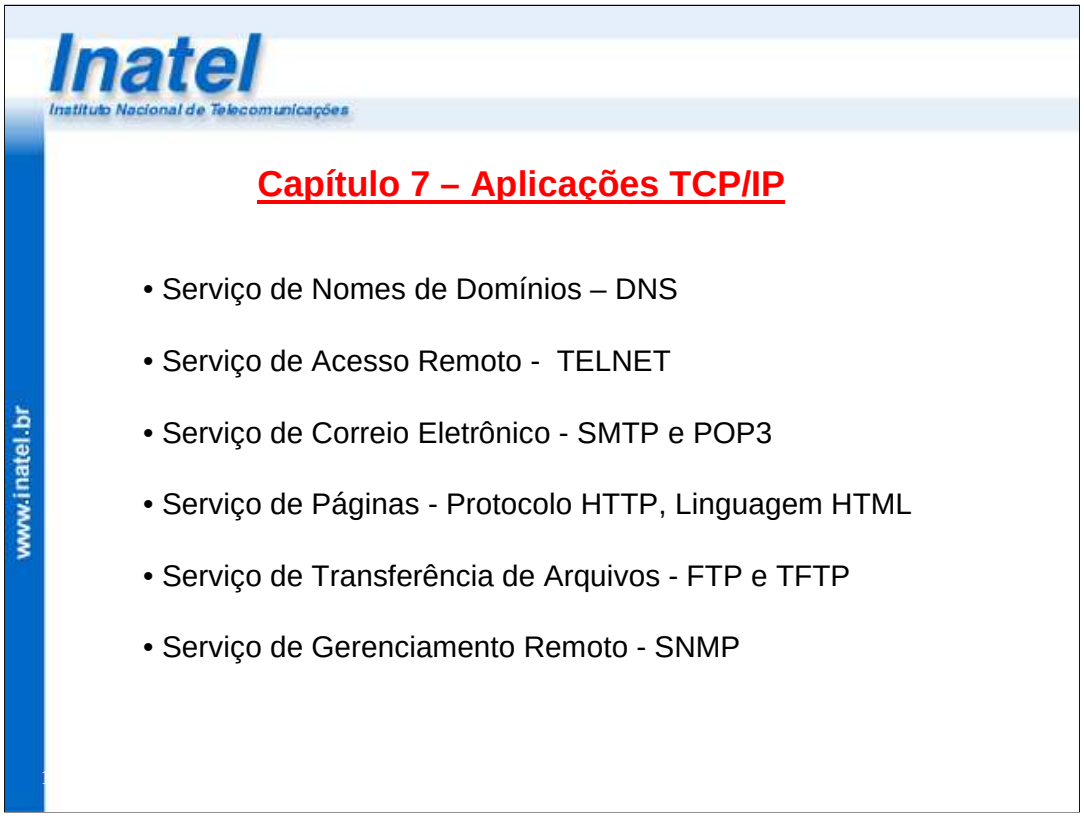


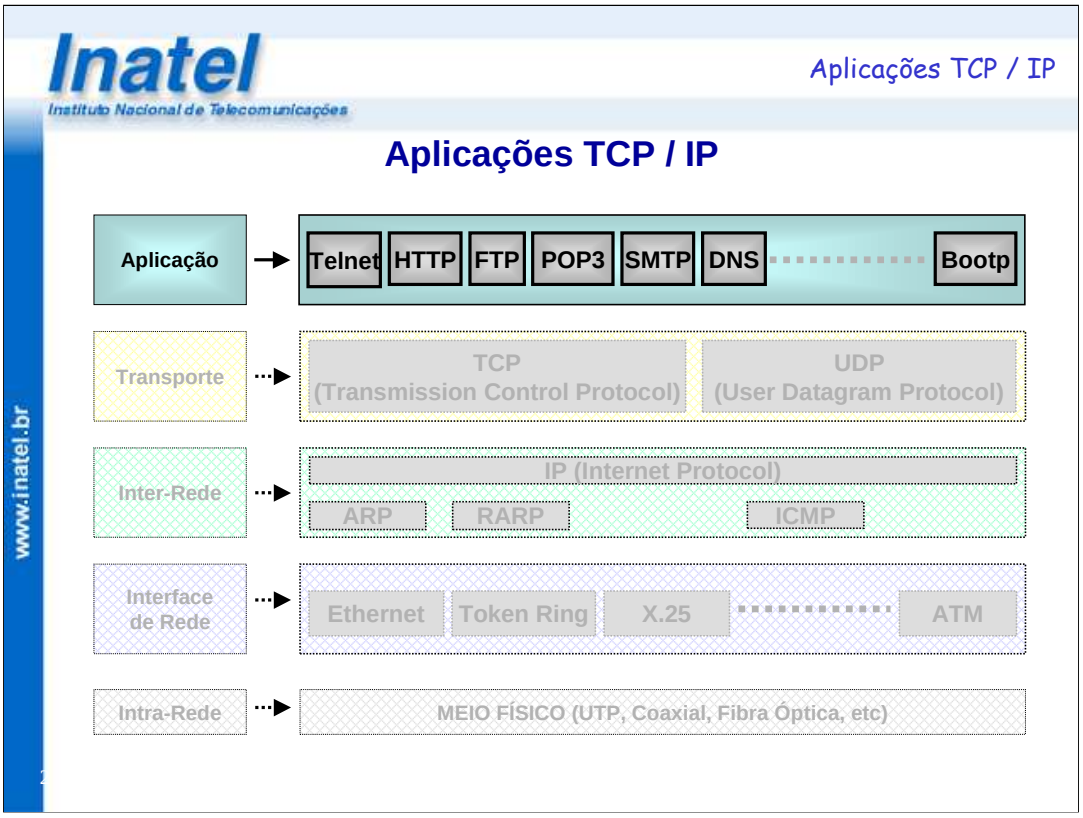
Neste capítulo serão vistos outros protocolos que fazem parte da pilha de protocolos TCP / IP como:

Serviço de correio eletrônico através da utilização dos protocolos da camada de aplicação, o SMTP (Simple Mail Transfer Protocol), o POP (Post Office Protocol).

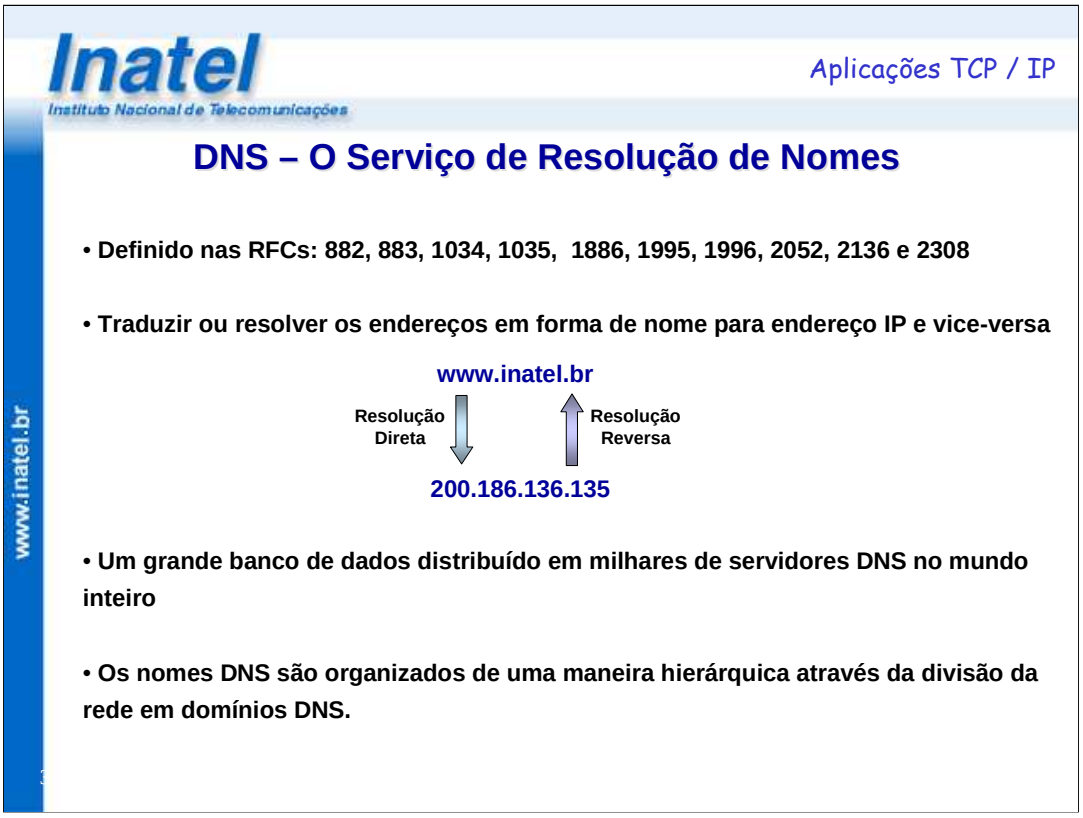
Serviço de Paginas da WEB através da utilização do protocolo HTTP (Hyper Text Transfer Protocol) com a linguagem HTML (Hyper Text Markup Language).

Serviço de transferência de arquivos utilizando o protocolo de aplicação FTP (File Transfer protocol).

E outros.

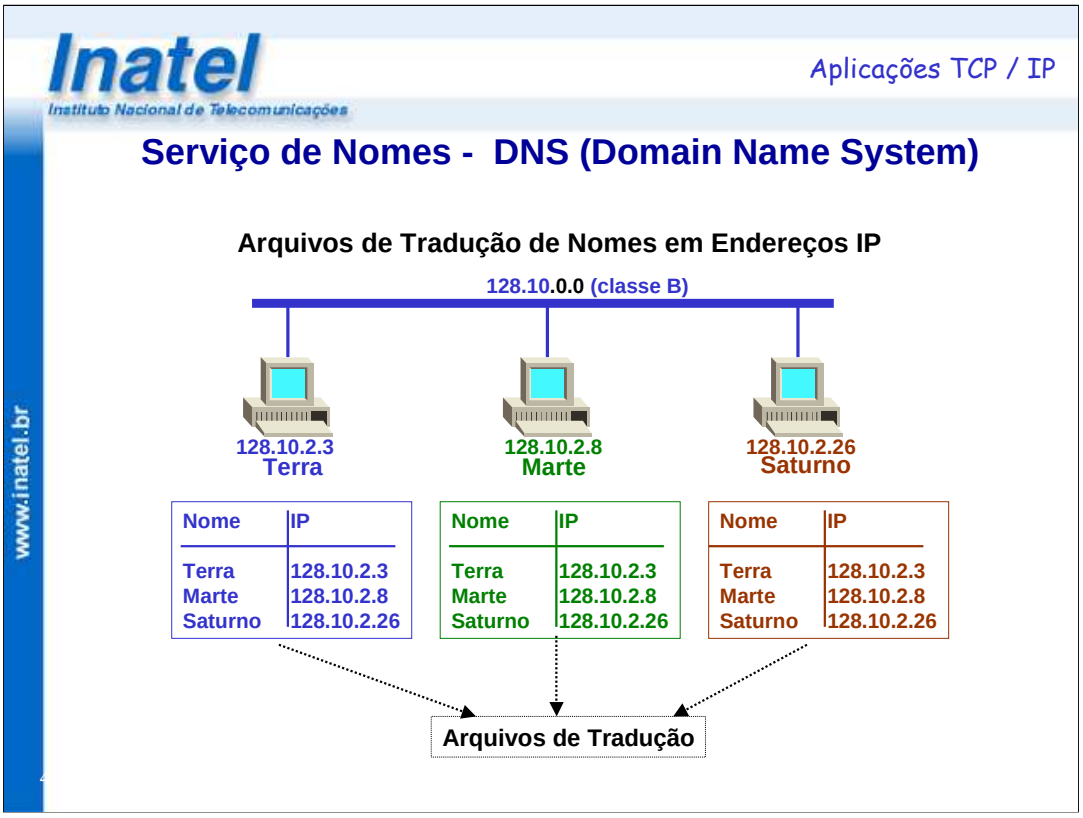


Neste capítulo serão vistos alguns protocolos que compõem a camada de aplicação do protocolo TCP / IP



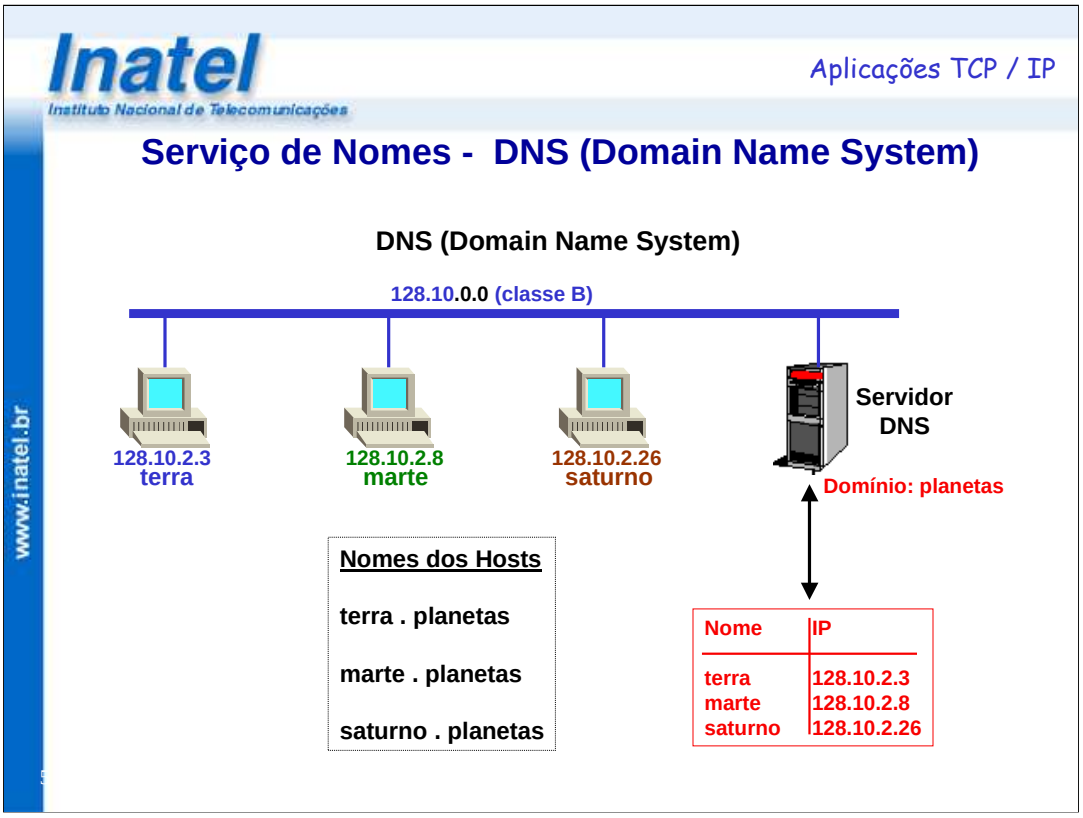
DNS (Domain Name System) é um serviço de resolução de nomes. Toda comunicação entre os computadores e demais equipamentos de uma rede baseada no protocolo TCP/IP é feita através do número IP. Porém não seria nada produtivo se os usuários tivessem que decorar, ou consultar uma tabela de números IP toda vez que tivessem que acessar um recurso da rede. Por exemplo, você digita www.microsoft.com/brasil, para acessar o site da Microsoft no Brasil, sem ter que se preocupar e nem saber qual o número IP do servidor onde está hospedado o site da Microsoft Brasil. Mas alguém tem que fazer este serviço, pois quando você digita www.microsoft.com/brasil, o protocolo TCP/IP precisa "descobrir" (o termo técnico é resolver o nome) qual o número IP está associado com o nome digitado. Se não for possível "descobrir" o número IP associado ao nome, não será possível acessar o recurso desejado.

