    - consultoria médica entre especialistas de diferentes partes do país
    - revisões técnicas entre especialistas
    - encontros eletrônicos
    - Pode envolver a interação bidirecional de dados, voz e imagem

Aplicações e Idéias para sua Dissertação

- Colaboração é usada em:
  - Telecomutação
  - Organizações virtuais
  - Desenvolvimento ou engenharia cooperativa
  - Telemedicina
  - Consultoria médica
  - Autoria de artes, música ou literatura
  - Entretenimento: TV interativa, jogos

Aplicações e Idéias para sua Dissertação

- Colaboração é usada em:
  - Compartilhamento de informação: Murais , grupos de discussão
  - Fábricas, lojas e escolas virtuais
  - Comunicação interpessoal:voz, video,Fax, correio eletrônico
  - Pesquisa científica e técnica
  - Aplicações governamentais

Aplicações e Idéias para sua Dissertação

- Conjunto de processos que podem ser impactados pela Internet
  - Saúde pública
  - Educação
  - Governo
  - Produção

Aplicações e Idéias para sua Dissertação

- Diagnósticos e Laudos Remotos
- Educação a Distância
- Bibliotecas Virtuais
- Acesso a Informações Governamentais
- Monitoração Ambiental
- Produção Automatizada
- Produçaõ Integrada
- Just-in-Time

Aplicações e Idéias para sua Dissertação

- Filmes por Demanda
- Escritórios Virtuais
- Empresas Virtuais
- Escolas Virtuais
- Lojas Virtuais
- Bancos Virtuais
- Processamento Altamente Paralelo e Distribuído

Administração

- **Utilitários de Linha de Comando (Windows)**
  - **arp-** arp.exe é utlizado para mapear um endereço IP para seu endereço de hardware. Primeiramente a cache de ARP local é verificada antes de enviar um ARP REQUEST em broadcast.
    - Opções
    - -a - View the contents of the local ARP cache table
    - -s - Add a static Arp entry for frequent accessed hosts
    - -d - Delete a entry

Administração

- **Utilitários de Linha de Comando**
  - **ipconfig –** é um utilitário para NT que mostra como a pilha IP está configurada.
    - **C:\ipconfig**

      Windows NT IP Configuration:

      Ethernet adapter E100B1:

      IP Address .....:198.133.234.23

      Subnet Mask .....:255.255.255.0

      Default Gateway.....:198.133.234.2

    - **Opções**
    - **/all - Extra information is revealed; IP host name, DNS, WINS server**
    - **/release - If DHCP is enabled, you release the lease with this switch.**
    - **/renew - The renew switch will update and renew DHCP lease information from the DHCP Server.**

Administração

- **Utilitários de Linha de Comando**
  - **netstat –** Mostra estatísticas dos protocolos e o estado atual de conexões TCP.
    - **Opções**
    - **-a - Displays all connections and listening ports.**
    - **-e - Displays Ethernet statistics. This may be combined with the -s option.**
    - **-n - Displays addresses and port numbers in numerical form.**
    - **-p proto - Shows connections for the protocol specified by proto; proto may be TCP or UDP. If used with the -s option to display per-protocol statistics, proto may be TCP, UDP, or IP.**
    - **-r - Displays the routing table.**
    - **-s - Displays per-protocol statistics. By default, statistics are shown for TCP, UDP and IP; the -p option may be used to specify a subset of the default.**

Administração

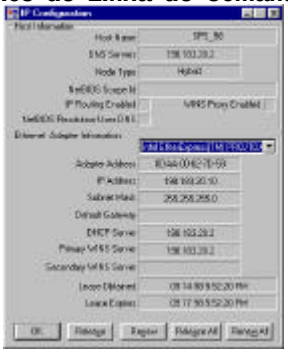
- **Utilitários de Linha de Comando**
  - **nbtstat –** Verifica o estado do NetBIOS sobre conexões TCP/IP e retorna o nome da sessão netbios e estatísticas de resoluçaõ de nomes.
    - **NBTSTAT [-a RemoteName] [-A IP address] [-c] [-n] [-r] [-R] [-s] [S] [interval]]**
  - Observação: Netstat funciona para conexões TCP/IP e Nbtstat funciona para conexões NetBIOS.

Administração

- **Utilitários de Linha de Comando**
  - **nslookup –** É utilizada para rastrear transações de DNS do começo ao fim.
  - **ping -** Ping.exe verifica configurações e testa conectividade através do envio de mensagens ICMP de "ECHO REQUEST".
  - **tracert –** Mostra a rota que um pacote percorre na rede de um computador a outro.
  - **winipcfg –** É uma versão GUI para Windows 95/98 do ipconfig.

Administração

- **Utilitários de Linha de Comando**



PARTE 5

CONCEITOS BÁSICOS DE INTRANET

O que vamos ver?

- **Introdução**
- **Motivação**
- **Classes de Intranets**
- **Modelos Organizacionais**
- **DHCP e WINS**
- **Roteamento (Windows®)**

Intranets

- **Introdução**
  - O interesse das ferramentas INTERNET como meio de comunicação e troca de informações atingiu grande popularidade.
  - Empresas cogitaram da possibilidade de sua utilização não apenas para o ambiente externo, mas também para o próprio ambiente da empresa.
  - A idéia era, disponibilizar informações e ferramentas de acesso já conhecidas da INTERNET para fins de comunicação interna numa organização.
  - Nasceu assim o conceito de Intranet, ou seja, uma INTERNET privada, onde os produtores e os consumidores de informação seriam os próprios profissionais da empresa.

Motivações

- Valor de mercado de uma empresa está se desvinculando do seu patrimônio físico e migrando para um parâmetro associado a capacidade de processar eficientemente informações, de modo a permitir à empresa se adaptar rapidamente e a baixo custo às mudanças do mercado.
- O correto tratamento das informações dentro das empresas assume uma importância cada vez maior no contexto atual, uma vez que é através deste parâmetro que as empresas coordenam suas atividades e atingem seus objetivos.

Motivações

- Nos últimos anos, o tratamento de informações nas empresas era feito por sistema proprietários de alto custo e nem sempre adaptáveis às mudanças que ocorriam dentro da empresa ou do seu próprio negócio (o mercado).
- Dependendo da especialidade da organização, um único sistema de gerenciamento de informações é na maior parte das vezes, incapaz de manipular toda a diversidade de informações existente de modo eficiente.

Motivações

- **Problemas para o tratamento de informações**
  - **Geração e Consumo de Informação**
    - Quem gera e quem consome?
  - **Diversidade da informação**
    - Utilização de várias mídias.
  - **Tempo de vida**
    - Depende do documento.
  - **Acesso e Confidencialidade**
  - **Rapidez de acesso**
  - **Padronização**
    - Forma de acessar amigável e constante.

Intranets como Sistema de Informação

- **Definição:**
  - Uma Intranet pode ser definida como uma infra-estrutura de comunicação baseada em padrões já consolidados da INTERNET e os serviços advindos do ambiente World Wide Web.
  - O que diferencia uma Intranet da INTERNET é, principalmente, o fato de que esta, apesar de fazer uso da tecnologia da grande rede, integra apenas usuários que estejam, de alguma forma, vinculados à organização considerada, sejam estes profissionais, fornecedores ou clientes.

Características e Vantagens

- É possível disponibilizar informações sobre marketing, pessoal, benefícios, política corporativa, etc., dentro e fora da instituição ou organização, para que funcionários, clientes, parceiros e pessoas afins tenha acesso às informações que lhes são convenientes e úteis.
- Em uma Intranet, o conhecido navegador Web torna-se um "cliente universal", capaz de fornecer acesso a uma variedade de bancos de dados e arquivos por meio do servidor web corporativo.
- Muitas páginas (home-pages) servem como ligação aos documentos e dados.

Características e Vantagens

- Menor Custo
  - Utiliza a tecnologia já disponível para Internet.
- Suporte à Heterogeneidade
  - Browsers multiplataforma.
- Facilidade de uso
  - Interfaces intuitivas e de fácil aprendizado.
- Escalabilidade
  - Desde dezenas até milhões de documentos.
- Padronização
  - A plataforma Web é neutra e global.

Serviços Disponíveis

- **Serviços de Recursos Humanos**
  - Manuais de empregados, informações sobre planos de saúde, folha de pagamento, planilha de férias, cardápio de restaurante, relatórios e boletins.
- **Serviços Logísticos e de Materiais**
  - Listas de mobiliário e imobilizados, Estoque e produtos de consumo do almoxarifado, mapas e plantas das edificações, etc.
- **Serviços de Sistemas de Informações**
  - Informações sobre dúvidas e sugestões de clientes obtidas de centrais de atendimento, dados de vendas, projeções, arquivos de dados para participantes de um projeto, "templates", etc.

Perfil do Usuário

- **A definição dos usuário de uma rede deste tipo é nitidamente diferente daqueles que acessam a a home-page de uma organização através da Internet.**
- **A maioria dos usuários são funcionários e pessoas relacionadas à organização.**
- **Estas pessoas estão a procura de informações que auxiliem e simplifiquem o seu trabalho.**
  - Bases de Dados e documentos de um setor;
  - Normas e procedimentos;
  - Informações sobre projetos;
  - Situação do estoque;
  - Boletins, etc.

Classes de Intranets

- **Intranet Estática**
  - Nesta classe de Intranet as informações da organização estão disponíveis em servidores Web na forma de documentos estáticos (são apenas cópias de documentos que já existiam na corporação em outras mídias).
  - As informações estão codificadas em páginas HTML e sua atualização implica na edição destas páginas.
  - Os usuários tem acesso às informações através do uso de browsers.
  - Informações Típicas:
    - políticas e procedimentos internos, regimentos, etc.

Classes de Intranets

- **Intranet Dinâmica**
  - Nesta classe de Intranet as informações da organização estão integradas em bases de dados que são acessadas pelos usuários dinamicamente em tempo-real.
  - Os usuários passam a ter acesso a e/ou templates que interagem com a base de dados e executam consultas.
  - Passa-se a interagir diretamente com as informações armazenadas na base de daos, não se limitando a consultar documentos estáticos.

Classes de Intranets

- **Intranet Transacional**
  - Esta classe de Intranet é uma evolução do modelo dinâmico que implementa mecanismos para efetuar transações seguras na Intranet.
  - Além de produzir informações dinamicamente, oferece ao usuário a possibilidade de realizar transações comerciais que envolvam movimentação financeira.

Modelos Organizacionais

- **Modelo Centralizado**
  - Neste modelo, todos os servidores Web são centralizados em um único sistema de computadores uma ou poucas máquinas confinadas em um único local).
  - Uma pessoa ou um grupo de pessoas fica como responsável pela configuração e administração do servidor e pela gerência dos serviços da Intranet.