O papel do DNS é exatamente este, "descobrir", ou usando o termo técnico, "resolver" um determinado nome, como por exemplo www.microsoft.com. Resolver um nome significa, descobrir e retornar o número IP associado com o nome. O DNS é, na verdade, um grande banco de dados distribuído em milhares de servidores DNS no mundo inteiro.



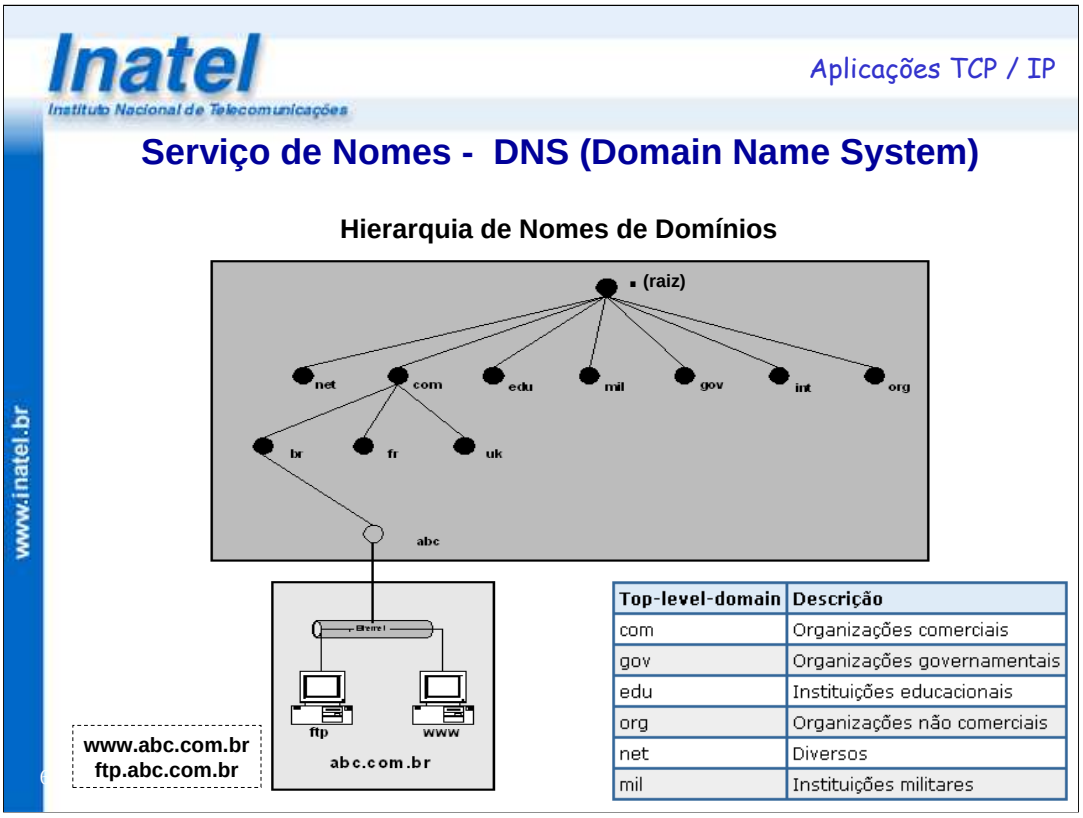
A identificação das máquinas pelos seus endereços de rede, não é popular entre os usuários, que preferem identificá-las por nomes fáceis de memorizar. Para que isto seja possível, é necessário traduzir entre nomes e endereços. O serviço de nomes tem esta responsabilidade.

Em redes de pequeno porte, as informações necessárias à identificação e à localização dos componentes na rede podem ser armazenadas em arquivos na próprias máquinas. Neste caso é necessário que o arquivo de nomes seja sempre atualizado pelo gerente da rede e que sua versão atual seja periodicamente copiada para todas as máquinas. Nestas redes, os nomes usados para identificar as máquinas não precisam Ter uma estrutura especial. O espaço de nomes pode ser plano, não precisa ser organizado de forma hierárquica. É necessário apenas garantir que não existam máquinas com nomes iguais. Isto pode ser garantido centralizando-se a escolha dos nomes. Estes arquivos contendo o nome e o endereço das máquinas são chamados de arquivos de tradução.



Em redes de grande porte, manter os arquivos de tradução em todas as máquinas é impraticável, pois o arquivo seria grande demais e precisaria ser atualizado com freqüência; além disso, um espaço de nomes plano seria ineficiente. A solução é distribuir as informações entre máquinas que prestam um serviço de diretório com informações sobre os componentes da rede e adotar uma hierarquia para os espaços de nomes. Uma vez adotada a hierarquia, os nomes só precisam ser diferentes em um mesmo nível da hierarquia e a escolha dos nomes pode ser distribuída.. Os servidores de diretório responsáveis por prover informações como nome e endereço das máquinas são normalmente chamados de servidores de nomes. Na rede Internet, o serviço de nomes usado é o Domain Name System (DNS).

O DNS apresenta uma arquitetura cliente-servidor, podendo envolver vários servidores DNS na resposta a uma consulta. Os formatos das informações, armazenadas em arquivos de tradução nos servidores, e o protocolo usado entre clientes e servidores são padronizados. A administração é descentralizada: cada gerente é responsável pela manutenção dos servidores DNS na sua rede.

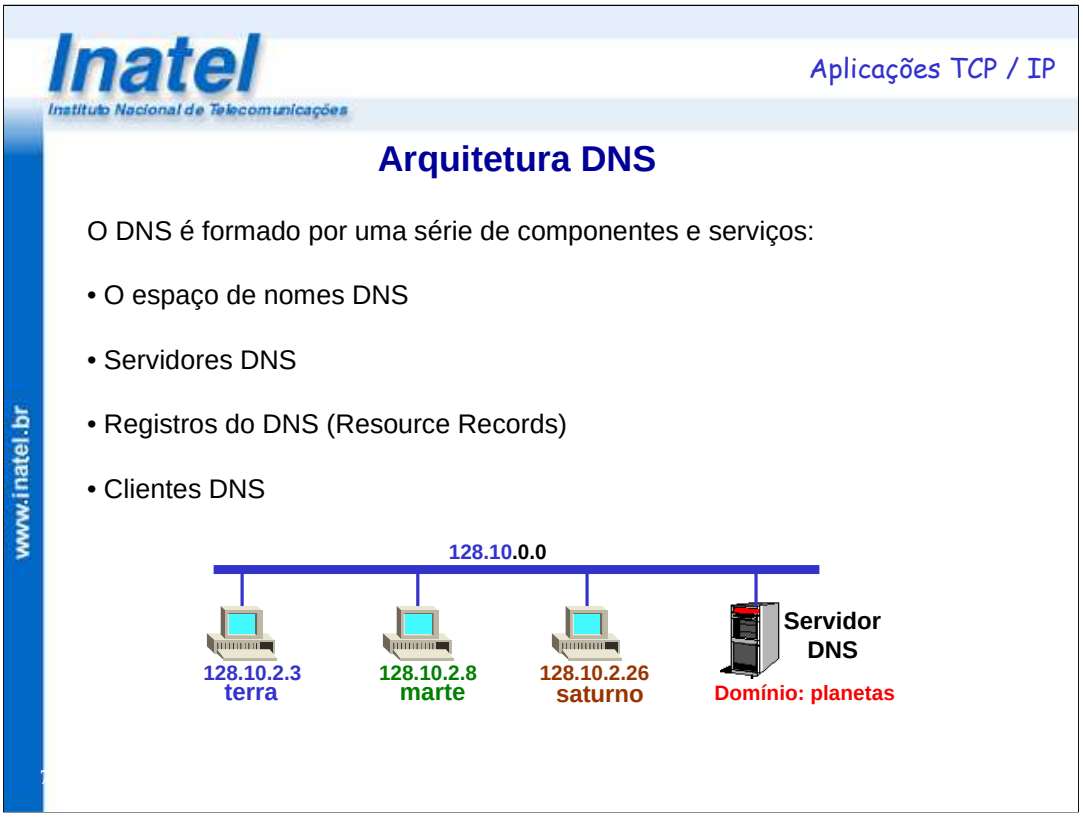


O espaço de nomes DNS é organizado de forma hierárquica em domínios compostos por máquinas sob uma mesma administração. Os domínios possibilitam a administração descentralizada das informações e cada um deles tem um nome de domínio.

O nome completo de um domínio, que pode chegar a 255 caracteres, é composto pelos nomes dos domínios intermediários separados por pontos e listados da esquerda para a direita. Quanto mais baixo o nível hierárquico, mais à esquerda estará o nome do domínio intermediário na composição do nome completo.

A quantidade de domínios intermediários varia entre organizações, já que os domínios refletem a estrutura adotada para a gerência da rede na organização.

Uma vez escolhido os nomes dos domínios, é necessário escolher os nomes das máquinas. Isto é responsabilidade dos gerentes dos domínios. Eles devem garantir que não existam máquinas com nomes iguais e que os nomes sigam um padrão estabelecido. Embora não seja obrigatório estabelecer um padrão para os nomes das máquinas, é comum escolher nomes que tenham algo em comum: nomes de animais, nomes de rios, nomes de estrelas, etc.



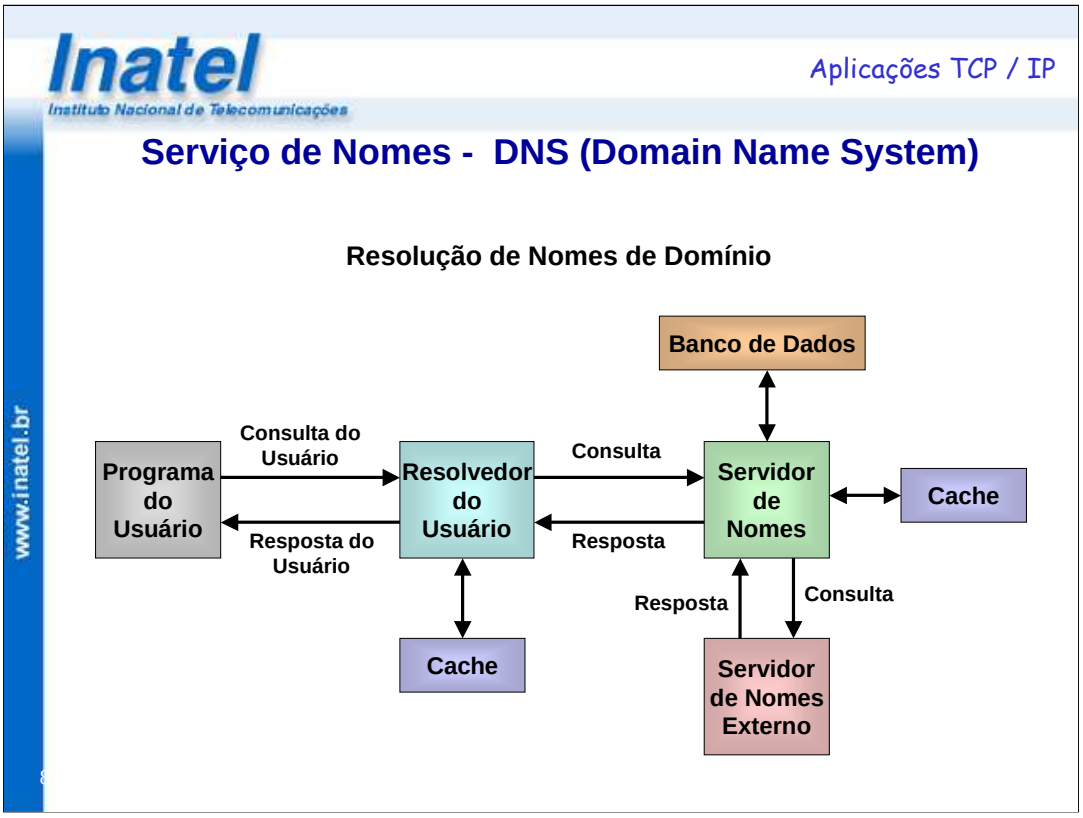
O DNS é formado por uma série de componentes e serviços, os quais atuando em conjunto, tornam possível a tarefa de fazer a resolução de nomes em toda a Internet ou na rede interna da empresa. Os componentes do DNS são os seguintes:

•**O espaço de nomes DNS:** Um espaço de nomes hierárquico e contínuo. Pode ser o espaço de nomes da Internet ou o espaço de nomes DNS interno da empresa.

•**Servidores DNS:** contém o banco de dados do DNS com o mapeamento entre os nomes DNS e o respectivo número IP.

•**Registros do DNS (Resource Records):** são as entradas do banco de dados do DNS. Em cada entrada existe um mapeamento entre um determinado nome e uma informação associada ao nome. Pode ser desde um simples mapeamento entre um nome e o respectivo endereço IP, até registros mais sofisticados para a localização de servidores de e-mail do domínio.

•**Clientes DNS:** conhecidos como resolvedores (resolvers). É um componente de software responsável por detectar sempre que um programa precisa de resolução de um nome e repassar esta consulta para um servidor DNS. O servidor DNS retorna o resultado da consulta, o resultado é retornado para o resolver, o qual repassa o resultado da consulta para o programa que originou a consulta.