Modelos Organizacionais

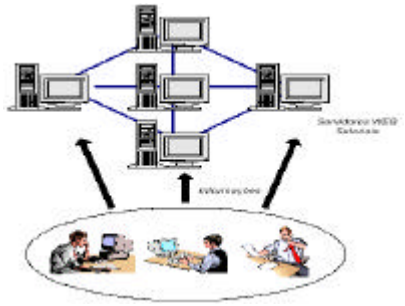
- **Modelo Centralizado**

Modelos Organizacionais

- **Modelo Distribuído**
  - Neste modelo, vários pontos de serviço são criados, cada um com o seu responsável.
  - Se existe necessidade de publicação de nova informação ou alteração, esta poderá ser feita pelo próprio usuário.
  - A principal vantagem deste modelo é a que ele permite que quem possua uma informação a compartilhar o faça rapidamente e com um mínimo de burocracia.
  - Esta também é a sua maior desvantagem, pois a anarquia e o caos pode tomar conta da rede.

Modelos Organizacionais

- **Modelo Distribuído**

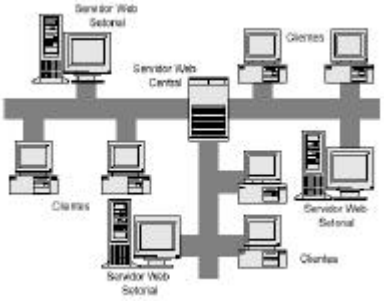


Modelos Organizacionais

- **Modelo Misto**
  - Este modelo procura unir as vantagens dos dois modelos anteriores.
  - Parte da organização é centralizada levando a uma maior padronização e controle da hierarquia.
  - Há uma distribuição de responsabilidades, com vários outros servidores setorizados de forma a impedir que uma falha do sistema paralise todos os serviços.

Modelos Organizacionais

- **Modelo Misto**



Implementando Intranets

- Em boa parte das empresas, a grande maioria da infra-estrutura necessária para o desenvolvimento de uma Intranet já existe.
- Uma outra parte a ser adquirida pela corporação pode ser obtida a custos irrelevantes ou mesmo sem custo algum.
  - Exemplos: softwares clientes, plug-ins, ferramentas de autoria, etc.
- Por outro lado, a implantação de uma Intranet, como qualquer tarefa de engenharia, não pode ser encaminhada de modo leviano, sob o risco de não se atingir o objetivo principal da tecnologia, que é o de promover benefícios no dia-a-dia da empresa.

Implementando Intranets

- As tecnologias da Intranet estão sendo vistas como a base para o desenvolvimento de sistemas de informações corporativos, enquanto os desenvolvedores não estão poupando esforços para produzir novos produtos ou para adaptar seus softwares à Internet.
- Esta avalanche de criatividade está trazendo enormes benefícios às organizações que procuram por produtos de fácil uso, baratos e escaláveis, a fim de criar um poderoso sistema de informações e cooperação dentro da corporação.

Implementando Intranets

- Uma das vantagens da adoção das Intranets é o fato de que a maior parte das empresas já dispõe de uma infra-estrutura de hardware que pode servir de ponto de partida para a implementação de um tal sistema.
- **A REDE FÍSICA**
  - Um dos benefícios da tecnologia Intranet é a possibilidade de aproveitamento da infra-estrutura de rede que existente na corporação.
  - Os protocolos TCP/IP são suportados pela maioria dos tipos de redes locais, incluindo Ethernet, LocalTalk, Novell e Token Ring.
  - A maioria dos equipamentos de interconexão, como bridges, roteadores e switchs também suportam os protocolos TCP/IP.

Implementando Intranets

- **MÁQUINAS SERVIDORAS E CLIENTES**
  - Uma grande variedade de plataformas de hardware para servidores estão disponíveis para satisfazer as diferentes necessidades das corporações.
  - As plataformas variam desde servidores de baixo custo e de fácil configuração, para uso de grupos de trabalho departamentais, até servidores poderosos baseados no sistema operacional Unix ou Windows NT, para uso na construção de backbones.
  - Independente da combinação de servidores usados por uma corporação, os serviços padrão oferecidos por eles podem ser utilizados por qualquer cliente em uma estação de trabalho, desktop ou laptop, ou ainda em palmtops.

Implementando Intranets

- **COMPONENTES DE SOFTWARE**
  - Protocolos de Rede
    - As Intranets são construídas tendo como base estrutural os protocolos TCP/IP.
  - Sistemas Operacionais de Rede
    - O sistema operacional de rede é o software que gerencia os recursos e controla a operação da rede.
    - Cada servidor da Intranet terá um SOR que suporta sua plataforma de hardware.
      - Windows NT, Novell Netware, Solaris Internet Server, etc.

Implementando Intranets

- **COMPONENTES DE SOFTWARE**
  - Aplicativos Intranet
    - Browsers Web, capazes de manipular páginas HTML (tecnologia utilizada para representar a maior parte de informações da Intranet) e suportar as principais linguagens da Intranet (como Java, JavaScript, ActiveX, etc...).
    - Aplicações para manipulação de e-mail.
    - Aplicações para manipulação de newsgroup.
    - Aplicações para troca de arquivos.
    - Aplicações para áudio e videoconferência.

Servidor DHCP

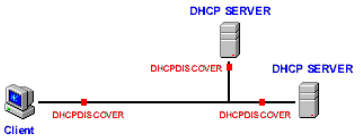
- **Definição**
  - O DHCP (Dynamic Host Configuration Protocol) é utilizado para associar automaticamente parâmetros TCP/IP para máquinas clientes.
  - Os endereços IP vêm de um "pool" chamado SCOPE e que é definido na base de dados do servidor DHCP.
  - O servidor garante um endereço IP associado a um cliente por um período de tempo chamado LEASE.

Servidor DHCP

- **Processo de Configuração DHCP – 4 passos**
  1. IP LEASE REQUEST
     - O cliente primeiro inicializa uma pilha limitada do conjunto de protocolos TCP/IP e se prepara para receber o "empréstimo" de um endereço IP do servidor DHCP da rede.
     - Através de um broadcast o cliente solicita este "empréstimo".
     - Esta requisição é enviada em uma mensagem DHCPDISCOVER, que contém o endereço de hardware (MAC address) do cliente e seu nome.

Servidor DHCP

- **Processo de Configuração DHCP – 4 passos**
  1. IP LEASE REQUEST

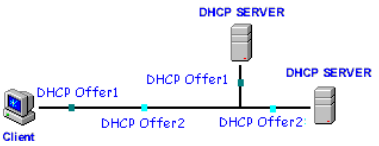


Servidor DHCP

- **Processo de Configuração DHCP – 4 passos**
  2. IP Lease Offer
     - O servidor DHCP envia uma mensagem DHCPOFFER em broadcast para o cliente.
     - O cliente pegará o primeiro IP que ele receber.
     - Se exitirem vários servidores DHCP na rede, os outros oferecimentos serão ignorados.

Servidor DHCP

- **Processo de Configuração DHCP – 4 passos**
  2. IP Lease Offer

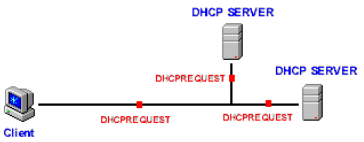


Servidor DHCP

- **Processo de Configuração DHCP – 4 passos**
  3. IP Lease selection
     - Depois que o cliente recebeu a oferta ele envia uma mensagem em broadcast para todos os servidores DHCP dizendo que já aceitou uma oferta.
     - Esta mensagem chamada DHCPREQUEST inclui o endereço IP do servidor cujo oferecimento foi aceito.
     - Todos os outros servidores retiram as suas ofertas.

Servidor DHCP

- **Processo de Configuração DHCP – 4 passos**
  3. IP Lease selection

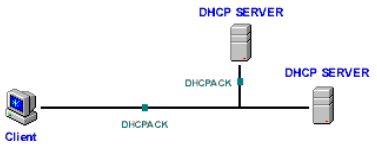


Servidor DHCP

- **Processo de Configuração DHCP – 4 passos**
  4. IP Lease selection
     - O servidor DHCP manda em broadcast um ACK para o cliente em uma mensagem DHCPACK, contendo um endereço IP emprestado válido.
     - Após receber o ACK, o cliente é plenamente inicializado e guarda o empréstimo em um registro.

Servidor DHCP

- **Processo de Configuração DHCP – 4 passos**
  4. IP Lease selection



Servidor DHCP

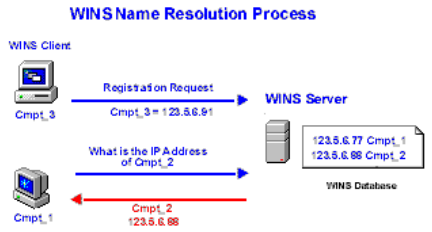
- **Renovação do empréstimo de endereço DHCP**
  - 1a. Tentativa de Renovação do empréstimo
    - **Após 50% do tempo do empréstimo.**
  - 2a. Tentativa de Renovação
    - **Imediatamente após se a 1a. Tentativa falhar.**
  - 3a. Tentativa
    - **Após 87,5% do tempo do empréstimo.**
  - Após 100% do tempo, se não houve renovação, o processo recomeça do início.

Servidor WINS (Windows®)

- WINS é um servidor de nomes NetBIOS da Microsoft.
- WINS elimina a necessidade de broadcasts para converter nomes de computadores em endereços IP.
- Um servidor WINS pode ser configurado tanto com WINS como com DNS para que possam conjuntamente resolver nomes NetBIOS e nomes qualificados apenas para clientes Microsoft.
- WINS é uma base de dados dinâmica, de forma que a resolução de nomes seja sempre atual e não necessite ser alterada manualmente como um arquivo lmhost.

Servidor WINS (Windows®)

- **Processo de Resolução de Nomes**



Servidor WINS (Windows®)

- **Processo de Registro de Nomes**
  - Quando um cliente WINS inicializa, ele registra seus nome NetBIOS mandando uma mensagem de "name request" para o servidor WINS configurado.
  - Todos os serviços ficam registrados a medida que são inicializados na base de dados do servidor WINS.
  - Se o servidor WINS está operando e o nome ainda não foi registrado por outra máquina, o servidor retorna umamensagem de "registration successful".

Servidor WINS (Windows®)

- **Processo de Registro de Nomes**

Roteamento (Windows®)

- **Windows® NT e Roteamento**
  - **Multihoming**
    - Um computador "multihomed" funciona como um roteador, isto é, possui duas ou mais placas de rede para duas ou mais sub-redes.
    - Multihome = possui lar em mais de uma sub-rede.
    - WINS manipula computadores multihomed e entradas também podem ser adicionadas no arquivo lmhost do computador.

Roteamento (Windows®)

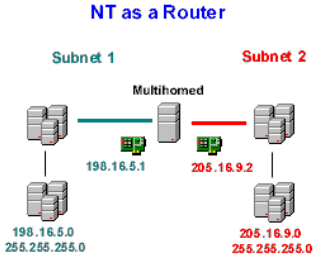
- **Windows® NT e Roteamento**
  - **Quando fazer Multihoming**
    - Muitas vezes esta pode ser a maneira mais fácil e barata para conectar duas ou mais redes.
    - Servidores de arquivo e de impressão, usados conjuntamente pelas diferentes sub-redes podem melhorar o desempenho da rede e ocupar a carga dos roteadores.

Roteamento (Windows®)

- **Windows® NT e Roteamento**
  - **Relembrando...**
    - O IP usa uma tabela de roteamento para descobrir para onde (por qual sub-rede) um pacote deve ser enviado.
    - Existem dois tipos de roteamento:
    - **Estático:** Não troca informações de roteamento com outros roteadores, utilizando apenas uma tabela de roteamento interna pré-programada.
    - **Dinâmico:** Aprende sobre alcançabilidade de outras redes utilizando algum dos muitos protocolos de roteamento, tais como RIP (Routing Internet Protocol) ou OSPF (Open Shortest Path First)

Roteamento (Windows®)

- **Windows® NT e Roteamento**
  - **Roteamento Estático**



Roteamento (Windows®)

- **Windows® NT e Roteamento**
  - **Roteamento Estático**
    - Na figura anterior, o roteador NT conhece as sub-redes 1 (198.16.5.0) e 2 (205.16.9.0).
    - Todos os hosts na sub-rede 1 usarão 198.16.5.1 como "default gateway".
    - Todos os hosts na sub-rede 2 usarão 205.16.9.2 como "default gateway".

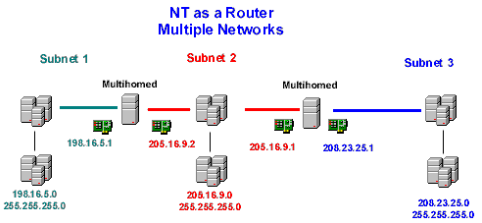
Roteamento (Windows®)

- **Windows® NT e Roteamento**
  - **Roteamento Estático**
    - **route –** utilitário utilizado para configurar roteadores estáticos.

route add [network] mask [netmask] [gateway] - Adds a route
route -p add [network] mask [netmask] [gateway] - Adds a persistent route.
route delete [network] [gateway] - Deletes a route.
route change [network] [gateway] - Modifies a route
route print Displays routing table.
Route -f - Clears all routes.

Roteamento (Windows®)

- **Windows® NT e Roteamento**
  - **Roteamento Estático**



Roteamento (Windows®)

- **Windows® NT e Roteamento**
  - **Roteamento Estático**
    - **Router 1-2**

Route -p -add 208.23.25.0 mask 255.255.255.0 205.16.9.1

- **Router 2-3**

Route -p -add 198.16.5.0 mask 255.255.255.0 205.16.9.2

Roteamento (Windows®)

- **Windows® NT e Roteamento**
  - **Roteamento Dinâmico**
    - Windows NT 4.0 suporta apenas o protocolo de roteamento RIP.

PARTE 6

FERRAMENTAS DE AUTORIA

Ferramentas de Autoria

- **Introdução**
  - Após construir a Intranet, será necessário fornecer ferramentas aos usuários para que eles desenvolvam conteúdo para ela.
  - Várias ferramentas de autoria Web estão disponíveis e ajudam na criação e publicação de conteúdo na Intranet.
  - Além disso, vários programas geram a saída no formato HTML e vários incluem utilitários de conversão que permitem converter o conteúdo existente em HTML.

Ferramentas de Autoria

- **Introdução**
  - Também será necessário fornecer aos desenvolvedores as diretrizes para criação e publicação de páginas Web, além de *templates* de páginas para maximizar a eficácia da comunicação da corporação.
  - Por fim, existem várias ferramentas de desenvolvimento de aplicações independentes de plataforma para a Intranet. Com elas é possível criar *scripts* CGI (*Common Gateway Interface*) que possibilitam a interação do *site* Web com as bases de dados corporativas, ou criar *applets*, com a linguagem Java, que podem ser disponibilizados em toda Intranet.

Linguagens de Autoria

- Antes de discutir algumas ferramentas conhecidas para autoria na Web, é importante apresentar algumas características das principais linguagens utilizadas para o desenvolvimento de páginas de uma Intranet.

Linguagens de Autoria

- ***Hypertext Markup Language - HTML***
  - É a linguagem nativa da Web.
  - Foi desenvolvida no final dos anos 80 na Suíça, por Tim-Berners Lee, com o objetivo de permitir a exibição de informações.
  - É uma linguagem de hipertexto baseada em marcadores (ou tags) que permitem definir os elementos que comporão a página.
  - Possibilita a definição de links (ou hiperlinks) que estabelecem um vínculo com uma nova página ou com uma seção da mesma ou de outra página, dando ao documento construído, a característica de hipertexto.

Linguagens de Autoria

- ***Hypertext Markup Language - HTML***
  - O aprendizado é simples, apresentando recursos para a introdução de imagens e associação de outros objetos (por exemplo, som ou vídeo) numa página Web
  - Oferece mecanismos para a criação de formulários para preenchimento on-line.

Linguagens de Autoria

- ***Java***
  - É uma linguagem desenvolvida pela Sun e que tem ganho, a cada dia, mais espaço na implementação de páginas Web.
  - Como linguagem de programação, Java é relativamente simples, muitas vezes apresentada como um subconjunto de C++.
  - A principal característica é a possibilidade de migração (via rede) de seu código e da sua execução nas mais diversas plataformas.

Linguagens de Autoria

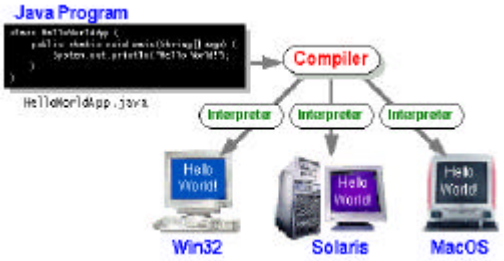
- ***Java***
  - Sua execução é baseada na geração de um código intermediário, denominado "bytecode", que é incorporado a páginas Web, transferido via rede no momento do carregamento da página.
  - Uma vez transferido para a máquina do usuário, este código é executado (através de um mecanismo de interpretação) por uma "máquina virtual Java", instalada no computador do usuário.
  - Para usuários da Web, a máquina virtual está embutida nos navegadores, como Netscape Communicator e Internet Explorer.

Linguagens de Autoria

- ***Java***
  - Desta forma, as aplicações Java escritas pelo autor de uma página Web serão executadas, sem a necessidade de adaptações, na maior parte das plataformas de hardware existentes na Web.
  - Por ser uma linguagem interpretada e por haver a necessidade de ser transferida via rede, o carregamento de uma página contendo aplicações Java (ou applets) normalmente se mostra mais lenta do que uma página HTML.

Linguagens de Autoria

- ***Java***



Linguagens de Autoria

- ***Java - Exemplo***
  - O exemplo a seguir mostra como construir um programa simples em Java.
  - Com isto, pretende-se mostrar alguns elementos da linguagem e um roteiro para consrução de aplicações.
  - O passos para a criação de um programa em Java envolvem os seguintes passos:
    - Criação de um arquivo fonte em Java.
    - Compilação do arquivo fonte.
    - Execução do programa.
    - Criação de um *Applet*.

Linguagens de Autoria

- *Java - Exemplo*
  - **Criação de um arquivo fonte em Java.**
    - Um arquivo fonte contém texto, escrito na Linguagem de Programação Java usando qualquer editor de textos, que pode ser entendido pelo programador e por outras pessoas.

```
/**
 * The HelloWorldApp class implements an application that
 * simply displays "Hello World!" to the standard output.
 */
class HelloWorldApp {
    public static void main(String[] args) {
        // Display "Hello World!"
        System.out.println("Hello World!");
    }
}
```

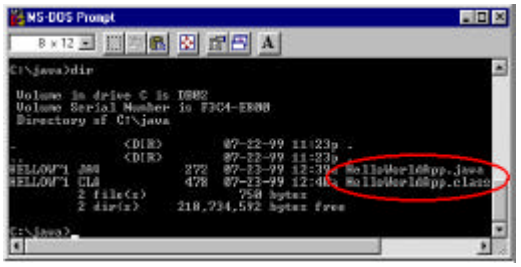
Linguagens de Autoria

- ***Java - Exemplo***
  - **Compilação do arquivo fonte em um arquivo bytecode.**
    - O compilador Java (javac) transforma o texto do arquivo fonte em instruções que podem ser entendidas pela Máquina Virtual Java (Java VM).

```
C:\javac HelloWorldApp.java
```

Linguagens de Autoria

- ***Java - Exemplo***
  - **Compilação do arquivo fonte em um arquivo bytecode.**



Linguagens de Autoria

- ***Java - Exemplo***
  - **Execução do programa.**
    - O interpretador da Máquina Virtual Java manipula o arquivo bytecode, transformando as instruções ali contidas em instruções executáveis pelo computador hospedeiro.

C:\java HelloWorldApp

Resultado

Linguagens de Autoria

- ***Java - Exemplo***
  - **Criação de um *Applet*.**
    - A criação de Applet Java chamado HelloWord, permite que, ao contrário da implementação anterior, o programa execute em um browser Web que possua embutido um interpretador Java, tal como o Netscape, o Microsoft Internet Explorer, etc.
    - Para criar este applet procederemos aos mesmos passos básicos vistos anteriormente: criação do arquivo fonte, compilação e execução do programa.

Linguagens de Autoria

- ***Java - Exemplo***
  - **Criação de um *Applet*.**
    - Criação do programa fonte e da página html que chamará o applet:

```
import java.applet.*;
import java.awt.*;
/**
 * The HelloWorld class implements an applet that
 * simply displays "Hello World!".
 */
public class HelloWorld extends Applet {
    public void paint(Graphics g) {
        // Display "Hello World!"
        g.drawString("Hello world!", 50, 25);
    }
}
```

Linguagens de Autoria

- ***Java - Exemplo***
  - **Criação de um *Applet*.**
    - Criação do programa fonte e da página html que chamará o applet:

```
<HTML>
<HEAD>
<TITLE>A Simple Program</TITLE>
</HEAD>
<BODY>
Here is the output of my program:
<APPLET CODE="HelloWorld.class" WIDTH=150 HEIGHT=25>
</APPLET>
</BODY>
</HTML>
```

Elementos para Construção de Intranets Dinâmicas

- **Uma Intranet Dinâmica deve possuir as seguintes características:**
  - Integração com bases de dados ou outras aplicações;
  - Interatividade do usuário com o sistema;
  - Geração automática de páginas HTML a partir de resultados de consultas ou outros processamentos;
  - Presença eventual de mecanismos de segurança de acesso e confidencialidade (principalmente no caso das chamadas Intranets Transacionais);
  - Presença eventual de mecanismos de replicação de bases de dados em diversos servidores por questões de segurança e eficiência.