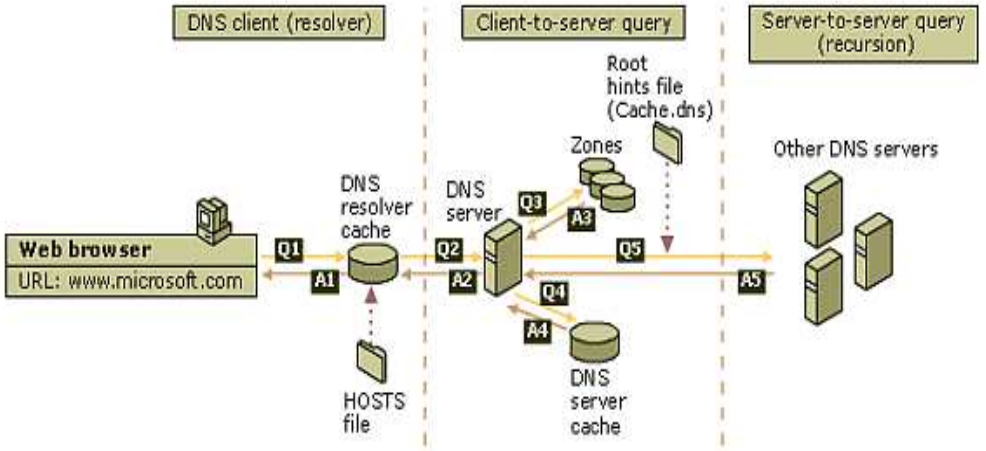


Na tradução ou resolução de nomes, ao receber uma consulta, o servidor DNS verifica se o nome a ser traduzido ou resolvido está em um domínio sob sua responsabilidade. Em caso afirmativo, envia uma resposta à consulta ao cliente que solicitou a consulta. Se o nome não estiver em um domínio sob sua responsabilidade, o servidor DNS procura um servidor DNS que saiba responder à consulta. Esta procura por um servidor DNS que saiba responder à consulta é realizada seguindo uma hierarquia de domínios DNS.

Na maioria das vezes, a resposta a uma consulta é bem rápida, já que os servidores DNS armazenam em uma área de memória, que opera como cache do serviço DNS, as respostas às consultas recentemente realizadas. Existe, portanto, a possibilidade de as informações desejadas estarem nos caches dos servidores DNS consultados, reduzindo assim o tempo de resposta a uma consulta.

Pesquisa DNS

Exemplo: Processo de Resolução de Nomes



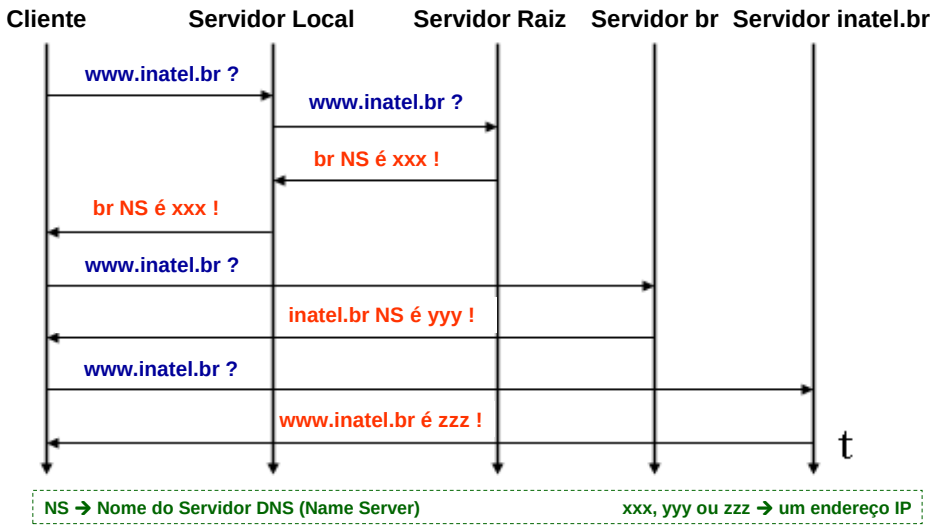
Nota: Para que um domínio seja registrado na Internet é obrigatório o uso de pelo menos dois servidores de nomes responsáveis pelo domínio criado. Esses servidores podem ser construídos na infra-estrutura da própria empresa ou em uma infra-estrutura terceirizada.

Existem diferentes maneiras como uma consulta pode ser resolvida. Por exemplo, a primeira vez que um nome é resolvido, o nome e o respectivo número IP são armazenados em memória, no que é conhecido como Cache do cliente DNS, na estação de trabalho que fez a consulta. Na próxima vez que o nome for utilizado, primeiro o "resolver" procura no Cache DNS no cliente, para ver se não existe uma resolução anterior para o nome em questão. Somente se não houver uma resolução no Cache local do DNS, é que será envida uma consulta para o servidor.

Chegando a consulta ao servidor, primeiro o servidor DNS consulta o cache do servidor DNS. No cache do servidor DNS ficam, por um determinado período de tempo, as consultas que foram resolvidas pelo servidor DNS, anteriormente. Esse processo agiliza a resolução de nomes, evitando repetidas resoluções do mesmo nome. Se não for encontrada uma resposta no cache do servidor DNS, o servidor pode tentar resolver a consulta usando as informações da sua base de dados ou pode enviar a consulta para outros servidores DNS, até que uma resposta seja obtida, processo este chamado de recursão.

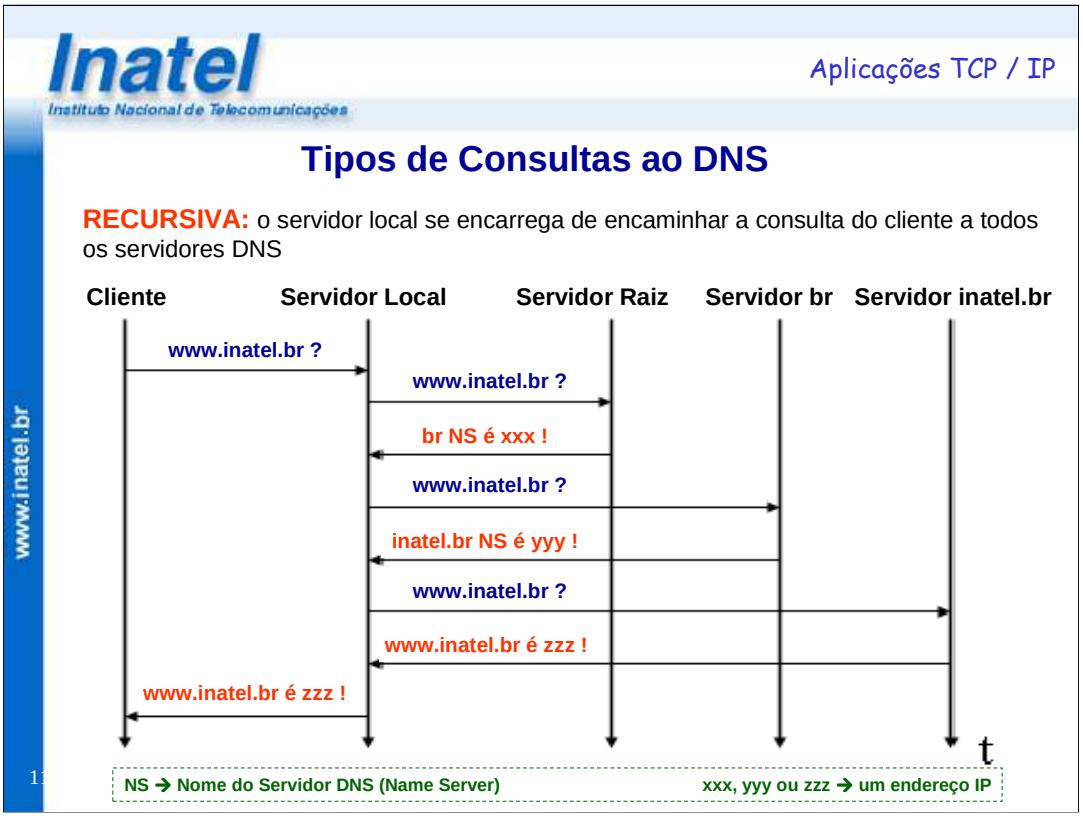
Tipos de Consultas ao DNS

ITERATIVA: O modo de operação default, suportado por todos os servidores DNS



NS → Nome do Servidor DNS (Name Server) xxx, yyy ou zzz → um endereço IP

Em relação aos seus clientes locais, um servidor DNS pode operar com dois tipos de consultas: **iterativas** e **recursivas**. O modo de operação default, suportado por todos os servidores, é o de consultas **iterativas**.



No modo de consulta **recursiva**, o servidor local se encarrega de encaminhar a consulta do cliente a todos os servidores DNS necessários até que ela seja resolvida. Esse modo de operação é opcional e não precisa ser implementado pelos servidores.

O processo descrito anteriormente, termina com o servidor DNS (após ter consultado vários outros servidores) retornando uma resposta positiva para o cliente, isto é, conseguindo resolver o nome e retornando a informação associada (normalmente o número IP associado ao nome) para o cliente. Mas nem sempre a resposta é positiva, muitos outros tipos de resultados podem ocorrer em resposta a uma consulta, tais como:

•**Authoritative (resposta com autoridade):** quando ele é o servidor responsável pelo domínio objeto da consulta.

•**Non-authoritative (resposta com não-autoridade):** quando ele respondeu por já ter a resposta em seu cache local.

•**Negative answer (resposta negativa):** Esta resposta pode indicar que um dos seguintes resultados foi obtido em resposta à consulta: Um servidor DNS que é autoridade para o domínio pesquisado, informou que o nome pesquisado não existe neste domínio ou um servidor DNS que é autoridade para o domínio pesquisado, informou que o nome pesquisado existe, mas o tipo de registro não confere.

Registros DNS

• **Arquivos de Zona** → arquivos-texto que contêm as definições dos nomes pertencentes a um determinado domínio e seus respectivos endereços IP

• **Para cada domínio sob a responsabilidade de um servidor DNS:**

- **um *arquivo de zona* direta** → para os mapeamentos nome à IP
- **um *arquivo de zona reversa*** → para os mapeamentos IP à nome

A cada domínio local sob a responsabilidade de um servidor DNS corresponde um *arquivo de zona* (arquivos-texto que contêm as definições dos nomes pertencentes a um determinado domínio e seus respectivos endereços IP). Para cada domínio também deve estar presente um *arquivo de zona reversa*, que relaciona os endereços IP aos nomes existentes no domínio.

Cada servidor DNS armazena localmente as informações sobre os domínios de sua responsabilidade. As informações sobre o domínio são armazenadas em *arquivos de zona direta* (para os mapeamentos *nome* à *IP*) e de *zona reversa* (para os mapeamentos *IP* à *nome*).

Registros DNS

Os registros DNS mais freqüentemente usados nos arquivos de zona são:

SOA → indica o início da zona de autoridade

NS → indica um servidor de nomes para a zona

MX → indica um servidor de e-mail para a zona

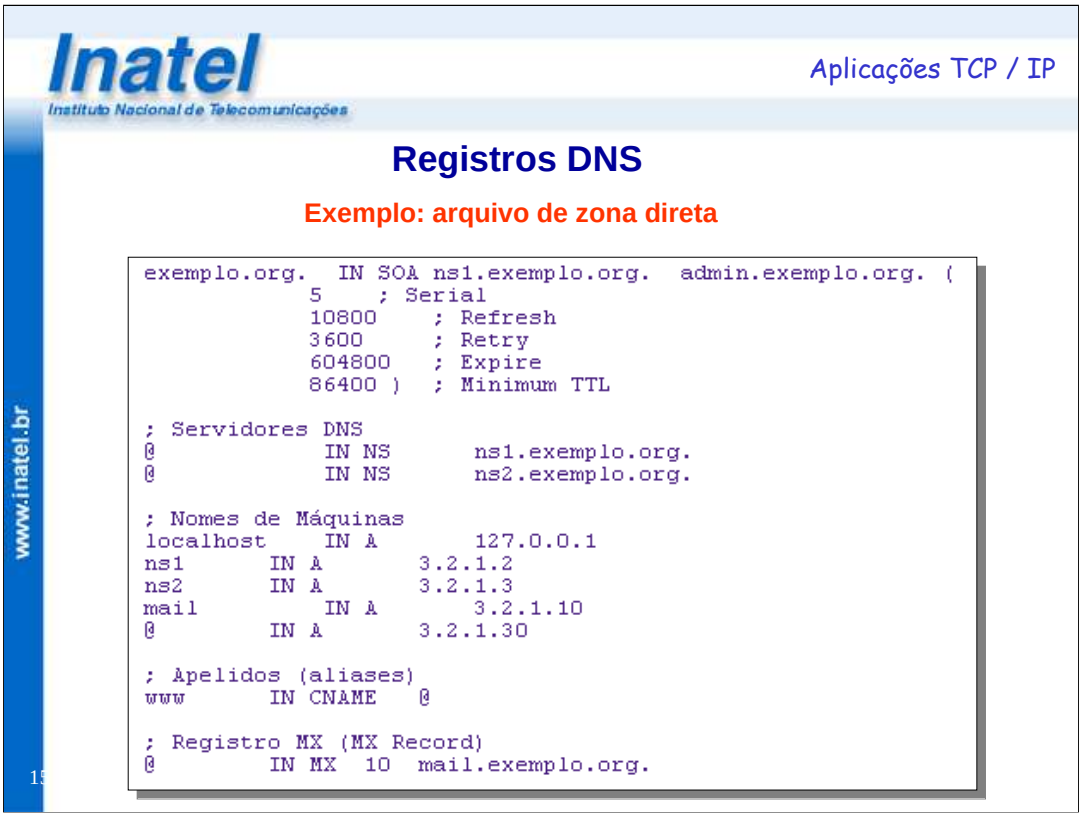
A → indica o endereço IP relativo a um nome de domínio (resolução direta)

TXT → string descrevendo o host (não interpretado)

HINFO → indica dados de hardware e software do host

CNAME → indica um alias (apelido) de nome de domínio

PTR → indica o nome de domínio relativo a um endereço IP (resolução reversa)



Note que cada nome de sistema que termina com um ``." é um nome exato, ao passo que tudo sem um ``." no final é referenciado à origem. Por exemplo, *www* é traduzido para *www + origem*. Em nosso arquivo de zona fictício, nossa origem é exemplo.org., então *www* será traduzido para www.exemplo.org..

O formato de um arquivo de zona é como segue:

nomedoregistro IN tipodoregistro valor

exemplo.org. → o nome de domínio, que também é a origem para este arquivo de zona

ns1.exemplo.org. → o servidor de nome primário/autoritativo para esta zona

admin.exemplo.org. → o endereço de correio eletrônico da pessoa responsável por esta zona, com a @ trocada. (<admin@exemplo.org> é substituído por *admin.exemplo.org*)

5 → o número de série do arquivo. Deve ser incrementado toda vez que o arquivo de zona é alterado. Hoje em dia, muitos administradores preferem o formato *aaaammddii* para o número de série. 2001041002 quer dizer que a última modificação foi feita em 10/04/2001, e os dígitos 02 ao final, significam que foi a segunda vez que o arquivo de zona foi alterado nesse dia.

Para arquivos de zona in-addr.arpa (DNS reverso), o mesmo formato é usado, exceto pelo fato de conter entradas *PTR* ao invés de *A* ou *CNAME*.

Este arquivo fornece o endereço IP adequado aos mapeamentos de nomes de sistemas de nosso domínio fictício acima.

Servidor DNS

Quanto à sua funcionalidade, um servidor DNS pode ser:

- **Primário:**
  - responsável por um domínio.
  - Inclusão, alterações ou exclusões dos registros da zona são feitas neste servidor.
- **Secundário:**
  - backup do servidor primário
  - recebe dele os arquivos de zona (*zone transfer)*
  - responde as requisições dos clientes quando requisitado.
- **Caching-only:**
  - apenas efetua consultas e retorna resultados, mantendo um cache local
  - não é responsável por nenhuma zona.

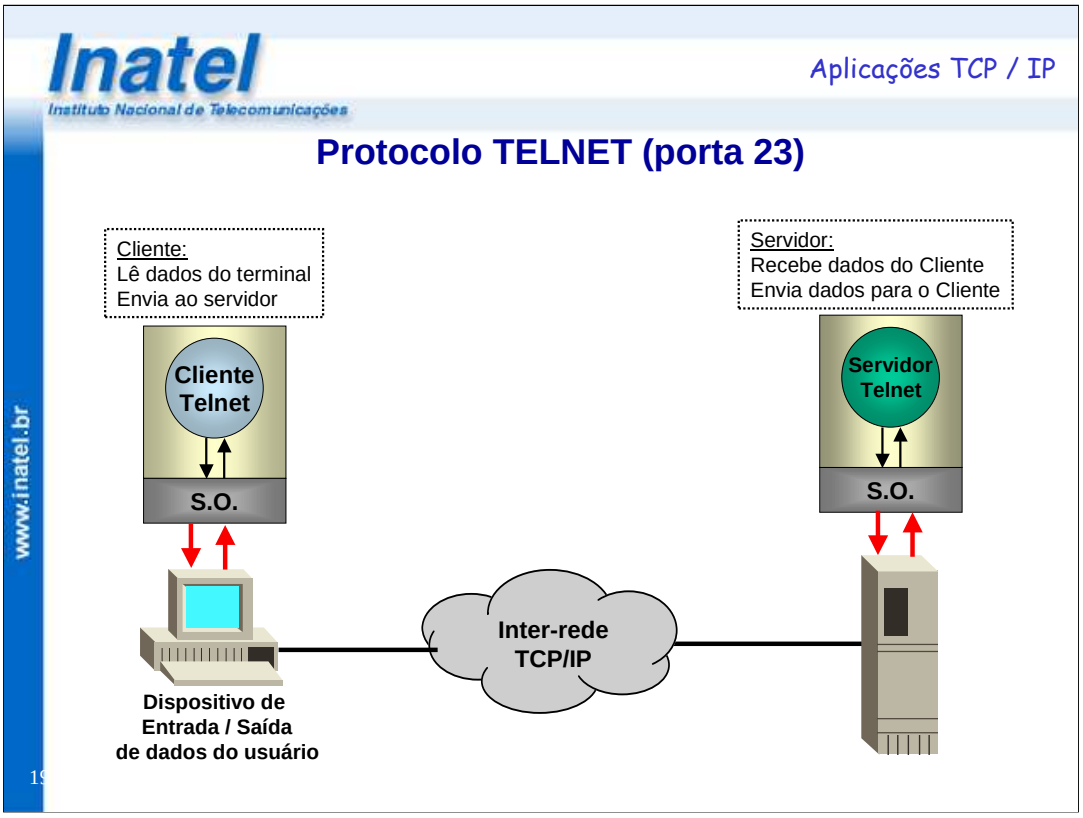
Quanto à sua funcionalidade, um servidor DNS pode ser:

•**Primário**: É o servidor responsável por um domínio. A inclusão, alterações ou exclusão dos registros da zona respectiva são feitas neste servidor.

•**Secundário**: funciona como backup do servidor primário, recebendo dele os arquivos de zona através de um processo chamado *zone transfer*; responde as requisições dos clientes quando requisitado.

•**Caching-only**: servidor DNS que apenas efetua consultas e retorna resultados, mantendo uma cache local; não é responsável por nenhuma zona.

O protocolo TCP/IP inclui um protocolo simples de terminal remoto denominado TELNET. O TELNET permite que um usuário em determinado site estabeleça uma conexão TCP com um servidor login situado em outro site. O TELNET transmite, então os toques no teclado do usuário diretamente ao computador remoto, como se estivessem sendo digitados no teclado conectado à máquina remota. Esse terminal também retorna a saída da máquina remota até a tela do usuário. O servidor recebe o nome de *transparente*, porque faz com que o teclado e o monitor do usuário pareçam estar conectados diretamente à máquina remota.

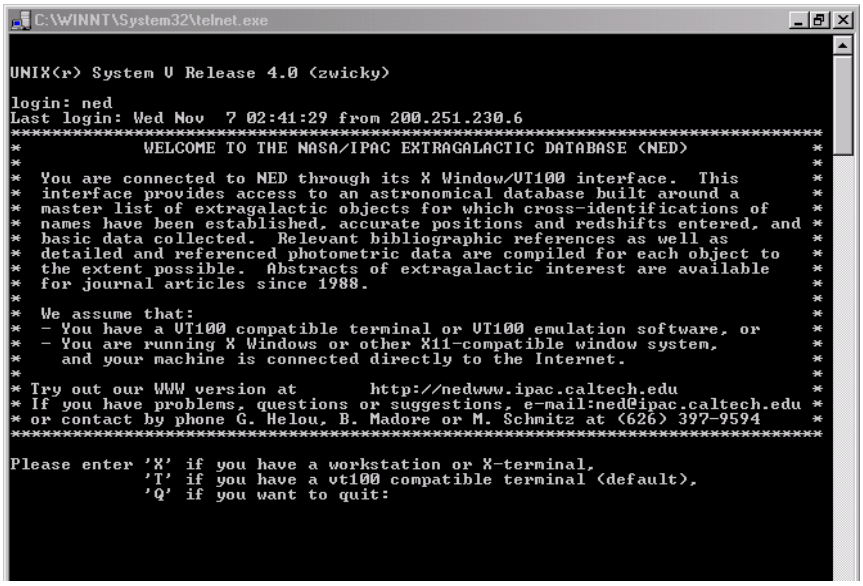


A Figura ilustra como os programas aplicativos implementam um cliente e servidor TELNET, quando um usuário chama o TELNET, um programa aplicativo existente na máquina do usuário torna-se o cliente. O cliente estabelece uma conexão TCP com o servidor por intermédio da qual irão se comunicar. Uma vez estabelecida a conexão, o cliente aceita toques de teclado do usuário e os envia ao servidor enquanto, simultaneamente, aceita caracteres que o servidor envia de volta e apresenta-os na tela do usuário. O servidor deve aceitar uma conexão TCP de um cliente e, a seguir, retransmitir dados entre a conexão TCP e o sistema operacional local.

Na prática, o servidor é mais complexo do que a figura representa porque precisa conduzir várias conexões simultâneas. Em geral, um processo de servidor-mestre aguarda novas conexões e cria um novo escravo para cuidar de uma conexão em particular. Desse modo, “o servidor TELNET” mostrado na Figura representa o escravo que trata de uma conexão em particular. A figura não mostra o servidor-mestre que espera novas solicitações, nem mostra os escravos cuidando das outras conexões.

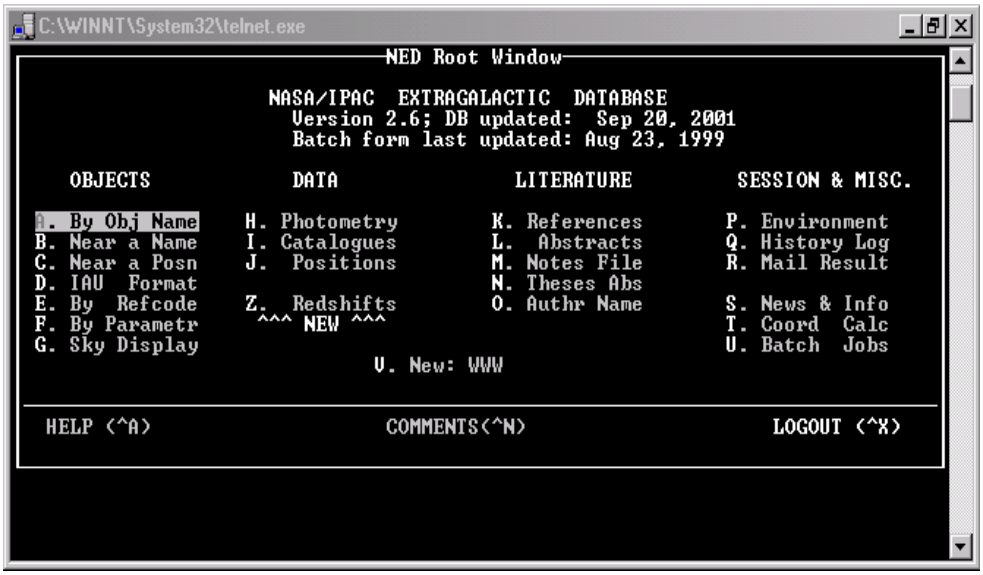
Protocolo TELNET (porta 23)

telnet ned.ipac.caltech.edu



A figura mostra a copia da tela de um acesso remoto via protocolo TELNET ao host da NASA, que contém um banco de dados extra-galático.

Protocolo TELNET (porta 23)



A tela mostrada é a seqüência da tela anterior.

Protocolo TELNET (porta 23)

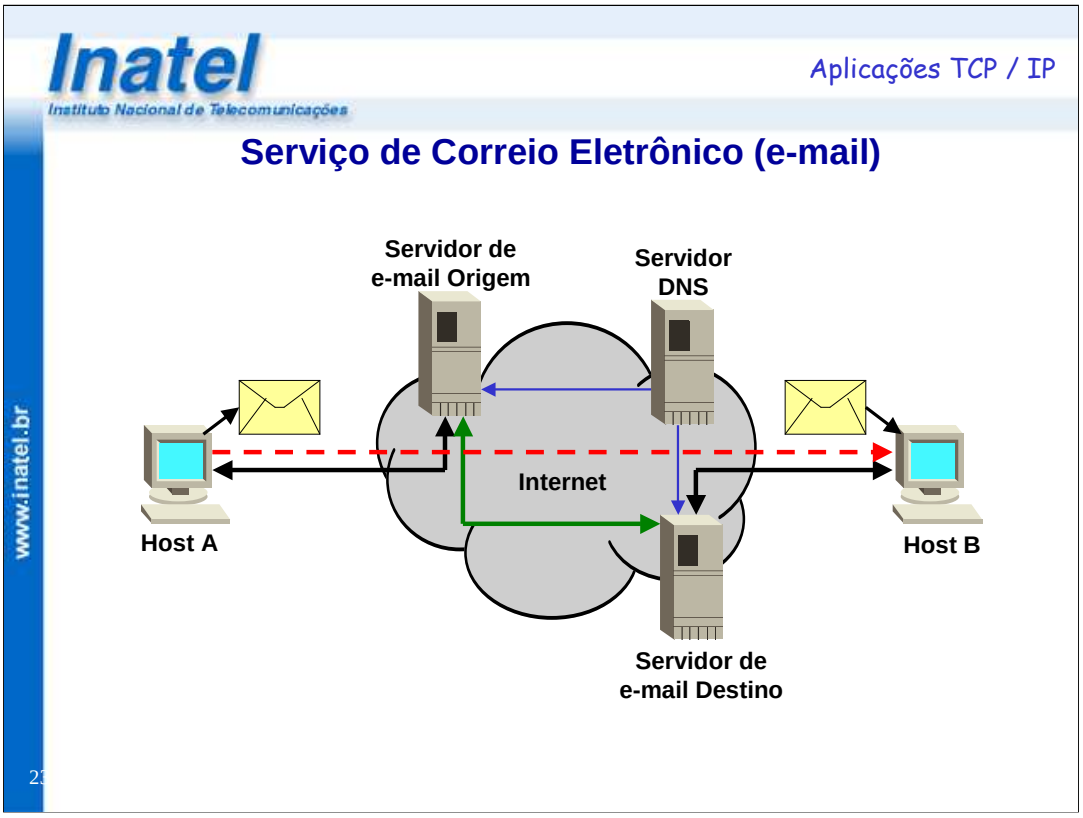
Alguns endereços para conexão

netfind.if.usp.br - Busca mundial de usuários na Internet. Digite netfind ao estabelecer a conexão.

ned.ipac.caltech.edu - Banco de dados Extragalático da NASA/IPAC. Digite ned na conexão.

spacelink.msfc.nasa.gov - Banco de dados da NASA. Digite guest ao se conectar.

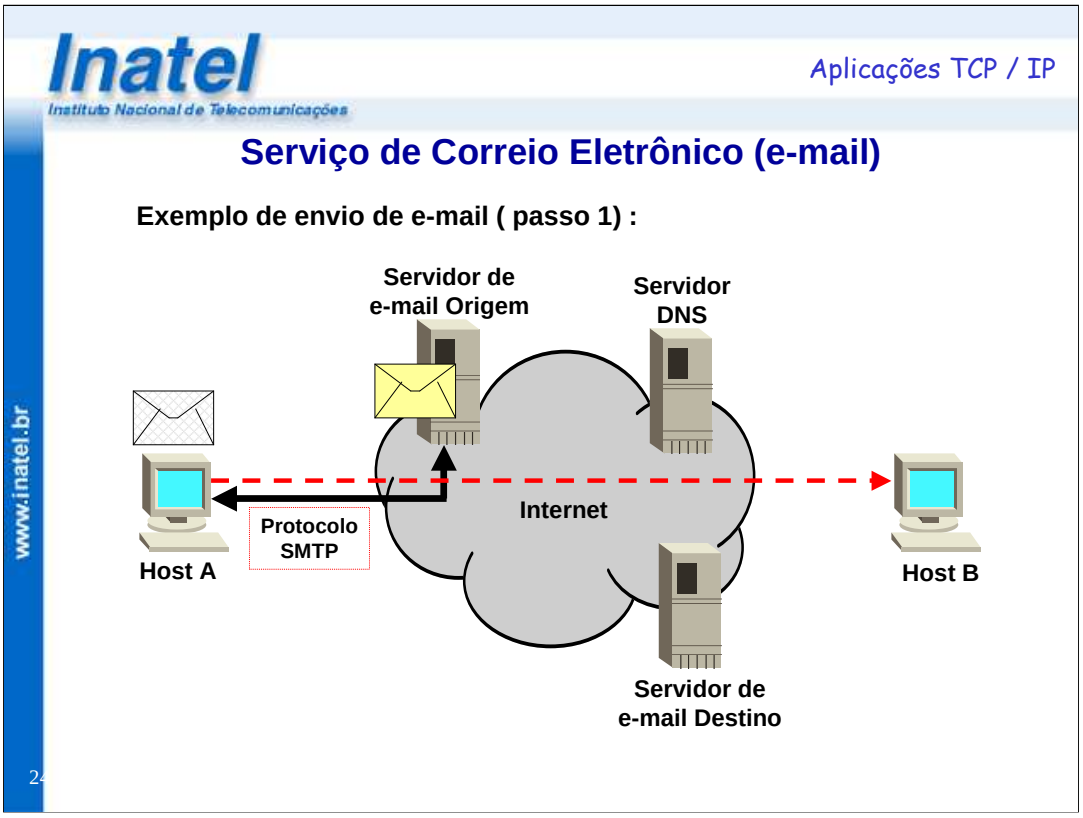
stis.nsf.gov - Informações científicas e tecnológicas. Digite public na conexão.