Elementos para Construção de Intranets Dinâmicas

- **Construção de Formulários**
  - **A delimitação de formulários na linguagem HTML é feita a partir do marcador FORM.**

```
<form>
...
</form>
```

  - **Na definição de um formulário, o autor pode definir alguns atributos informando o propósito do formulário:**

Atributo	Descrição
ACTION="URL"	Especifica a URL que vai processar o resultado
METHOD= GET | POST	Especifica o método de troca de dados com a ação

Elementos para Construção de Intranets Dinâmicas

- Construção de Formulários
  - Para a criação de entradas de dados, o autor têm à sua disposição uma variedade de tipos de campos. A definição de um campo é feita pelo marcador <INPUT>, onde os seguintes atributos podem ser definidos:

Atributo	Descrição
onBlur="função"	Aciona função quando o campo perde o destaque
onChange="função"	Aciona função quando os dados no campo mudam
onClick="função"	Aciona função quando é realizado um click do mouse
onFocus="função"	Aciona função quando o campo é destacado
onLoad="função"	Aciona função quando os frames são carregados
onMouseOver="função"	Aciona função quando o mouse é posicionado no campo
onSelect="função"	Aciona função quando o usuário seleciona texto do campo

Elementos para Construção de Intranets Dinâmicas

- Construção de Formulários
  - Exemplo

Elementos para Construção de Intranets Dinâmicas

- Construção de Formulários
  - Exemplo

```
<HTML>
<HEAD> <TITLE>Envie seu E-mail</TITLE> </HEAD>
<BODY TEXT="#000000" BGCOLOR="#CCCCCC">
<CENTER><B><FONT SIZE=+1>QUESTIONÁRIO</FONT></B></CENTER>
<BR>
<CENTER>Dê sua contribuição para o aprimoramento da disciplina enviando
suas sugestões.</CENTER>
<P><FORM method="POST" ACTION="mailto:mauro@inf.ufsc.br">
<B>Seu nome:</B>
<INPUT type="text" size="40" name="Nome" cols="60" rows="1"></INPUT>
<BR>
<BR><B>Seu e-mail:</B>
<INPUT type="text" size="40" name="Mail" cols="60" rows="1"></INPUT>
<BR>
```

Elementos para Construção de Intranets Dinâmicas

- Construção de Formulários
  - Exemplo - Continuação

```
<P><B>Sua área de atuação:</B>
<INPUT type="checkbox" name="Tipo" value="Engenharia">
<INPUT type="checkbox" name="Tipo" value="Computação">
<INPUT type="checkbox" name="Tipo" value="Administração"></INPUT>
<BR>
<BR><B> Escreva seus comentários</B>
<BR><TEXTAREA name="Comentários" rows=4 cols="60"></TEXTAREA>
<UL>
<CENTER><INPUT TYPE=submit VALUE="Enviar sugestões"><B>
</B><INPUT type=reset value="Limpar formulário"></CENTER>
</UL>
</BODY>
</HTML>
```

Elementos para Construção de Intranets Dinâmicas

- *Common Gateway Interface (CGI)*
  - Apesar de viabilizar a entrada de dados por parte dos usuários, os formulários não definem como esta informação poderá ser processada pelo sistema.
  - Para isto deve existir um mecanismo que permita o processamento das informações fornecidas pelo usuário.
  - Um dos mecanismo mais utilizados são os CGIs ou Common Gateway interfaces.

Elementos para Construção de Intranets Dinâmicas

- *Common Gateway Interface (CGI)*
  - As CGIs constituem-se numa interface para programas externos que irão interagir com servidores de informação, como por exemplo, os servidores Web.
  - Programas de CGI são utilizados comumente para o processamento de formulários, podendo ser escritos nas mais diversas linguagens (C, C++, shell scripts, Visual Basic e Perl).
  - Os programas CGI normalmente são armazenadosnum diretório especial designado pelo administrador da rede, isto por razões de segurança.

Elementos para Construção de Intranets Dinâmicas

- ***Common Gateway Interface (CGI)***
  - Os scripts CGI podem ser utilizados para as aplicações mais diversas.
  - Um exemplo corriqueiro de utilização deste mecanismo são os chamados contadores de acesso (ou hit counters), utilizados nas páginas Web para registrar o número de visitantes que uma página teve num dado período.

Elementos para Construção de Intranets Dinâmicas

- ***Common Gateway Interface (CGI)***
  - Entretanto, uma das aplicações mais importantes dos scripts CGIs é sem dúvida a possibilidade de acesso a registros de bases de dados, o que vai proporcionar à Intranet um nível de interatividade comparável aos dos Sistemas de Gerenciamento de Informações de natureza proprietária, com a vantagem de utilizar protocolos de comunicação padronizados, interfaces apropriadas ao negócio da empresa e de representar custos de instalação e manutenção relativamente mais baixos.

Elementos para Construção de Intranets Dinâmicas

- ***Common Gateway Interface (CGI)***
  - Independente do pacote de gerenciamento de bases de dados utilizado, a interação com o sistema é feita basicamento visando duas finalidades:
    - Encaminhamento de solicitações de consulta (eventualmente utilizando uma linguagem específica como SQL) e de comandos para o sistema de bases de dados;
    - Recepção e processamento do resultado da pesquisa.

Elementos para Construção de Intranets Dinâmicas

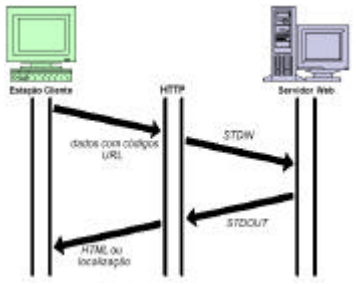
- ***Common Gateway Interface (CGI)***
  - Numa transação, existem praticamente três elementos envolvidos:
    - O navegador cliente, instalado na máquina do usuário, que vai acionar o programa CGI;
    - O protocolo HTTP, que é o protocolo a nível de aplicação que rege a comunicação entre servidores e clientes Web;
    - O script de gateway.

Elementos para Construção de Intranets Dinâmicas

- ***Common Gateway Interface (CGI)***
  - O servidor HTTP ativa o script de gateway solicitado, transferindo os dados num formato de entrada padrão, denominado *STDIN*, ou então sob a forma de variáveis de ambiente do servidor.
  - O script é então executado no servidor, produzindo eventualmente como saída um conjunto de dados a ser retornado para o cliente.
  - Estes dados são então transferidos via saída padrão, a qual é denominada STDOUT e, finalmente, entregues ao navegador sob a forma de código HTML.

Elementos para Construção de Intranets Dinâmicas

- ***Common Gateway Interface (CGI)***



Elementos para Construção de Intranets Dinâmicas

- ***Common Gateway Interface (CGI)***
  - **Exemplo**
    - Neste exemplo é mostrado um script CGI escrito em Perl capaz de gerar uma página HTML de resposta para a entrada do usuário.

Elementos para Construção de Intranets Dinâmicas

- ***CGI* - Exemplo - Continuação**

```
<HTML>
<HEAD>
<TITLE>Exemplo de CGI</TITLE>
</HEAD>
<BODY TEXT="#000000" BGCOLOR="#C0C0C0">
<B>PESQUISA SOBRE O FUTURO TÉCNICO DA SELEÇÃO</B>
<BR>
<HR WIDTH="100%">
<FORM METHOD="POST" ACTION="http://www.inf.ufsc.br/cgi-bin/proc.pl">
Digite seu nome<INPUT name="Nome">
<BR>
<HR WIDTH="100%">
Digite o nome do técnico que você deseja para a seleção <INPUT name="Coach">
<HR WIDTH="100%">
<BR><INPUT type="submit" value="Enviar"><INPUT type= "reset" value="Limpar">
</FORM>
</BODY>
</HTML>
```

Elementos para Construção de Intranets Dinâmicas

- ***CGI* - Exemplo - Continuação**

```
#!/bin/perl
use CGI;
$html = new CGI ;
Content-type: text/html \n\n
print "<HTML><HEAD></HEAD><BODY>Ok, ", $html->param('Nome') ,
"<BR>Seu voto em ",$html('Coach')," foi registrado!!!<P></BODY></HTML>\n" ;
```

Elementos para Construção de Intranets Dinâmicas

- ***CGI* - Exemplo - Continuação**
  - A primeira linha (**#!/bin/perl**) informa a localização, no sistema UNIX, do interpretador Perl (neste caso, no diretório **bin**). O objetivo desta linha é indicar que o script deverá ser interpretado pelo interpretados Perl e não pelos interpretadores de comandos do UNIX.
  - A linha **use CGI** informa a utilização de um módulo pré-escrito em Perl (**CGI.pm**)que permite tratar os parâmetros recebidos via http.
  - A linha seguinte (**$html = new CGI**), indica a declaração de uma variável que está relacionada ao uso do módulo CGI, para poder tratar os parâmetros enviados do navegador.

Elementos para Construção de Intranets Dinâmicas

- ***CGI* - Exemplo - Continuação**
  - A seguir, é definida uma linha para informar o tipo MIME do arquivo que deverá ser retornado ao navegador. Neste caso, será um arquivo de texto, formato html, o que é especificado pelo comando (Content-type: text/html)
  - Finalmente, o comando que vai gerar o texto html relativo ao arquivo. Isto é feito através de um comando de impressão, que gera os marcadores básicos de um documento html e que embute no texto os valores dos parâmetros que o usuário havia digitado na página html anterior.

PARTE 7

SEGURANÇA NA INTERNET

O que vamos ver?

- Introdução
- Tipos de Ataque
- Tipos de Atacantes
- Roteiro de Ataque
- Firewalls

Segurança na Internet

- Introdução
  - A Internet foi projetada visando fornecer conectividade entre computadores para uma comunidade restrita de usuários que confiavam mutuamente entre si.
  - Ela não foi projetada para um ambiente comercial, para tráfego de informações valiosas ou sensíveis, ou para resistir a ataques mal-intencionados.

Segurança na Internet

- Introdução
  - Durante a década de 80, antes da popularização da Internet, os computadores foram alvos de ataques individuais e isolados.
  - A solução adotada foi relativamente simples: incentivar os usuários a escolherem boas senhas, prevenir o compartilhamento indiscriminado de contas e arquivos e eliminar os *bugs* de segurança de programas como *sendmail, finger* e *login* à medida que eles iam sendo descobertos.

Segurança na Internet

- Introdução
  - **Na década de 90, entretanto, os ataques estão se tornando mais sofisticados e organizados:**
    - Senhas e outras informações importantes são capturadas por *network sniffers*.
    - Computadores são invadidos ou paralisados por ataques do tipo *IP spoofing*.
    - Sessões são desviadas através de *connection hijacking*.
    - Dados são comprometidos pela inserção de informação espúria via *data spoofing*.