O correio eletrônico (e-mail) é, provavelmente, o aplicativo mais largamente usado. Os protocolos básicos de correio da Internet provêm troca de correspondência e mensagens entre hosts TCP / IP.

Os sistemas de correio eletrônico utilizam uma técnica chamada de spool. Quando o usuário envia uma mensagem de correspondência, o sistema coloca uma cópia em sua memória particular (spool) juntamente com uma identificação do usuário, do destinatário, do equipamento de destino e do tempo de depósito. O sistema, então, inicializa a transferência para o equipamento remoto como uma atividade em background, permitindo que o transmissor continue a executar outras atividades do computador.

O processo de transferência de mensagens em background torna-se um cliente. Primeiramente, o processo utiliza o DNS para mapear o nome da máquina do destino para um endereço IP, tentando, depois, formar uma conexão TCP para o servidor de correspondência do equipamento de destino. Se essa operação for bem-sucedida, o processo de transferência encaminha uma cópia da mensagem ao servidor remoto que armazena a cópia na área de spool do sistema remoto. Tão logo o cliente e o servidor concordem que a cópia foi recebida e armazenada, o cliente remove a cópia local.



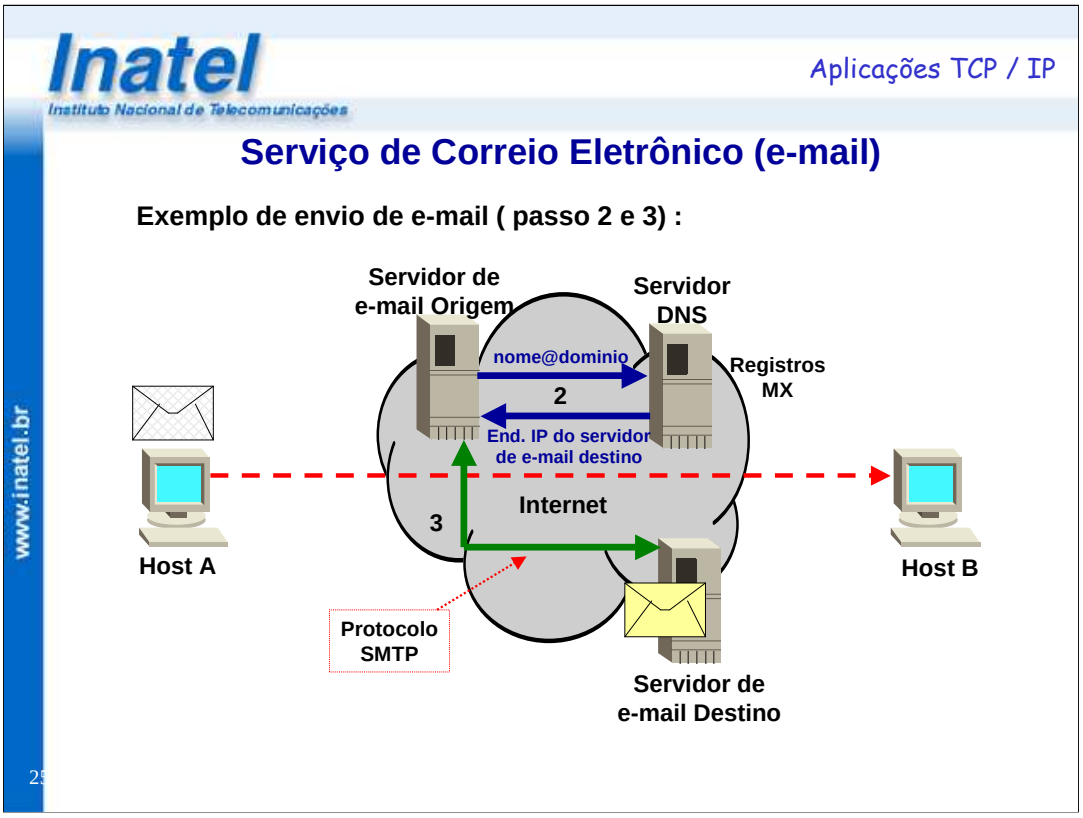
Neste exemplo vamos ver como é feita a transferência de e-mail entre os hosts origem e destino.

Devemos observar os seguintes passos:

• O host origem deve compor a mensagem a ser enviada e endereçá-la.

•O host origem através do protocolo de aplicação SMTP abre uma conexão TCP com o servidor de origem e envia o e-mail no formato do protocolo SMTP.

• Pronto ! o e-mail já foi enviado ao servidor de origem e está armazenado (spool).

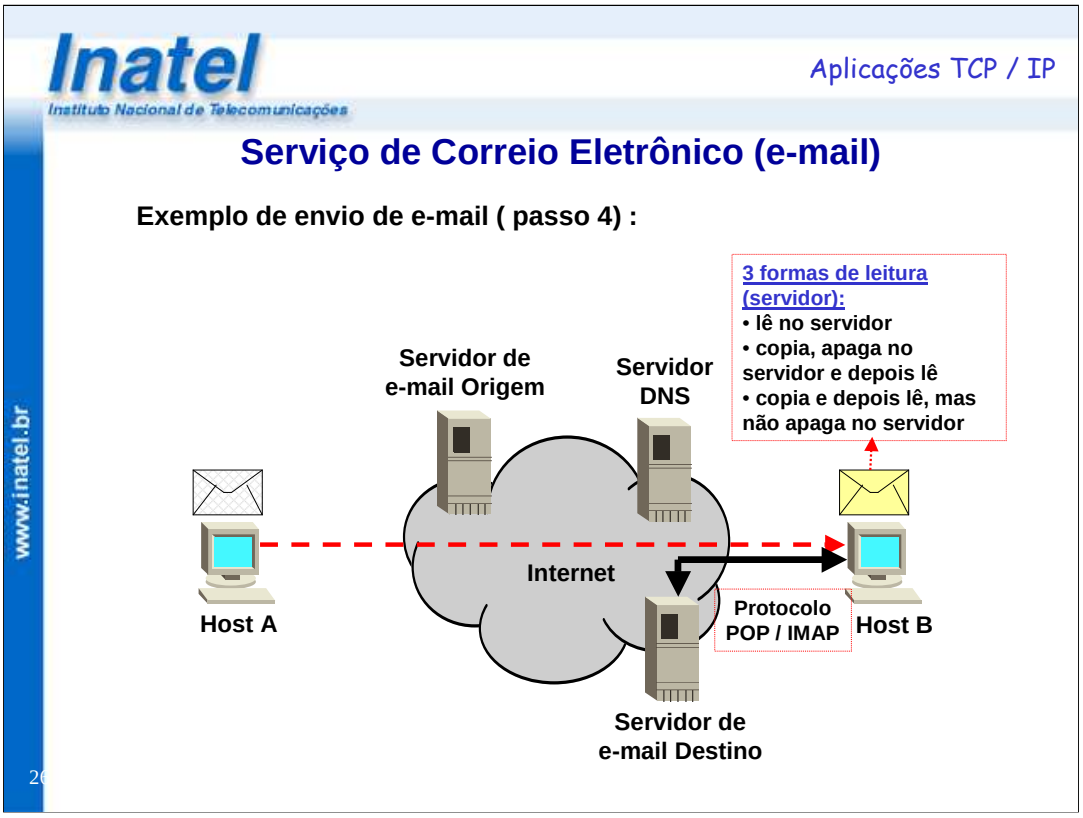


Próximo passo:

• O servidor de e-mail de origem consulta o servidor de DNS para mapear o endereço de destino em um endereço IP.

• O servidor de origem estabelece uma conexão TCP com o servidor destino usando o protocolo de aplicação SMTP para enviar o e-mail ao servidor destino.

• Após esta operação, o e-mail fica então armazenado no servidor de destino endereçado.



Próximo passo:

• O usuário destino no host destino, através de um aplicativo gera um comando para ler a sua caixa postal no servidor.

• Este comando usa o protocolo de aplicação POP ou IMAP, que faz uma autenticação do usuário através de seu nome e password, e após conferência, busca através destes protocolos (POP ou IMAP) os e-mails armazenados no servidor destino.

Existem três maneiras para a interação entre a máquina do usuário e o servidor de correio eletrônico:

• .As mensagens são acessadas no servidor e não são transferidas para a máquina do usuário.

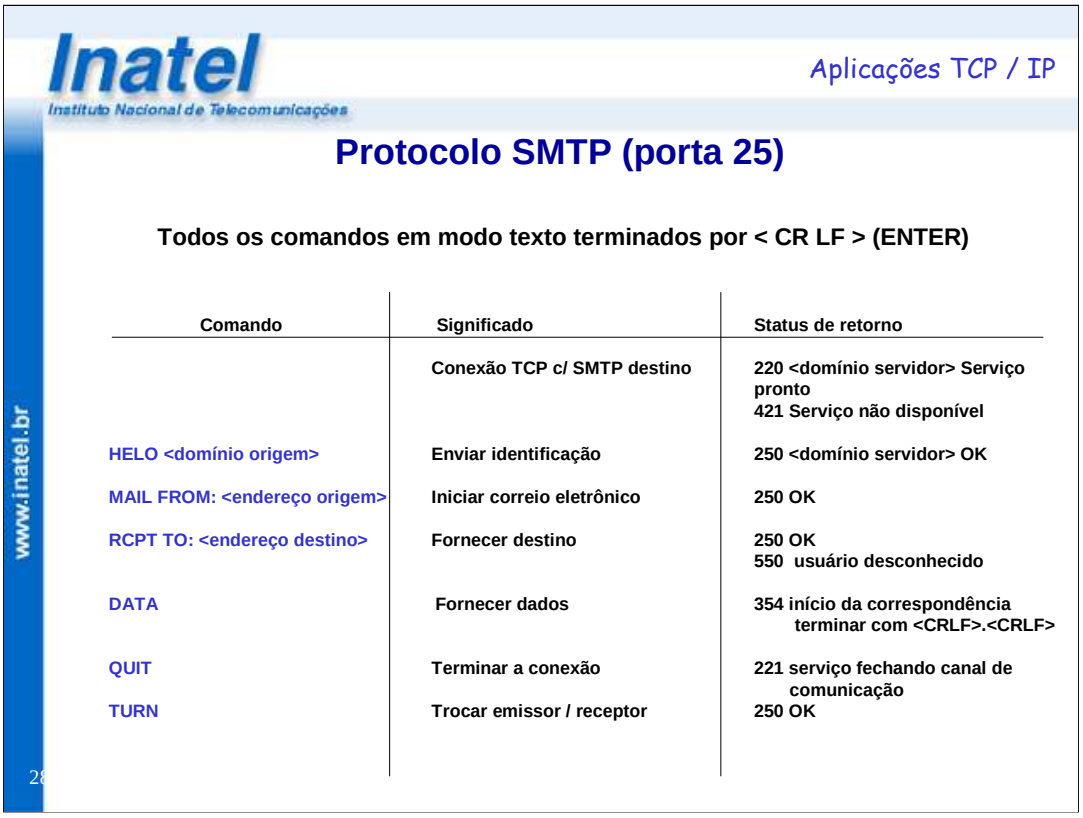
• .A máquina do usuário acessa o servidor, transfere as mensagens para o seu disco e remove as mensagens do servidor. As mensagens são então acessadas na própria máquina do usuário.

O protocolo SMTP (Simple Mail Transfer Protocol) é um protocolo da camada de aplicação na pilha de protocolo TCP / IP. Ele especifica um padrão para troca de mensagens entre máquinas, ou seja, especifica o formato exato de mensagens que um cliente utiliza em um equipamento para transferir mensagens de correio eletrônico para um servidor de outra máquina.

A comunicação entre um cliente e um servidor SMTP consiste em um texto ASCII legível. Apesar do SMTP definir rigidamente o formato do comando, as pessoas podem facilmente ler uma transcrição entre um cliente e um servidor.

O SMTP é o principal protocolo para correio eletrônico usado na Internet. Este protocolo oferece seus serviços através da porta 25 e utiliza os serviços do TCP para transporte.

O SMTP define como se dá a entrega das mensagens, mas não define as facilidades providas pelos programas de interface com o usuário.



Ainda que os comandos e respostas estejam rigidamente definidos, a troca pode ser facilmente compreendida. Todos os comandos / respostas / dados trocados são linhas de texto delimitadas por < CR LF > (ENTER). Todas as respostas possuem um código numérico no início da linha.

A seguir estão listados os principais comandos do protocolo SMTP para troca de mensagens de correio eletrônico entre um cliente e um servidor:

HELO <domínio origem>

MAILFROM: <endereço origem>

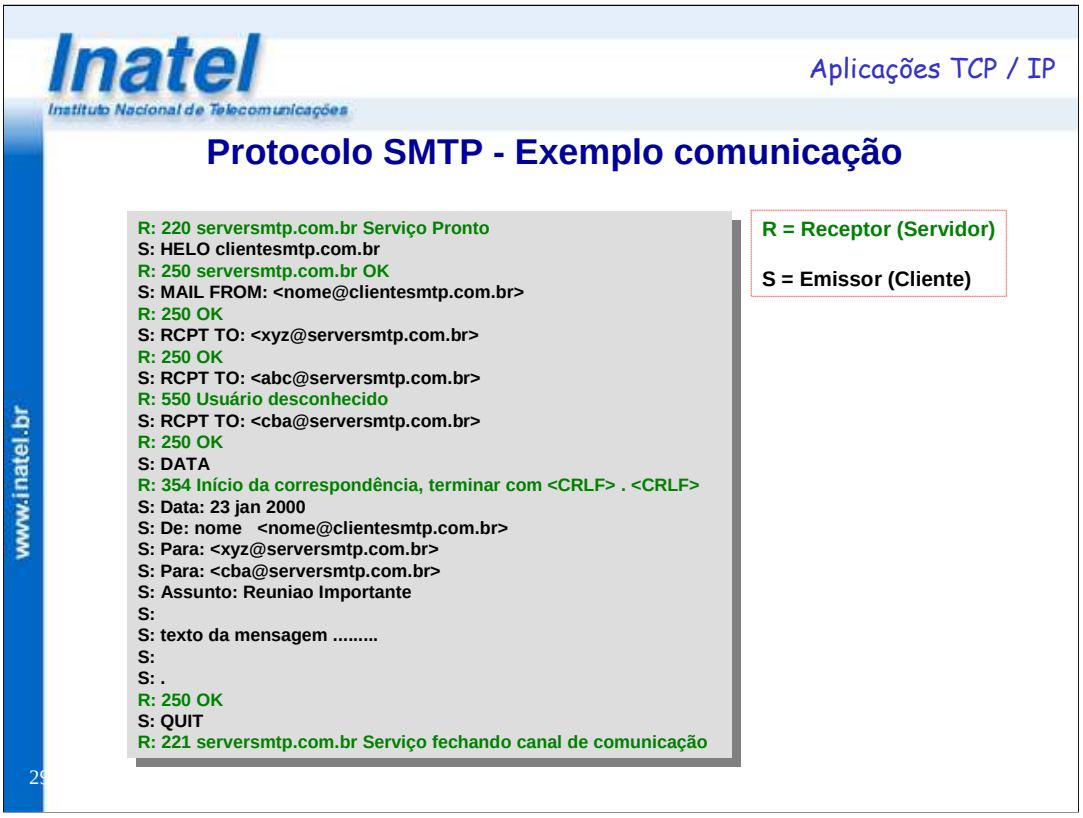
RCPT TO: <endereço destino>

DATA

QUIT

TURN

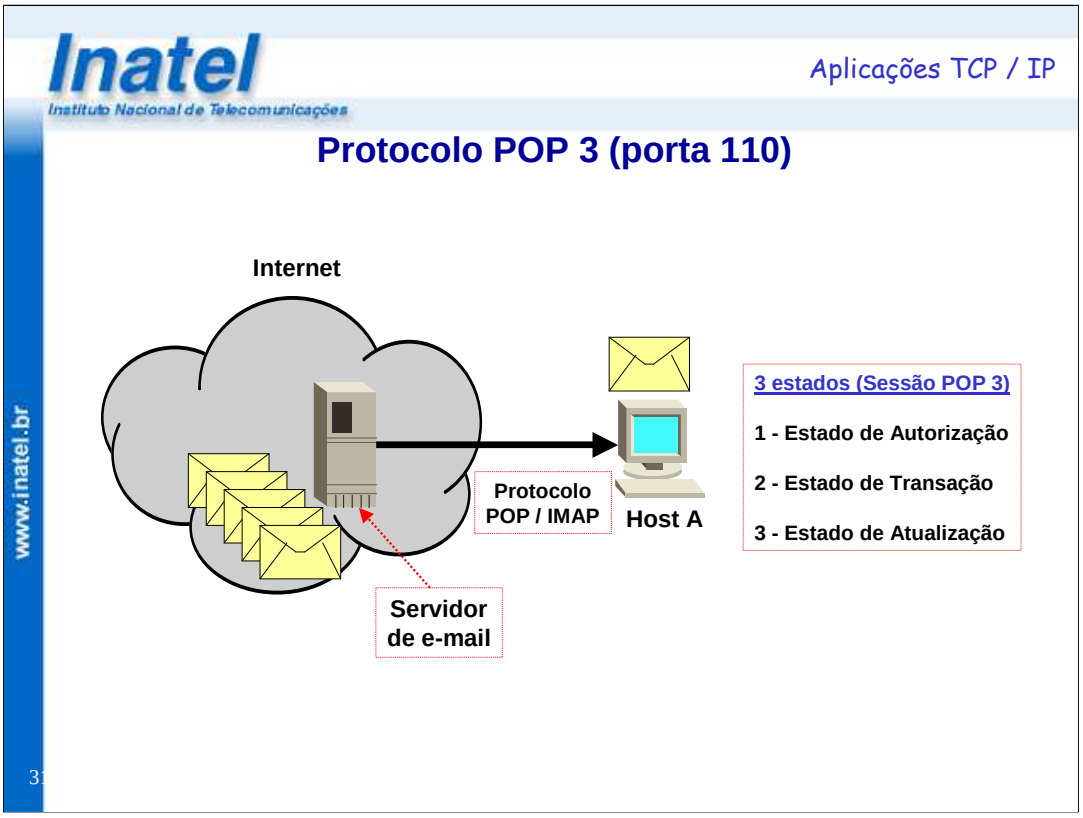
As respostas aos comandos SMTP são formadas de três dígitos seguidos por um espaço e uma linha de texto. O primeiro dígito identifica a categoria do código de resposta:



O exemplo mostra um usuário cliente enviando correspondência eletrônica para um Servidor de Correio através do protocolo SMTP.

O POP (Post Office Protocol), cuja versão atual é a 3 (por isso o nome POP 3), é um protocolo da camada de aplicação TCP / IP. E é bastante simples, sendo este o motivo de sua popularidade. O POP não define aspectos quanto à interface com o usuário, isto deve ficar a cargo do software aplicativo, nem analisa o conteúdo das mensagens. Apenas permite que as mensagens sejam transferidas de uma caixa postal em um servidor de correio eletrônico para a máquina do usuário. Para enviar mensagens o usuário precisa utilizar o SMTP.

O servidor de correio eletrônico deve ser configurado como um servidor POP e estar aguardando uma conexão TCP na porta número 110. Quando a conexão é estabelecida, o servidor e a máquina do usuário se comunicam através de comandos e respostas semelhantes aos utilizados pelo SMTP.

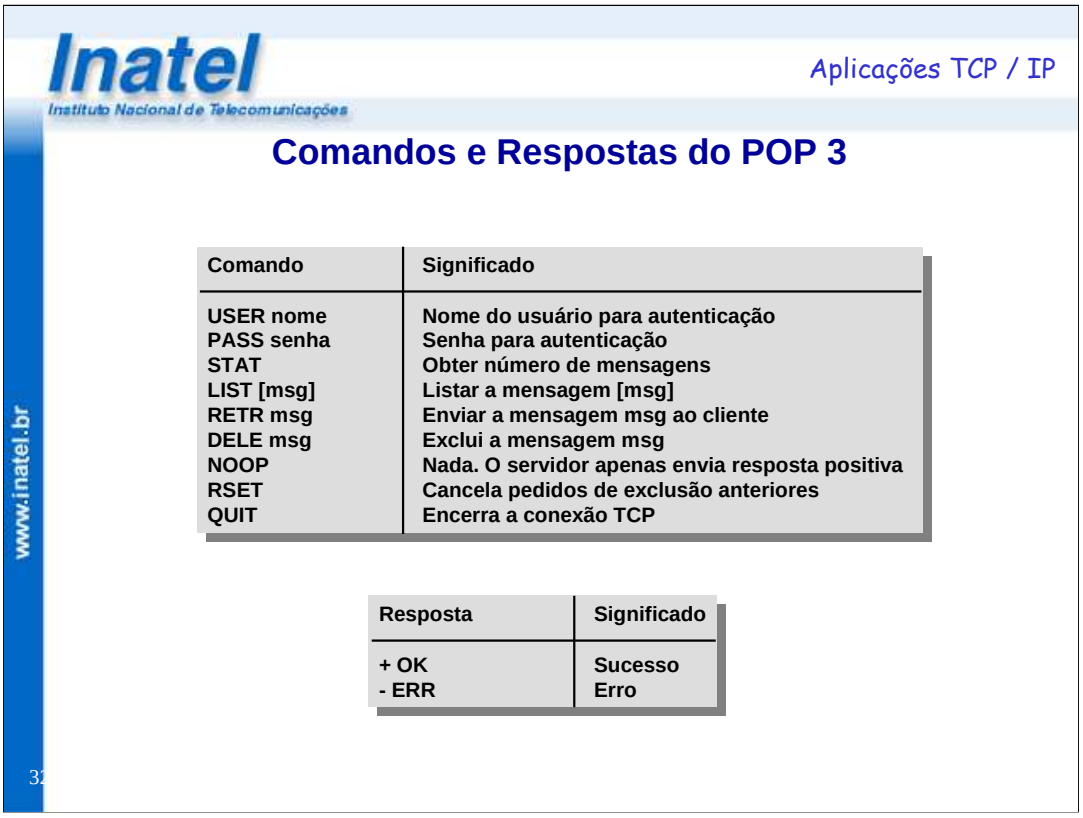


Os clientes POP 3 estabelecem uma conexão TCP com o servidor usando a porta 110. Quando a conexão é estabelecida, o servidor POP 3 envia uma mensagem de saudação ao cliente. A sessão então entra no ***estado de autenticação***. Se o servidor verifica a identificação (ID) com sucesso, a sessão entra no ***estado de transação***. Neste estado, o cliente pode acessar a caixa de correio. Quando o cliente envia o comando QUIT, a sessão entra no ***estado de atualização*** e a conexão é encerrada.

Os três estados para uma sessão POP 3 são detalhados a seguir:

Estado de Autenticação: Neste estado, o cliente envia a identificação ao servidor. Isto é implementado de duas formas: usando os comandos USER e PASS ou usando o comando APOP.

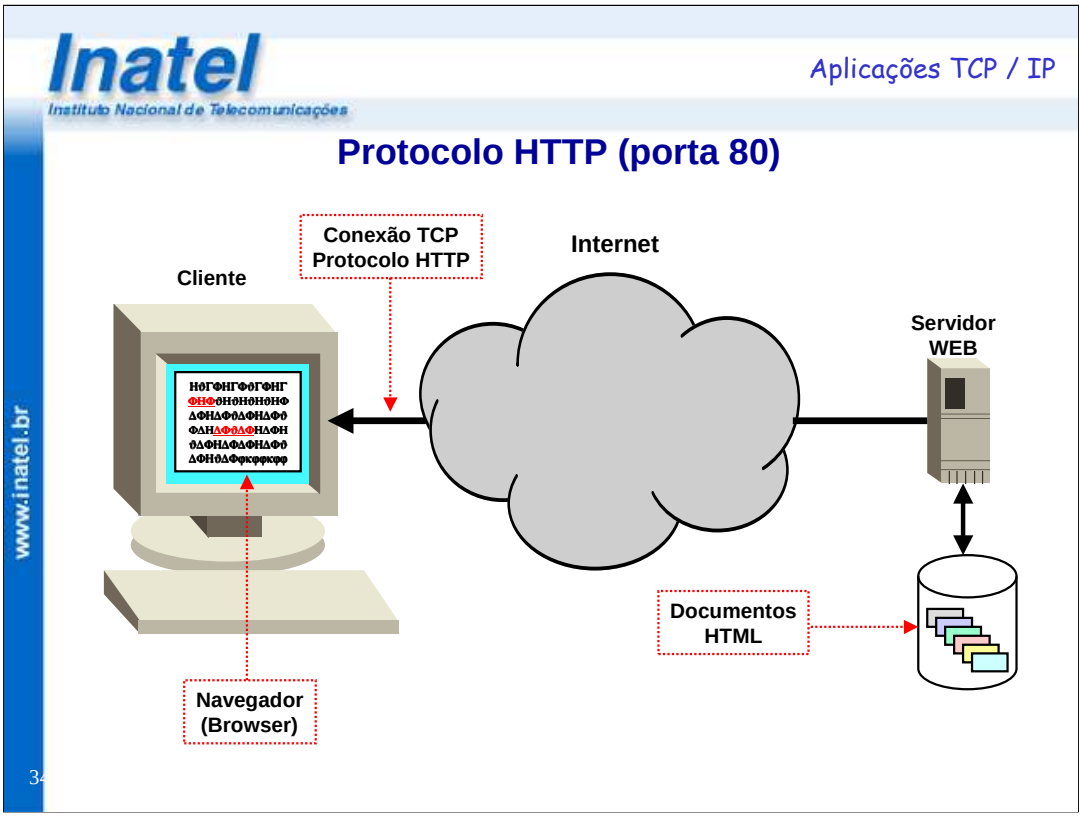
Estado de Transação: Neste estado, o cliente pode emitir comandos para listar, receber e excluir mensagens. Note que a ação da exclusão não é realizada neste estado. O cliente deve enviar o comando QUIT para sair deste estado e passar ao próximo.



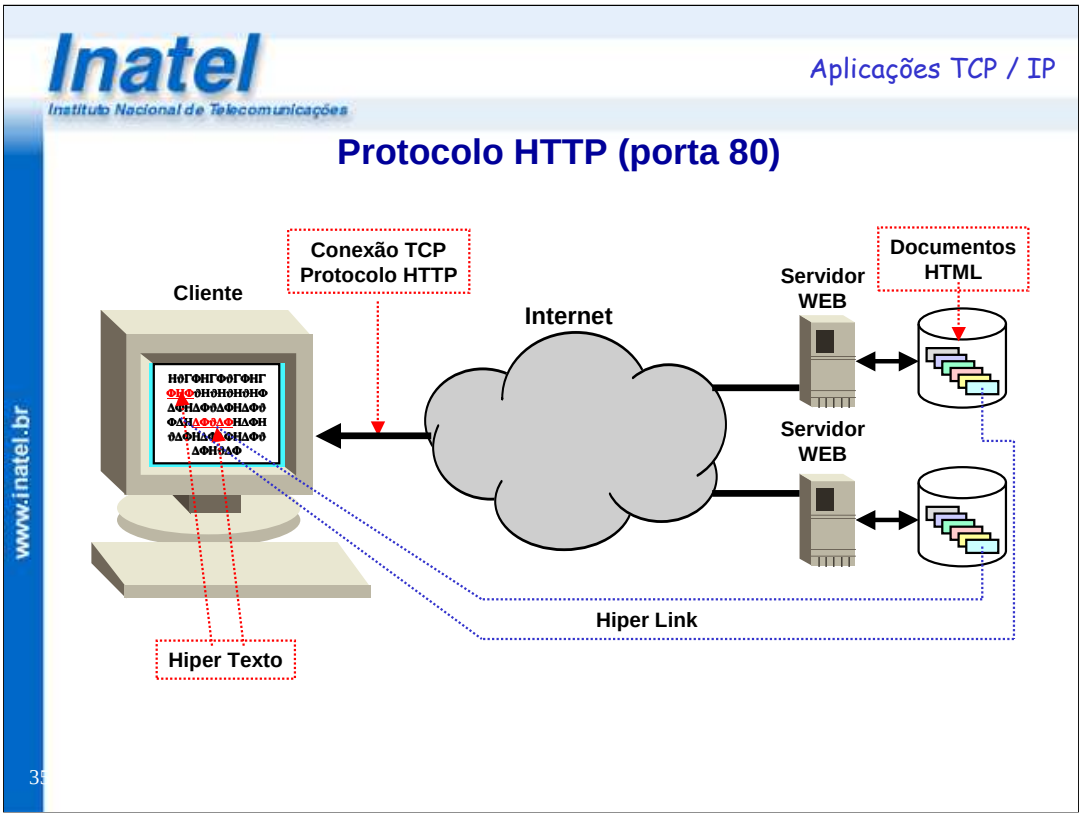
Os comandos POP 3 consistem de uma palavra-chave e eventualmente de um ou mais argumentos seguindo a palavra chave. As palavras-chave tem três ou quatro caracteres e são separadas dos argumentos por um caractere de espaço. Cada argumento pode Ter no máximo 40 caracteres de comprimento.