Segurança na Internet

- Introdução
  - **Estes ataques são diretamente relacionados ao protocolo IP que não foi projetado para o ambiente atual da Internet:**
    - Embora projetado para ser tolerante à falhas de hardware, o IP não possui muita resistência contra ataques intencionais.
    - O IP não foi projetado para fornecer segurança; assumiu-se que esta tarefa seria realizada por protocolos de maior nível de abstração.

Segurança na Internet

- Introdução
  - IP está em permanente evolução; futuras versões provavelmente fornecerão a segurança e a confiabilidade requeridas. Esta caraterística, entretanto, também tem suas desvantagens, uma vez que o IP está sendo usado em ambientes para os quais não foi originalmente projetado.

Segurança na Internet

- **Introdução**
  - **Brechas na segurança de um sistema não constituem licença para agir de forma ilegal se aproveitando de tais lacunas.**
  - Acesso não autorizado constitui violação das regras na Internet, não importa quão frágil seja a segurança de um computador ou rede.
  - Legislação sobre acesso não autorizado começa a aparecer em vários países
    - USA Computer Fraud and Abuse Act of 1986, Title 188 U.S.C. section 1030 -- crime acessar sem autorização computadores governamentais e de instituições financeiras .

Segurança na Internet

- **Introdução**
  - Projeto de lei que tramitou no congresso brasileiro
  - Art. 4o. Toda rede de computadores cujo acesso é oferecido ao público, ou a uma comunidade restrita, mediante remuneração de qualquer natureza, deverá ter um administrador de rede legalmente constituído.

Segurança na Internet

- **Introdução**
  - Art. 5o. O administrador de rede é responsável pelos serviços de rede, pela segurança do controle de acesso e pela proteção do equipamento do usuário contra operações invasivas de terceiros, intencionais ou não, nos termos contratuais estabelecidos com o usuário, respeitadas as disposições da Lei No. 8.078, de 11 de setembro de 1990, que "dispõe sobre a proteção do consumidor e dá outras providências".

Segurança na Internet

- **Introdução**
  - Art. 8o. O administrador da rede e o provedor de cada serviço são solidariamente responsáveis pela segurança, integridade e sigilo das informações armazenadas em bases de dados à consulta ou manuseio por usuários da rede.
  - Punições, que envolvem inclusive cadeia, tal como evidencia, entre outros o artigo 32:
  - Art. 32. Os administradores de redes integradas de computadores, os provedores de serviços e de informações que, no exercício da função, provocam desvio nas finalidades estabelecidas para o serviço.

Segurança na Internet

- **Abordagem Básica**
  - **O que vai ser protegido? Vale a pena?**
  - **Contra que tipo de ataque?**
  - **Quais os ataques prováveis ?**
  - Implementar mecanismos de proteção de modo eficiente e com custo aceitável.
  - Revisar o processo continuamente e aperfeiçoar os mecanismos de proteção cada vez que um ataque é percebido.
  - O custo de proteger contra um ataque deve ser menor do que o valor da perda se um ataque é realizado.

Segurança na Internet

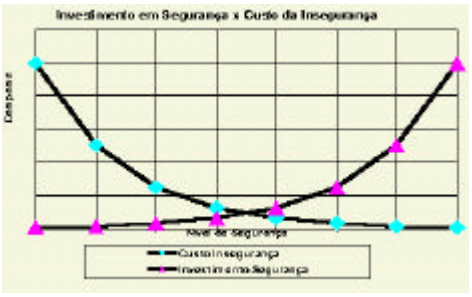
- **Identificando o Alvo**
  - **Hardware:** cpu, placas, teclados, terminais, estações de trabalho, PC, impressoras, unidade de disco, linhas, servidores de terminais, modems, repetidores, pontes e roteadores.
  - **Software:** programas fonte, programas objeto, utilitários, programas de diagnóstico, sistemas operacionais, programas de comunicação.
  - **Dados:** durante a execução, armazenado on-line, arquivados off-line, backups, trilhas de auditoria, BD, em trânsito na rede.

Segurança na Internet

- **Identificando o Alvo**
  - **Pessoas:** usuários, administradores.
  - **Documentação:** sobre programas, hardware, sistemas, procedimentos administrativos locais.
  - **Suprimentos:** papel, formulários, fitas de impressão, meio magnético.

Segurança na Internet

- **Mapeamento dos Riscos**



Segurança na Internet

- **Protegendo seus Dados**
  - **Sigilo**
    - Você não quer que outras pessoas acessem suas informações.
  - **Integridade**
    - Você não quer que outras pessoas as modifiquem.
  - **Disponibilidade**
    - Você deseja que elas estejam prontas para serem usadas.

Segurança na Internet

- **Protegendo seus Recursos**
  - Você não deseja que pessoas não autorizadas estejam utilizando sua CPU e seu espaço em disco.
  - Você gastou um bom tempo e dinheiro nos seus recursos computacionais, é seu direito determinar como eles serão utilizados.

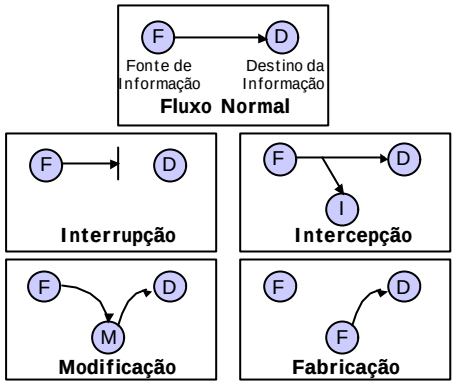
Segurança na Internet

- **Protegendo sua Reputação**
  - Você não quer que um intruso manipule seus dados ou seus recursos.
  - Você não quer que um estranho forje sua identidade.

Tipos de Ataques

- **Intrusão**
  - Atacantes utilizam seus computadores como se fossem usuários legítimos.
- **Roubo de informações**
  - Pode ser ativo ou passivo.
- **Negação de serviços (*denial of service*)**
  - Impedimento de você utilizar seus próprios recursos.

Ameaças na Segurança



Tipos de Atacantes

- **Curiosos**
  - São estudantes ou "micreiros" que passam o tempo navegando na Internet e procurando alguma coisa para se divertir.
    - Normalmente aprendem com os programas e ferramentas prontas que estão na Web e são facilmente pegos.

Tipos de Atacantes

- **In-House**
  - São funcionários ou ex-funcionários que procuram causar problemas para a empresa em que atuam ou atuaram.
    - São movidos por vingança, ou mesmo por dinheiro, e têm interesse em prejudicar a empresa em questão.

Tipos de Atacantes

- **Técnicos**
  - Normalmente são os que criam programas que causam danos, são extremamente bons no que fazem e espalham rapidamente suas novas técnicas através da Internet.
    - Pessoas problemáticas com dificuldade de integração na comunidade que trabalham pelo prazer da destruição.

Tipos de Atacantes

- **Profissionais**
  - **Criam novas ferramentas e também se utilizam do que já existe pronto. O diferencial é que são profissionais, ou seja, recebem pelo que fazem.**
    - Trabalham para grupos terroristas ou de espionagem industrial, normalmente são mais velhos, muito inteligentes e difíceis de serem pegos.

Pontos de Risco

- Pontos de acesso
- Enlaces
- Linhas discadas
- Servidores de terminais
- Sistemas mal configurados
- Bugs de software
- Acesso por pessoal interno

Principais Vulnerabilidades

- Má configuração dos serviços, o que permite a pessoas sem autorização ter acesso a dados confidenciais. Podem também causar a queda de todo o sistema caso recebam mais dados do que consigam tratar.
- Serviços não utilizam nenhuma forma de criptografia nos dados a serem transmitidos pela Internet. Dados confidenciais que trafegam pela Internet podem ser interceptados, incluindo senhas de usuários.
- Serviços utilizam mecanismos de autenticação fáceis de serem enganados. Enganando o sistema de autenticação, pessoas podem se passar por usuários legítimos ou máquinas confiáveis.

Principais Vulnerabilidades

- Implementação de clientes e servidores dos serviços apresentam *bugs*. Explorando estes *bugs*, pessoas podem executar ações às quais não têm permissão.
  - Ao longo dos anos, diversos *bugs* foram encontrados nos mais distintos produtos de diferentes fornecedores, sendo utilizados por atacantes para conseguir acesso.
  - É função dos fornecedores liberar versões que os corrijam, e é função dos administradores de sistemas implantá-las. Caso esta implantação demore, atacantes poderão se valer de *bugs* já divulgados e amplamente discutidos.

Segurança na Internet

- **Notícias**
  - Foi descoberta uma falha na segurança do software Mosaic, utilizado para armazenar informações em computadores ligados à World Wide Web.
  - A falha permite que os hackers tomem o controle dos servidores da Rede, fazendo com que haja o risco de a Rede tornar-se vulnerável ao ataque de "worms", programas automatizados que apagam sistematicamente instalações da Rede.

Segurança na Internet

- **Notícias**
  - "Esta é a primeira vulnerabilidade realmente seria da Rede.", comentou um cientista de computação do Computer Incident Advisory Capability, do Departamento de Energia.
  - O National Center for Supercomputing Applications da Universidade de Illinois, que criou o Mosaic, criou um software "remendo" que verifica o comprimento das strings de comando, desta forma impedindo que qualquer pessoa inclua uma linha extra com comandos potencialmente danosos.
    (Wall Street Journal 21/02/95 B8)

Segurança na Internet

- **Notícias**
  - **Exemplo: The WORM**
    - 2/nov/1988
    - Copiava a si mesmo de máquina a máquina
    - Carregava as várias máquinas infectadas preterindo o atendimento a outros usuários
    - MIT, NASA, US ARmy Ballistic Research Lab desconectaram-se da rede
    - Roberto Morris - 5 anos de prisao $ 250.000 jan/90

Segurança na Internet

- **Notícias**
  - **Active X control crashes Windos 95**
    - Information page with a link to a page which loads the control:
    - http:16/10/96/www.halcyon.com/mclain/ActiveX /
    - Exploder is an Active X control which demonstrates security problems with Microsoft's Internet Explorer.
    - Exploder performs a clean shutdown of Win95 and will turn off the power on machines that have a power conservation BIOS (green machines).

Segurança na Internet

- **Notícias**
  - **Novell HTTP server**
    - **If you are running the Novell HTTP server, please disable the CGI's it comes with it until you understand (fully understand) what the security risks are.**
    - **The CGI in question is convert.bas (yes, cgi's in basic, stop laughing).**
    - **A remote user can read any file on the remote file system using this CGI.**
    - **This means that if you are running the Novell HTTP server and have the 'out of box' CGI's, you are breached.**
    - **Exploit code:**
    - **http:16/10/96/victim.com/scripts/convert.bas?../../anything/you/want/to/view**

Roteiro de Ataque

1. Selecionar um alvo.
2. Coletar informações sobre alvo. Existem diversos métodos para conseguir informações sobre um alvo. Um ponto de partida é a utilização de serviços como finger, showmount e rpcinfo. Todas as ferramentas empregadas por administradores para gerenciamento são também de grande valor para o atacante. DNS, whois, sendmail, ftp e uucp são outros serviços que fornecem ao atacante valiosas informações durante a fase de obtenção de dados.

Roteiro de Ataque

3. Lançar um ataque sobre o alvo. Para tentar entrar em um sistema, o atacante utiliza vários métodos que exploram vulnerabilidades conhecidas de serviços, servidores e sistemas operacionais. Alternativamente, o atacante pode simplesmente tentar adivinhar senhas de usuários na máquina alvo.

Roteiro de Ataque

4. Destruir evidências da invasão. Geralmente, as ações realizadas pelo atacante para conseguir entrar na máquina ficam registradas em arquivos de log. É importante que eles sejam alterados de modo a encobrir estes passos e evitar sua análise pelo administrador do sistema.

Roteiro de Ataque

5. Obter senhas de outras contas. Quanto mais contas forem comprometidas pelo atacante melhor. Na maioria das vezes, um simples ataque do dicionário no arquivo */etc/passwd* é necessário para obtenção de um considerável número de senhas.

Roteiro de Ataque

6. Obter acesso *root* na máquina invadida. Tendo acesso a uma conta de usuário, o atacante terá direitos limitados. Assim, é importante conseguir acesso *root*, pois deste modo disporá de todo o sistema, empregando-o para realizar os passos seguintes e lançar futuros ataques. Para conseguir direitos *root*, atacantes podem empregar diversos métodos, explorando geralmente *bugs* existentes em programas.

Roteiro de Ataque

7. Instalar ferramentas para captura de senhas. Para isto, atacantes podem instalar monitores de rede ou cavalos-de-tróia. Entre os programas candidatos para serem substituídos por cavalos-de-tróia estão *login, telnet e ftp*. Caso estes estejam protegidos e sua alteração seja impossível, atacantes podem, ainda, explorar erros tipográficos dos usuários. Para isto, basta colocar programas chamado *telent* (ou *logn, fpt*, etc) em diretórios utilizados pelas vítimas.

Roteiro de Ataque

8. Configurar caminhos secundários de entrada na máquina invadida; para o caso da rota principal ser descoberta e fechada. Dispondo de direitos *root*, fica extremamente fácil para um atacante construir rotas alternativas para entrar no sistema. Entre elas estão a inserção de um novo usuário ou a reconfiguração de alguns serviços.

Roteiro de Ataque

9. Encontrar outras máquinas que confiam na máquina invadida. Para isto, basta analisar arquivos como *.rhosts* e *hosts.equiv*.
10. Utilizar a máquina invadida como base para lançar outros ataques.

Principais Formas de Ataque

- **Engenharia Social**
  - A engenharia social é um método de ataque que consiste em enganar as vítimas através do emprego de informações adquiridas por pesquisa.
  - O atacante se vale destas informações para induzir pessoas de boa fé a executam ações indevidas e perigosas.
  - O intruso pode utilizar-se de vários meios para lançar um ataque de engenharia social, sendo telefonemas e mensagens de correio eletrônico falsificadas os mais comuns.

Principais Formas de Ataque

- **Denial-of-Service**
  - Um ataque *denial-of-service* tem como objetivo impedir o uso legítimo do sistema. Para isto, um intruso inunda o sistema ou a rede com mensagens, processos ou requisições, de modo que nenhum trabalho possa ser realizado.
  - Muito difícil de impedir se uma máquina aceita conexões do mundo externo (correio eletrônico, FTP anônimo, etc).
  - É importante que se configure os serviços de modo que se um deles for inundado, o resto do site permaneça operacional.

Principais Formas de Ataque

- **Exploração de Bugs**
  - Uma das maneiras mais comuns de se conseguir acesso em um sistema é explorar furos de implementação presentes em programas e sistemas operacionais.
  - Quanto maior o seu tamanho, maior o número de bugs. Assim, máquinas expostas a ataques devem executar o mínimo necessário de programas, e estes, preferencialmente, devem ser bem escritos e exaustivamente testados.
  - A falha de apenas um componente é o suficiente para que o sistema inteiro seja comprometido por um atacante.

Principais Formas de Ataque

- **Exploração de protocolos**
  - O protocolo TCP/IP representa um risco de segurança simplesmente porque ele permite que usuários remotos acessem arquivos e dados de outros equipamentos.
  - Quando foi projetado, não foi levado em consideração o aspecto segurança, pois naquela época as pessoas envolvidas não tinham idéia de quão utilizado ele seria.
  - Atacantes exploram algumas de suas características para conseguir acesso não-autorizado em sistemas de computação. Muitos desses são derivados de falhas no mecanismo de autenticação.

Principais Formas de Ataque

- **IP Spoofing**
  - No *IP spoofing,* o atacante utiliza o endereço IP de uma máquina confiável juntamente com algum protocolo que faz autenticação baseada em endereços. Deste modo, este ataque permite que pessoas utilizando qualquer máquina se passem por usuários legítimos de uma máquina que é confiável em determinada rede.

Principais Formas de Ataque

- **IP Spoofing**
  - A idéia básica deste ataque é estabelecer uma conexão com o alvo, enganando o handshake inicial do protocolo TCP.
  - O principal ponto do sequence number attack é "adivinhar" o ISN (Initial Sequence Number) gerado pelo host alvo. Para isto,é utilizada uma característica da implementação do 4.2BSD Unix, juntamente com os protocolos TCP/IP.

Principais Formas de Ataque

- **IP Spoofing**
  - Sejam três hosts, X, S, C. O atacante está lançando o ataque a partir de X em S, personificando C, em quem S confia.
  - X retira de operação C, enchendo a porta 21 (canal de controle do FTP) com requisições de conexão.
  - X estabelece uma conexão real com S e grava o número inicial de seqüência retornado por S.
  - X envia um pacote SYN tendo como origem a porta 21 e destino porta 514 (servidor de execução remota). O endereço fonte contido no cabeçalho deste pacote é alterado para conter o endereço IP de C.

Principais Formas de Ataque

- **IP Spoofing**
  - S faz a autenticação da requisição de conexão baseada em endereço. S envia um pacote de resposta para C, que é ignorado pois C está fora de operação.
  - X envia um pacote ACK para S, com o número de seqüência "adivinhado", ou seja, o número previamente adquirido somado com 64.
  - X tem uma conexão legítima com S na porta 514.
  - X envia dados contendo um comando a ser executado em S.
  - S "pensa" que recebeu uma comando rsh (remote shell) de C, uma máquina confiável, executando-o.

Principais Formas de Ataque

- **IP Spoofing**
  - O ataque descrito acima se utiliza de uma característica de implementação, tendo êxito somente em máquinas que estejam utilizando o 4.2BSD Unix como sistema operacional.
  - Porém, existem generalizações que permitem ao atacante, com um pouco mais de trabalho, forjar conexões em qualquer outro host, independente do seu sistema operacional.
  - Para isto, o atacante deve fazer algumas conexões reais de teste, para tentar descobrir a lei de geração dos números de seqüência e conseguir predizê-lo na hora do ataque.

Principais Formas de Ataque

- **DNS Spoofing**
  - Em ataques ao DNS, a idéia básica do DNS Spoofing é subverter o servidor de nomes, e com isto permitir que máquinas não confiáveis (as do atacante) se passem por máquinas confiáveis.
  - Para lançar este ataque, o intruso deve ter inicialmente controle sobre o host servidor de DNS e saber o nome de uma máquina em quem o alvo confia. Com isto altera-se o registro do DNS que mapeia o endereço IP da máquina confiável para o seu nome, modificando-o para que contenha o endereço da máquina atacante.

Principais Formas de Ataque

- **DNS Spoofing**
  - A partir deste momento o intruso terá livre acesso em serviços que realizam autenticação baseada em nomes.
  - A maioria dos novos sistemas possuem métodos contra este tipo de ataque, utilizando para isto uma técnica conhecida com cross-check. Nela, o nome retornado pela consulta é submetido novamente ao serviço de nomes. Se o endereço utilizado para a conexão é diferente do retornado pelo cross-check, a conexão é abortada e uma violação de segurança é apontada.

Principais Formas de Ataque

- **Source Routing Attack**
  - Este ataque se utiliza dos mecanismos de roteamento disponíveis e da opção *loose source route* do protocolo IP para induzir a máquina alvo a acreditar que o ataque é, na realidade, uma operação legítima proveniente de uma outra máquina confiável.
  - A opção *loose source route* disponibiliza um mecanismo para que a origem de um datagrama possa fornecer informações de roteamento usadas pelos *gateways* para direcioná-lo ao destino. Deste modo um processo pode iniciar uma conexão TCP fornecendo um caminho explícito para o destino, sobrescrevendo o processo usual de roteamento.

Principais Formas de Ataque

- **Source Routing Attack**
  - Sejam três máquinas, X, A e B. Seja a situação em que o intruso em X lança um Source Routing attack em A que confia em B.
  - O intruso, com algum tipo de ataque, desestabiliza B, ou espera até que ela esteja desligada.
  - O intruso configura X para que contenha o endereço IP de B. Neste momento o atacante está personificando a máquina confiável.

Principais Formas de Ataque

- **Source Routing Attack**
  - O intruso utiliza rlogin ou rsh para acessar A. Para isto deve utilizar pacotes IP com opção loose source route ativada e corretamente configurada, contendo um caminho válido de X para A.
  - A aceita as requisições de X, pensando que elas são de B. A partir deste momento X detêm uma conexão legítima com A.
  - As respostas de A são enviadas para X através do caminho inverso descrito na opção loose source route dos datagramas recebidos por A.

Principais Formas de Ataque

- **Source Routing Attack**
  - Pode ser empregada, também, para alterar a rota dos pacotes e, deste modo, desviar dos sistemas de segurança de um domínio.
  - Duas defesas são:
    - utilizar versões dos servidores rlogin e rsh que não aceitam conexões com a opção loose source route ativada.
    - utilizar filtros de pacote que não permitam que pacotes com a opção ativada entrem no site. O uso deste enfoque é aconselhado porque o domínio pode disponibilizar outros serviços com autenticação baseada em endereços que não dispõem do mecanismo citado acima.

Principais Formas de Ataque

- **RIP**
  - Para que hosts em diferentes redes consigam se comunicar, é necessária a presença de um roteador (ou de um conjunto deles) cuja função é identificar o melhor caminho que um pacote deve seguir a fim de encontrar seu destino.
  - Inicialmente um roteador só conhece as redes a que está diretamente conectado, sendo as demais conhecidas através de rotas estáticas ou de protocolos de roteamento.