O servidor envia uma resposta ao comando que foi emitido pelo cliente. Esta resposta deve ser de até 512 caracteres e iniciar com um indicador de status que mostra quando a resposta é positiva (+ OK) ou negativa (- ERR). O servidor deve enviar estes indicadores em maiúsculas.

O HTTP (HyperText Transfer Protocol) é um protocolo da camada de aplicação na pilha de protocolos TCP / IP. O HTTP é um protocolo projetado para permitir a transferência de documentos HTML (HyperText Markup Language). Os documentos em HTML são a unidade de transferência de informação entre os servidores WEB e os navegadores (programa aplicativo)



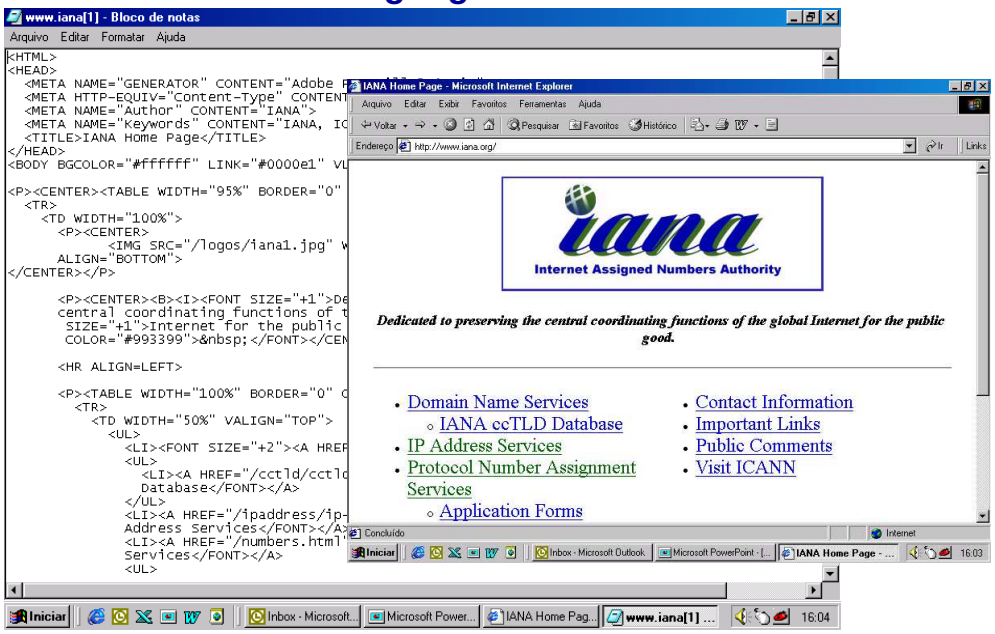
A comunicação entre servidores e navegadores ocorre através de regras definidas no protocolo de aplicação HTTP. O HTTP utiliza o TCP para transporte e presta serviço na porta 80. Esse protocolo utiliza pares de mensagens de solicitação e resposta. Cada transação normalmente resulta no estabelecimento de uma conexão TCP e não são armazenadas informações de estado entre transações. A maioria das conexões são iniciadas pelos navegadores (browsers) e encerrada pelos servidores após enviar as respostas.



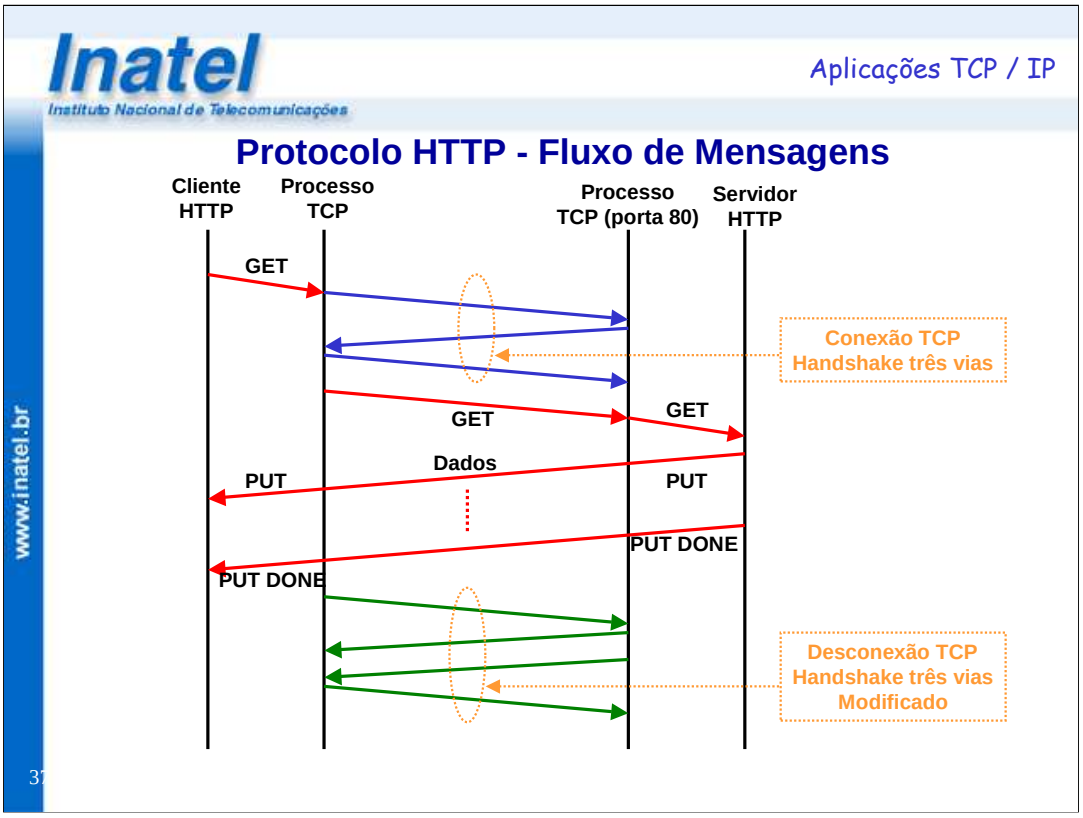
As mensagens trocadas entre navegadores e servidores podem ser de solicitação ou de resposta. As mensagens de resposta contêm um corpo com os dados e um código que informa se a solicitação foi aceita ou se algum erro ocorreu.

O HTTP é simples e descreve como os navegadores podem obter documentos dos servidores. Os dados transferidos por esse protocolo podem conter, por exemplo: texto, áudio, vídeo, etc.

Linguagem HTML



O HTML é uma linguagem usada para criar documentos de hipertexto. Estes incluem links para outros documentos que contém informações adicionais sobre a expressão ou assunto assinalado. Tais documentos podem conter outros elementos além de texto, como figuras, clipes de áudio e vídeo e applets java. Estes documentos podem estar na mesma máquina que os originais, ou em uma máquina em outra rede do outro lado do mundo !



O HTTP baseia-se em uma atividade de requisição-resposta. Um cliente, executando um aplicativo chamado de navegador, estabelece uma conexão com um servidor HTTP enviando uma requisição ao servidor na forma de um método de requisição. O servidor responde com uma linha de status, incluindo a versão do protocolo da mensagem e um código de sucesso ou erro, seguido por uma mensagem contendo informações do servidor. Uma transação HTTP divide-se em quatro etapas:

. O navegador abre a conexão

. O navegador envia um requisição ao servidor

. O servidor envia uma resposta ao navegador com os dados solicitados

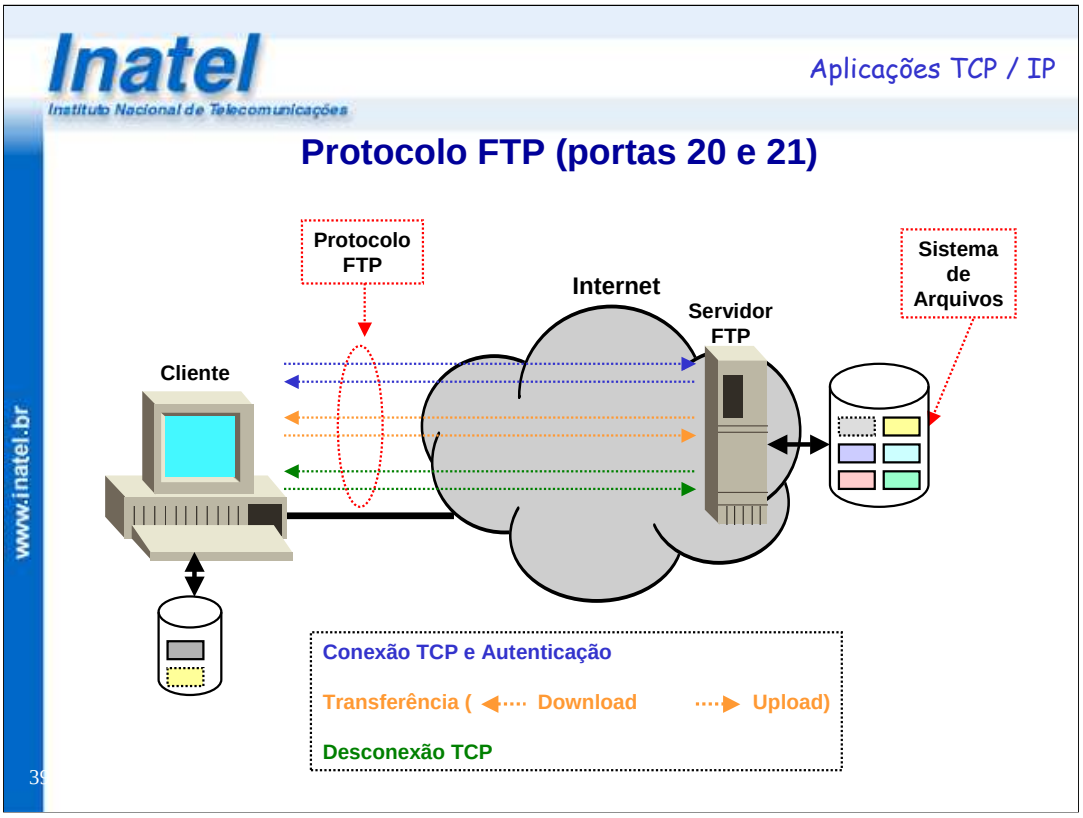
. A conexão é fechada pelo servidor

Na Internet, a comunicação HTTP geralmente ocorre em conexões TCP. A porta padrão é a de número 80, mas outras portas também podem ser usadas.

O FTP (File Transfer Protocol) é um protocolo para transferência de arquivos em uma interligação em redes TCP / IP. Ele faz parte da camada de aplicação na pilha de protocolos TCP / IP.

O FTP usa o TCP como protocolo de transporte a fim de prover conexões ponto a ponto confiáveis. E o serviço é provido nas portas 20 e21. Além de transferir arquivos, através do FTP é possível também autenticar usuários e gerenciar arquivos e diretórios.

A transferência de arquivos entre máquinas pode ser realizada de forma interativa, a partir de comandos digitados pelo usuário, ou não-interativa, a partir de comandos armazenados em um arquivo. A transferência não-interativa é normalmente programada para que se realize em um horário preestabelecido; isto possibilita, por exemplo, que arquivos grandes sejam transferidos em horários em que há pouco tráfego na rede.

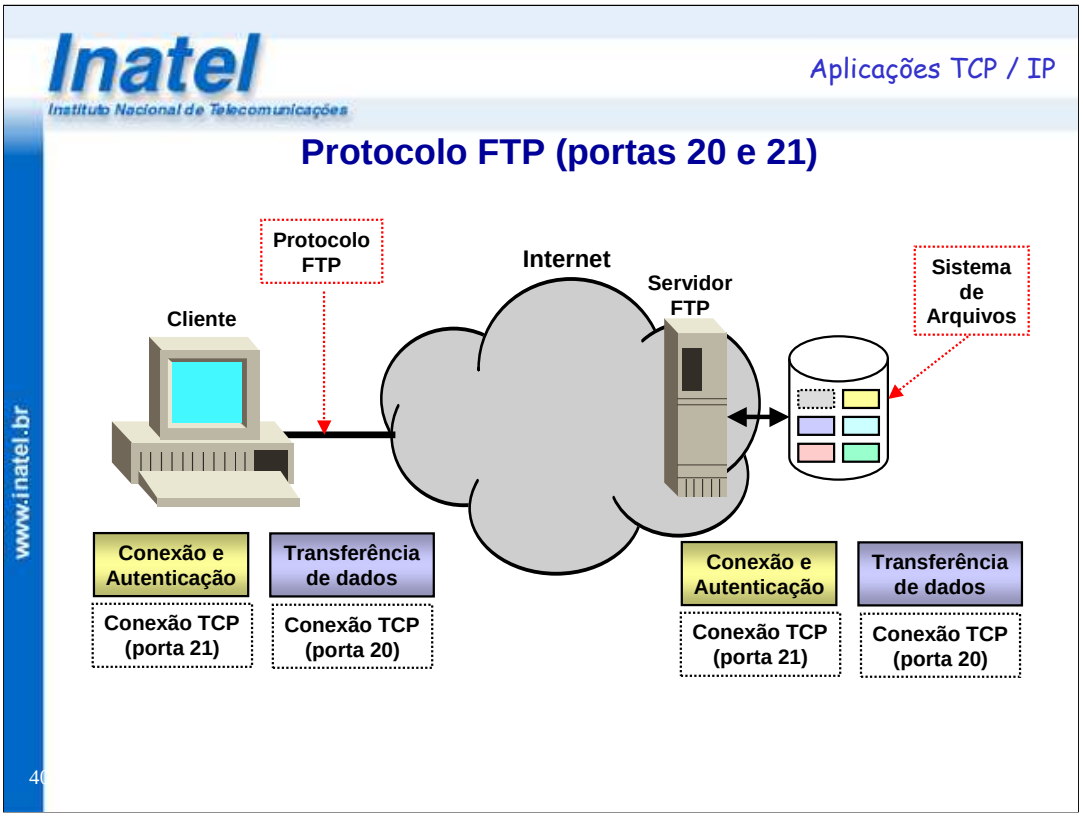


A cópia de arquivos de uma máquina para outra é uma das operações mais freqüentemente usadas. A transferência de dados entre o cliente e o servidor pode ser em ambas as direções. O cliente pode enviar um arquivo à máquina servidora. Ele pode também solicitar um arquivo deste servidor.

Para acessar arquivos remotos, o usuário deve identificar-se ao servidor. Neste ponto, o servidor é responsável por autenticar o cliente antes de permitir a transferência de arquivos.

Do ponto de vista de um usuário FTP, a ligação é orientada a conexão. Em outras palavras, é necessário ter ambos os hosts executando TCP / IP a fim de estabelecer uma transferência de arquivos.