Principais Formas de Ataque

- **RIP**
  - Quando se utiliza protocolos de roteamento, informações são trocadas automaticamente entre roteadores e quaisquer mudanças de caminho são atualizadas dinamicamente.
  - Entre os protocolos de roteamento mais utilizados está o RIP (Routing Informatin Protocol) cujas atualizações são realizadas em intervalos de tempo fixos e pré-definidos e que geralmente não verifica a veracidade dos dados recebidos. Esta fragilidade do RIP pode ser utilizada por atacantes para enganar o sistema de roteamento.

Principais Formas de Ataque

- **RIP**
  - Em um ataque utilizando o RIP, o intruso consegue personificar uma máquina específica, através do envio de informações de roteamento falsas para gateways que envolvam caminhos entre o alvo e o atacante.
  - Deste modo pacotes destinados ao computador confiável são direcionados para a máquina do atacante.
  - O intruso deverá personificar uma máquina que, de preferência, esteja desligada, esteja à algum tempo em idle ou esteja inoperante, em virtude de algum ataque do tipo denial-of-service.

Principais Formas de Ataque

- **RIP**
  - Existe uma variante mais sutil e perigosa deste ataque. Nela, o atacante personifica uma máquina que está ativa. Deste modo, os pacotes do alvo para ela serão enviados para o atacante.
  - Neste momento eles poderão ser visualizados ou alterados pelo intruso. Após são enviados para o destino correto através de IP source address routing.
  - Já existem hoje em dia roteadores que aceitam o protocolo RIP versão 2, que especifica um melhoramento em diversos aspectos em relação ao RIP, incluindo autenticação nas mensagens de atualização.

Principais Formas de Ataque

- **ICMP**
  - O ICMP (Internet Control Message Protocol) é um protocolo utilizado para fazer a manutenção de conexões TCP/IP. Ele também é usado para gerar uma grande quantidade de ataques. Entres as mensagens ICMP mais exploradas por atacantes estão a redirect e destination unreachable.
  - A redirect é utilizada por gateways para avisar máquinas sobre melhores rotas. Os ataques produzidos com esta mensagem subvertem o sistemas de roteamento, se assemelhando aos ataques no RIP.

Principais Formas de Ataque

- **ICMP**
  - A mensagem destination unreacheable é utilizada para informar a um host que o destino da sua conexão não pode ser encontrado.
  - Esta mensagem pode ser enviada por um roteador, caso nenhuma rota para o destino esteja disponível, ou se a máquina destino for inexistente ou se está inativa.

Principais Formas de Ataque

- **ICMP**
  - A destination unreacheable pode, também, ser enviada pelo próprio host destino. Neste caso, o host está afirmando que a porta a que a conexão se refere não pode ser encontrada.
  - A destination unreacheable pode ser utilizada para terminar conexões específicas existentes e, deste modo, promover ataques do tipo denial-of-service.

Principais Formas de Ataque

- **Sniffers**
  - Na grande maioria das redes, os pacotes são transmitidos para todos os computadores conectados ao mesmo meio físico.
  - Entretanto, é possível reprogramar o interface de rede de uma máquina para que ele capture todos os pacotes que circulam pelo meio, não importando o destino.
  - O interface de rede que opera deste modo é dito em modo promíscuo, e esta técnica é denominada de sniffing.

Principais Formas de Ataque

- **Sniffers**
  - Como em um ambiente de rede normal trafegam pela rede muita informação sensível, como por exemplo nomes de usuários e senhas (username e passwords), fica fácil para um programa sniffer obter estas informações.
  - A utilização desniffers é difícil de ser detectada. Se ele estiver somente coletando dados e não respondendo a nenhuma informação.
  - Diversas medidas podem ser adotadas contra sniffers, mas a maioria delas requer o uso de hardware específico, como hubs ativos ou então interfaces de rede que não possuam modo promíscuo. No lado dos aplicativos, podem ser utilizados programas que utilizem criptografia.

Principais Formas de Ataque

- **Ataque do dicionário**
  - Um dos arquivos mais cobiçados por atacantes é o /etc/passwd, devido ao fato dele conter as senhas de todos os usuários de uma máquina ou rede.
  - As senhas são cifradas através de um algoritmo unidirecional, que não permite a reversão do texto cifrado novamente para o texto normal.

Principais Formas de Ataque

- **Ataque do dicionário**
  - O algoritmo, o crypt(3), é uma variante do DES (Data Encryption Standard), que usa a senha (de 8 caracteres) como chave decifragem. Para adicionar uma maior complexidade a este processo, ele é repetido 25 vezes. O resultado final, de 8 bytes, é transformado em 11 caracteres visíveis (cujo bit mais significativo é zero, e de onde se eliminam caracteres de controle).

Principais Formas de Ataque

- **Ataque do dicionário**
  - Para impedir que usuários com a mesma senha tenham o mesmo texto cifrado, o UNIX utiliza ainda uma pitada de sal (a grain of salt). A cada usuário é atribuído um número randômico de 12 bits, o salt number, cuja única finalidade é produzir saídas distintas para usuário distintos.
  - Quando um usuário efetua o login, o número salt é recuperado e utilizado juntamente com a password fornecida pelo usuário para gerar um texto cifrado. Se o texto resultante é igual ao texto armazenado, o usuário é autenticado como legítimo.

Principais Formas de Ataque

- **Ataque do dicionário**
  - A eficácia de todos estes cuidados fica comprometida pelo hábito das pessoas de utilizar senhas facilmente memorizáveis, como nomes próprios ou palavras de uso corriqueiro.
  - No ataque do dicionário, o atacante compõe um dicionário e, dispondo de suficiente poder de processamento, experimenta todas as palavras deste dicionário contra o texto cifrado armazenado no arquivo /etc/passwd.

Principais Formas de Ataque

- **Ataque do dicionário**
  - Se um usuário com número salt s possui como texto cifrado o string x, então no momento em que a palavra w do dicionário, em conjunção com o número s produzir como resultado x, então o atacante sabe que a senha correspondente é w.
  - Para impedir este ataque, os usuários devem ser conscientizados para não usarem palavras "fáceis", ou seja, que tenham grande probabilidade de constar em um dicionário. Boas sugestões são combinações de letras e números, uso de palavras com grafia errada, ou letras iniciais das palavras de uma frase.

Mecanismos de Proteção

- A definição de uma política de segurança é o primeiro passo para que se possa escolher e implementar quais os mecanismos de proteção serão utilizados.

Mecanismos de Proteção

- **É necessário que as seguintes questões sejam profundamente consideradas:**
  - o que se está querendo proteger?
  - o que é preciso para proteger?
  - qual a probabilidade de um ataque?
  - qual o prejuízo se o ataque for bem sucedido?
  - implementar procedimentos de segurança irá ser vantajoso no ponto de vista custo-benefício?

Mecanismos de Proteção

- **Quatro posturas definem os 4 P's da segurança:**
  - **Paranóico:** Tudo é proibido, mesmo aquilo que deveria ser permitido. Como regra, a conexão à Internet nunca deveria ter sido estabelecida.
  - ⇒ **Prudente:** Tudo que não é explicitamente permitido é proibido. É a melhor postura atual, apesar de requerer uma boa administração.
  - **Permissivo:** Tudo que não é explicitamente proibido é permitido. Esta era a postura até o início da década de 90.
  - **Promíscuo:** Tudo é permitido, inclusive o que deveria ser proibido.

Mecanismos de Proteção

- A política de segurança deve estar sempre sendo revisada, pois ao longo do tempo as necessidades se alteram.
- A segurança pode ser implementada a nível de *hosts* ou a nível de rede.
- Com segurança de *hosts*, cada máquina é protegida isoladamente. Este enfoque funciona bem quando implantado em domínios pequenos, mas normalmente é um processo complexo, demorado e caro tornar cada máquina segura.

Mecanismos de Proteção

- Na segurança a nível de rede, todas as máquinas de um domínio são protegidas por apenas um mecanismo que está presente entre os canais de comunicação que conectam máquinas internas com máquinas externas.
- Com a adoção deste enfoque, o domínio estará protegido independentemente da configuração e das vulnerabilidades das máquinas internas.

Mecanismos de Proteção

- **Estratégias de Segurança:**
  - ***least privilege*:** dar a usuários, administradores e programas somente os privilégios que são necessários para que suas tarefas sejam realizadas. Nunca se deve dar mais poder do que o necessário.
  - ***defense-in-depth*:** nunca confiar em somente um mecanismo para realizar a segurança. Utilizar dois ou mais mecanismos é uma boa alternativa pois implementa redundância. Caso um componente falhe, o sistema ainda estará protegido pela presença dos demais.

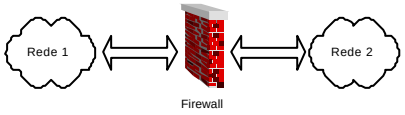
Mecanismos de Proteção

- **Estratégias de Segurança:**
  - ***choke point*:** força que toda a comunicação entre a rede interna e a Internet passe por apenas um canal. Neste canal devem estar presentes componentes de segurança e monitoramento a fim de torná-lo seguro.
  - ***weakest link*:** deve-se eliminar, ou se impossível, monitorar todos os pontos fracos do sistema.
  - ***fail-safe*:** caso um componente falhe, ele deve parar de funcionar de modo a não permitir o acesso do atacante. Até que seja consertado ele negará também acesso de pessoas autorizadas.

Mecanismos de Proteção

- **Firewalls**
  - Um *firewall* é um conjunto de componentes colocados entre duas redes e que coletivamente implementam uma barreira de segurança.
  - Um *firewall* pode ser considerado um *choke point* pois todo o tráfego entre as redes interna e externa (Internet) deve passar por ele.

Firewalls



Firewalls

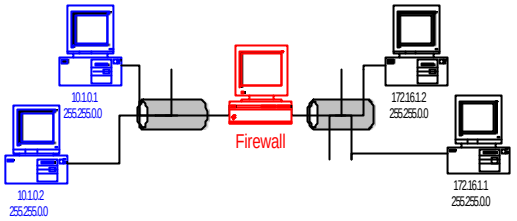
- **É um ótimo local onde aplicar a política de segurança.**
  - Por exemplo, se a política de segurança impede o uso de FTP para o exterior, todos os pedidos de conexão com servidores FTP externos serão filtrados pelo *firewall* e não serão passados para à Internet.

Firewalls

- **Para que servem?**
  - Controlar os serviços a serem disponibilizados.
  - Proteger uma rede de ataques externos.
  - Registrar a comunicação entre as máquinas internas e externas.
  - Esconder máquinas internas.
  - Converter endereços IP.
  - Criptografar e autenticar tráfego de dados.

Firewalls

- **Para que NÃO servem?**
  - Bloquear comunicação entre máquinas da mesma sub-rede.
  - Impedir ataques de pessoas internas.



Firewalls

- **Mecanismos de Implementação**
  - Normalmente um firewall pode ser implementado utilizando dois mecanismos: filtragem de pacotes e servidores *proxy*.
- **Servidores Proxy**
  - Servidores *proxy* são programas que "conversam" com servidores externos em nome dos clientes internos. Clientes *proxy* conectam-se em servidores *proxy* que conectam-se nos servidores reais. O servidor *proxy* recebe resposta do servidor real e a redireciona para o cliente*proxy*.

Firewalls

- **Filtros de Pacotes**
  - Filtros de pacote realizam um roteamento seletivo de pacotes.
  - Como roteadores normais, eles redirecionam o pacote analisando o endereço destino. Porém, com base em outros dados (endereço destino, endereço fonte, porta origem, porta destino) eles podem aceitar ou negar um pacote.
    - Caso o pacote seja aceito, o procedimento é o normal.
    - Caso ela seja negado o filtro de pacote simplesmente o descarta.

Firewalls

- **Filtros de Pacotes**
  - Filtros de pacote são uma maneira barata para se implementar a política de segurança.
  - Filtros de pacote são flexíveis, dando ao administrador a chance de realizar filtragens baseada em serviços ou endereços de máquinas.

Firewalls

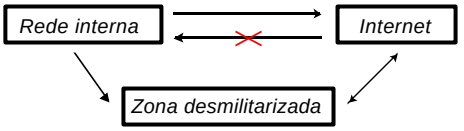
- **Filtros de Pacotes**
  - Realizando filtragem baseada em serviços ele pode, por exemplo:
    - permitir que usuários internos utilizem telnet para acessar hosts externos e impedir o inverso.
    - permitir que máquinas externas acessem o servidor de e-mail da organização e impedir acesso externo em serviços perigosos, como TFTP, NFS, rlogin, etc.
    - bloquear qualquer tráfego do interior para o exterior.

Firewalls

- **Filtros de Pacotes**
  - Com filtragem baseada em endereços, o administrador pode:
    - permitir qualquer tráfego proveniente da rede x.y.z.w que é considerada confiável pela política de segurança.
    - impedir a entrada de qualquer pacote cujo endereço representa uma máquina interna (esta regra impede a maioria dos ataques IP spoofing).
    - permitir que a máquina externa r.s.t.u.v se conecte no servidor de e-mail da organização. Esta regra é muito comum, e permite que um servidor de mail confiável faça a transferência das mensagens.

Firewalls

- **Técnicas de Proteção**
  - Zona Desmilitarizada
    - Utilizada para disponibilizar serviços com pouca confiabilidade.
    - Isola os serviços privados dos serviços públicos.

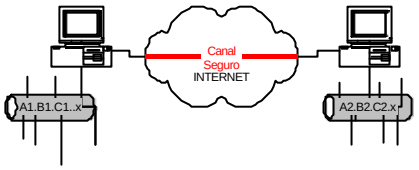


Firewalls

- **Técnicas de Proteção**
  - Conversão de Endereços (NAT)
    - Técnica utilizada para converter endereços IP de máquinas internas em tempo real.
    - Possibilita o acesso à Internet a partir de máquinas com endereços IP reservados.
    - Permite a existência de um número maior de máquinas internas do que o número de endereços IP válidos.
    - Feito de forma transparente.

Firewalls

- **Técnicas de Proteção**
  - Rede Virtual Privada (VPN)
    - Canal onde todo o tráfego de dados é autenticado e criptografado.
    - Pode existir a nível de rede ou aplicação.



Firewalls

- **Firewalls Comerciais**
  - Firewall-1 (Check Point)
  - Raptor Eagle (Axent)
  - Guardian (NetGuard)
  - Gauntlet (Network Associates)
  - Borderware (Secure Computing)
  - Firewall Aker

Mecanismos de Proteção

- **Mecanismos de autenticação**
  - A grande maioria dos serviços da Internet que necessitam identificar um usuário utilizam o mecanismo "alguma coisa que você sabe", ou seja, senhas.
  - Apesar de ser um método fácil, rápido e barato, a utilização de senhas é um grande problema de segurança, pois elas podem ser capturadas por sniffers ou descobertas por um ataque do dicionário.
  - Uma solução possível é utilizar senhas que não são reusáveis, como as one time passwords [Har96]. A senha ainda pode ser capturada, mas ela não terá nenhuma utilidade para o atacante.

Mecanismos de Proteção

- **Ferramentas de detecção de falhas**
  - **SATAN (Security Analysis Tool for Auditing Network):** é o sistema de auditoria mais completo disponível em domínio público. Ele pode ser utilizado em três modos (leve, normal e pesado), dependendo da profundidade da análise que se deseja. SATAN procura em todos os serviços oferecidos por erros de configuração e bugs conhecidos.
  - **COPS (Computer Oracle and Password Program):** outro sistema de auditoria, que inclui verificação do uso de passwords "fáceis".

Mecanismos de Proteção

- **Ferramentas de detecção de falhas**
  - **TIGER:** é um conjunto de scripts e programas que também visam a auditoria de um sistema, mas sua ênfase maior está em erros de permissões de arquivos.
  - **Tripwire:** é um analisador de integridade de arquivos e diretórios. Tem como objetivo detectar alterações indevidas, como as que ocorrem tipicamente em uma intrusão do sistema. Utiliza funções de hash unidirecionais, como MD5, SHA e CRC de 32 bits.
  - **Crack:** visa testar as senhas de um sistema Unix, realizando sobre elas o ataque do dicionário.

Mecanismos de Proteção

- **Ferramentas de detecção de falhas**
  - **Npasswd e Passwd+:** programas que realizam uma série de testes (programáveis) sobre as senhas no momento que os usuários as registram.
  - **Swatch (Simple Watcher):** monitora os arquivos de log e permite ao administrador realizar ações específicas em resposta à ocorrência de diversos eventos.
  - **Trimlog:** gerencia arquivos de log.

Mecanismos de Proteção

- **Métodos criptográficos**
  - O fato da informação trafegar pela rede em forma clara permite que um intruso qualquer capture pacotes e leia esta informação
  - Uma maneira de impedir este tipo de ataque é utilizar métodos criptográficos. Alguns sistemas que utilizam estes métodos são listados a seguir:

Métodos Criptográficos

- A Criptografia tem sido utilizada a séculos (ou mesmo milênios), para proteger informações "sensíveis" quando elas são transmitidas de um local para outro.
- Em um sistema criptográfico, a mensagem é criptografada utilizando uma chave.
- O texto cifrado (ciphertext) é então transmitido para o destinatário e descriptografado usando uma chave para reaver a mensagem original.

Métodos Criptográficos

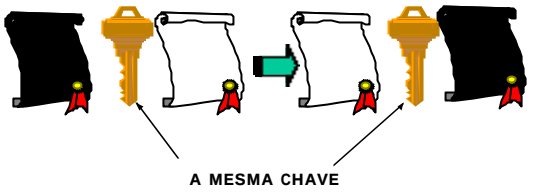
- **Existem dois métodos básicos de criptografia hoje em dia:**
  - A Criptografia de CHAVE-SECRETA, e
  - A Criptografia de CHAVE-PÚBLICA.

Métodos Criptográficos

- **Criptografia por CHAVE-SECRETA**
  - A Criptografia por CHAVE-SECRETA, também conhecida como Criptografia SIMÉTRICA, usa a mesma chave para criptografar e descriptografar a mensagem.
  - Deste modo, tanto o remetente quanto o destinatário da mensagem devem compartilhar um segredo chamado de CHAVE.

Métodos Criptográficos

- **Criptografia por CHAVE-SECRETA**



Métodos Criptográficos

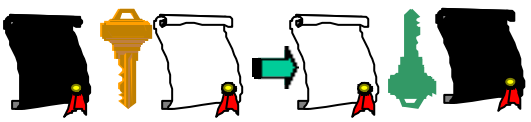
- **Criptografia por CHAVE-SECRETA**
  - Um algoritmo bem conhecido de criptografia por CHAVE-SECRETA é o Data Encryption Standard (DES), que é utilizada por instituições financeiras para criptografar PINs (personal identification numbers).
  - O problema é:
    - como distribuir a CHAVE?

Métodos Criptográficos

- **Criptografia por CHAVE-PÚBLICA**
  - A Criptografia por CHAVE-PÚBLICA, também conhecida com Criptografia ASSIMÉTRICA, usa duas chaves:
    - Uma chave para criptogafar a mensagem, e
    - Outra chave para descriptografar a mensagem.

Métodos Criptográficos

- **Criptografia por CHAVE-PÚBLICA**



Métodos Criptográficos

- **Criptografia por CHAVE-PÚBLICA**
  - As duas chaves estão matematicamente relacionadas de modo que os dados criptografados utilizando uma das chaves, só pode ser descriptografado utilizando a outra.
  - Cada usuário possui duas chaves, uma chave pública e uma chave privada.
  - Este usuário distribui então a chave pública.

Métodos Criptográficos

- **Criptografia por CHAVE-PÚBLICA**
  - Devido a esta relação entre estas duas chaves, o usuário e qualquer pessoa de posse da chave pública pode criptografar os dados e transmití-los ao usuário. Os dados só poderão ser descriptografados através da chave privada.
  - Assim, a segurança é mantida desde que o usuário não revele a ninguém a sua chave privada (que foi gerada por ele).

Métodos Criptográficos

- **Criptografia por CHAVE-PÚBLICA**
  - O algoritmo RSA (inventado por Rivest, Shamir, and Adleman) é um ds algoritmos mais populares para criptografia de Chave-Pública.

Métodos Criptográficos

- **PGP (Pretty Good Privacy):** desenvolvido por Philip Zimmerman em 1991, destina-se a comunicação segura via correio eletrônico.
  - Utiliza o algoritmo de chave única IDEA, a função de hash MD5 para integridade e o algoritmo de chave pública RSA para gerenciamento de chaves e assinatura digital.
  - As chaves podem variar entre 512 e 1024 bits.
  - Não utiliza nenhuma autoridade de certificação de chaves, mas é o próprio usuário que distribui suas chaves públicas.

Métodos Criptográficos

- **RIPEM (Riordan's Internet PEM):** uma implementação das normas PEM (Privacy Enhanced Mail). Sua especificação pode ser encontrada nos RFC 1421 a 1424 [Sch96].
- **SSL (Secure Sockets Layer):** desenvolvido pela Netscape Communications, tem como objetivo gerar segurança e privacidade entre duas aplicações, como HTTP, telnet ou FTP. No início da comunicação são trocadas entre as aplicações quais a versão do protocolo e os algoritmos a serem utilizados, é realizada a autenticação mútua e finalmente a negociação das chaves de criptografia.

Métodos Criptográficos

- **IPv6:** a nova versão do Internet Protocol.
  - Possui suporte a autenticação e privacidade, implementadas através de extensões do cabeçalho, seguindo o cabeçalho principal.
  - O campo destinado a autenticação é o authentication header (AH) e o para privacidade é o encapsulating security payload (ESP).
  - Maiores detalhes podem ser encontrados nos RFCs 1825 a 1829.