O servidor FTP procura por conexões nas portas 20 e 21. Duas conexões são usadas: na porta 21 é para o login e na porta 20 é para gerenciar a transferência de dados. Caso seja necessário acessar o host remoto, o usuário deve ter um nome de usuário e senha para acessar os arquivos e diretórios. O usuário que inicia a conexão assume a função de cliente, enquanto que a função do servidor é fornecida pelo host remoto.



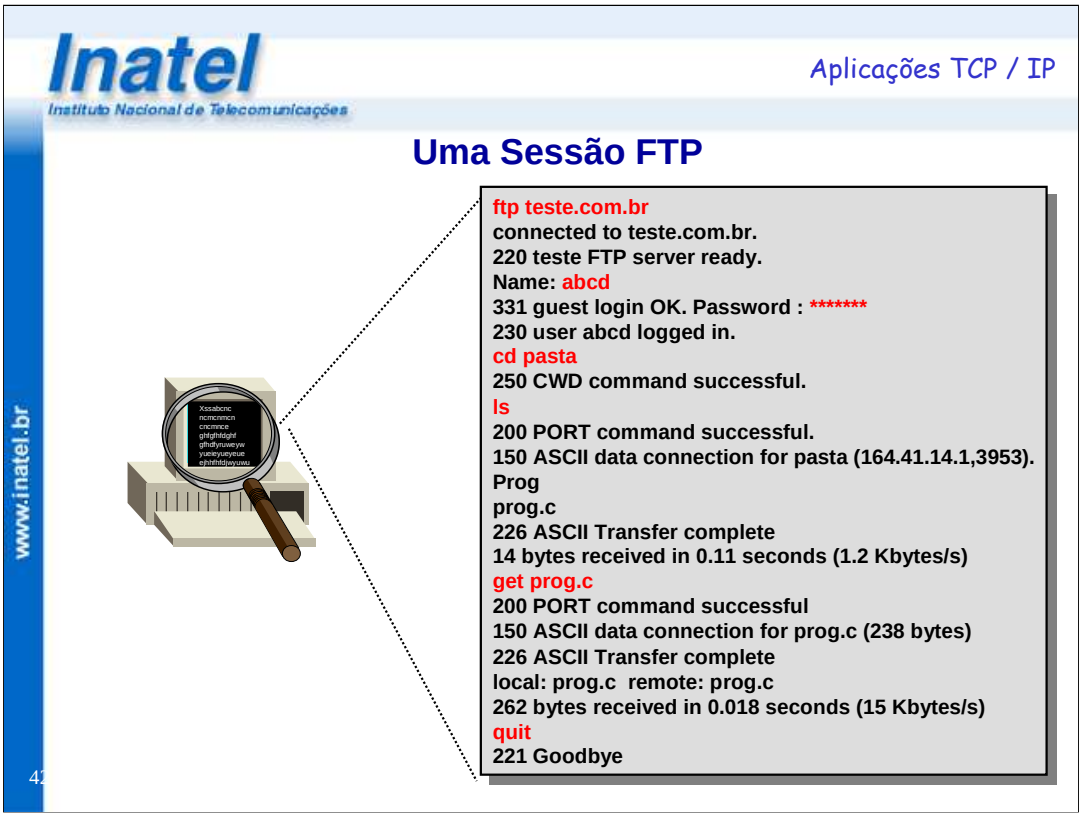
O processo de controle do cliente conecta-se ao processo de controle do servidor usando uma conexão TCP pela porta 21, enquanto que os processos de transferência de dados relacionados usam sua própria conexão TCP na porta 20. Em geral, os processos de controle e a conexão de controle permanecem ativos enquanto o usuário mantém a sessão de FTP em funcionamento. No entanto, o FTP estabelece uma nova conexão de transferência de dados para cada transferência de arquivos. Uma vez que a conexão de controle desaparece, a sessão FTP é finalizada e o software de ambas as extremidades encerra todos os processos de transferência de dados.

Além de passar os comandos ao servidor, o FTP usa a conexão de controle para permitir que os processos de controle do cliente e do servidor coordenem o uso de portas de protocolo TCP dinamicamente atribuídas e a criação dos processos de transferência de dados que usam essas portas.

Cada comando FTP resulta em pelo menos uma resposta do servidor. Cada resposta contém um código de três dígitos, um espaço e uma linha de texto .A seguir são listados alguns comandos:

cd	troca para outro diretório
close	termina a sessão
delete	apaga um arquivo
get	recebe um arquivo
help	informa sobre comandos ftp disponíveis
mget	recebe múltiplos arquivos
mput	envia múltiplos arquivos
put	envia um arquivo
pwd	informa qual é o diretório atual
quit	termina a sessão e abandona

O comando help pode ser usado para se obter uma descrição resumida de cada um dos comandos.



Este é um exemplo de uma sessão FTP, através do qual uma conexão é estabelecida e alguns comandos são executados.

O FTP é ativado na máquina do usuário pelo comando ftp, o qual aceita várias opções. Além das opções, é possível especificar o nome ou o endereço da máquina na qual o serviço é prestado.

Uma vez estabelecida a conexão, o usuário especifica o nome da conta e a senha para acesso. Uma vez autenticado, o usuário é posicionado no diretório raiz da conta cujo nome foi especificado. Após a autenticação, o prompt é apresentado e comandos podem ser digitados. Muitas instalações TCP / IP implementam o que é conhecido como FTP anônimo, que significa permitem acesso público a alguns diretórios de arquivos. O usuário remoto precisa apenas usar o nome de login anonymous e a senha guest. Um usuário identificado por anonymous tem direitos limitados de acesso às informações armazenadas no servidor.

TFTP (Trivial File Transfer Protocol) é executado sobre o UDP. O TFTP não necessita da senha do usuário para acesso, não opera com múltiplas conexões, tornando-se, portanto, menor e mais simples que o *FTP*. Opera no modo de transferência de blocos com tamanho fixo de 512 *bytes*, aguardando uma mensagem de reconhecimento para cada bloco transmitido antes de enviar o próximo. É especificado pela [RFC 1350] e usa a porta 69 do UDP.

O protocolo TFTP é uma opção para que não necessita da robustez do protocolo FTP. TFTP usa o protocolo UDP para fazer a entrega do pacote ao contrario do protocolo FTP que usa o protocolo TCP. O uso do TFTP é voltado para aqueles que não necessitam de uma certa precisão na entrega dos pacotes, e também não requeiram uma visualização dos diretórios e bem como uma autenticação do usuário que esta acessando o TFTP servidor.

Protocolo SNMP

- SNMP – Simple Network Management Protocol (RFC 1157)
- Protocolo padrão da Internet para gerenciar dispositivos em redes IP
- MIB (*Management Information Base*): É um banco de dados armazenado no elemento a ser gerenciado
  - Informações Estáticas
    - Configurações de equipamentos (identificação, modelo, etc)
  - Informações Dinâmicas
    - Relacionada a eventos na rede (número de pacotes recebidos, número de colisões, etc).
  - Informações Estatísticas
    - São derivas da informações dinâmicas

As informações armazenadas na MIB estão divididas em dois grupos: estáticas e dinâmicas.

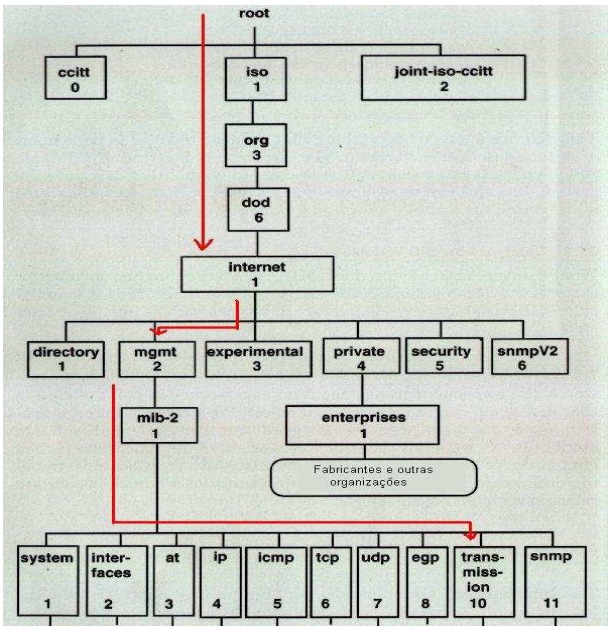
• Informações Estáticas: As informações estáticas são aquelas informações que não se alteram durante a operação da rede. Nestas informações podemos obter as configurações do equipamento, sua identificação (modelo, fabricante, etc).

• Informações Dinâmicas: As informações dinâmicas são variáveis que se alteram durante a operação da rede. Nestas informações dinâmicas é que poderemos obter dados que nos permitem medir o desempenho da rede. Valores como número de pacotes enviados e recebidos, número de colisões, entre outros, podem ser obtidos.

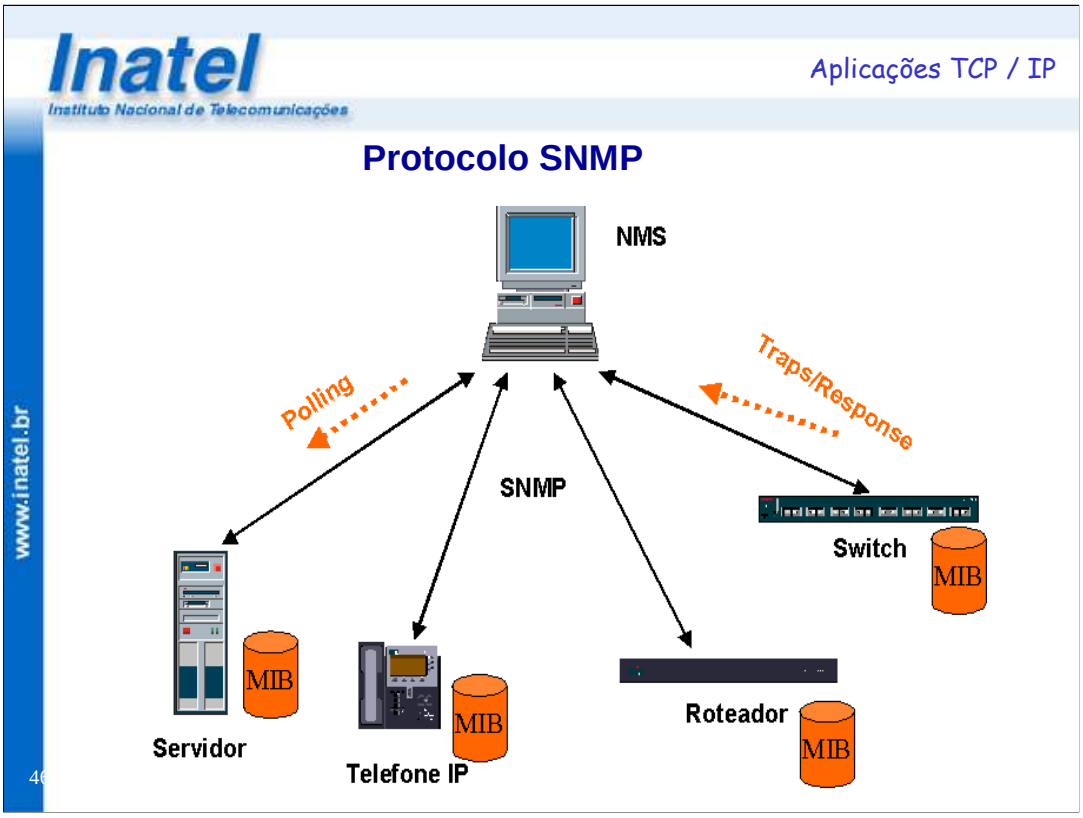
• Informações Estatísticas: As informações estatísticas são derivadas das informações estáticas obtidas. São necessárias operações matemáticas para chegarmos a estes valores. Por exemplo, a utilização de um enlace será obtido a partir da medida da variação do número de bits enviados em intervalos regulares de tempo.

Protocolo SNMP

- Dados armazenados em forma de árvore

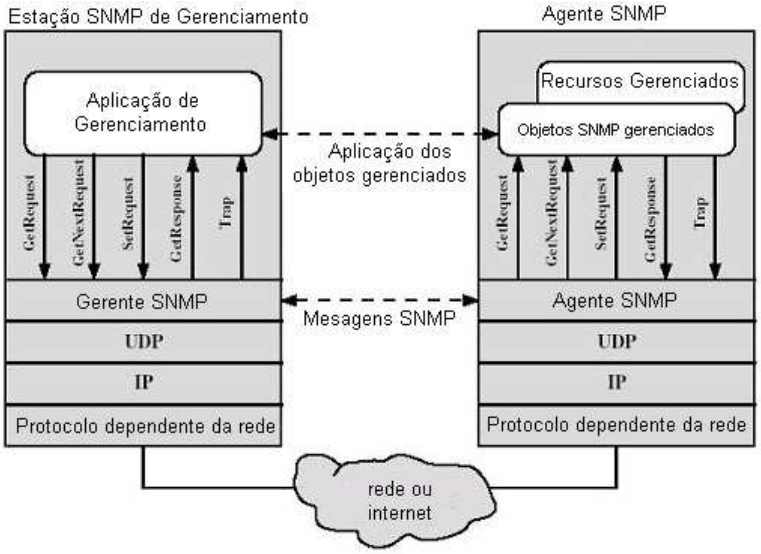


A estrutura usada para o armazenamento de dados na MIB é na forma de uma árvore. Para acessarmos uma determinada variável dentro da MIB devemos indicar todo o caminho até esta variável.



A família de protocolos TCP/IP possui um protocolo para coleta de dados em MIB's: o protocolo SNMP.

Protocolo SNMP



A estação de gerenciamento SNMP deve acessar, através da rede, os equipamentos gerenciados para realizar a coleta de dados da MIB.

SNMP – Versão 1

- Protocolo usado para o acesso a dados armazenados nas MIB's
- Transportado sobre UDP
  - Simplicidade
- Problemas de segurança
- Implementa apenas 5 funções

Todas as versões do protocolo SNMP são bastantes simples. Basicamente a função deste protocolo é coletar dados na MIB dos equipamentos gerenciáveis. Em todas as versões o transporte do protocolo SNMP é feito pelo protocolo UDP.

A versão 1 do protocolo SNMP implementa apenas 5 funções para acesso aos dados na MIB. Esta versão não possui nenhum mecanismo de segurança, como formas de autenticar o usuário.

As 5 funções implementadas pelo protocolo SNMP são:

• *Get-Request*: Esta função é usada para acessar uma variável específica na MIB do elemento.

• *Get-Netx-Request*: Esta função é usada para o acesso a valores em seqüência na MIB do equipamento. Ela é útil quando estamos buscando vários valores de forma seqüencial na MIB.

• *Set-Request*: É a função usada para alterar valores na MIB do equipamento.

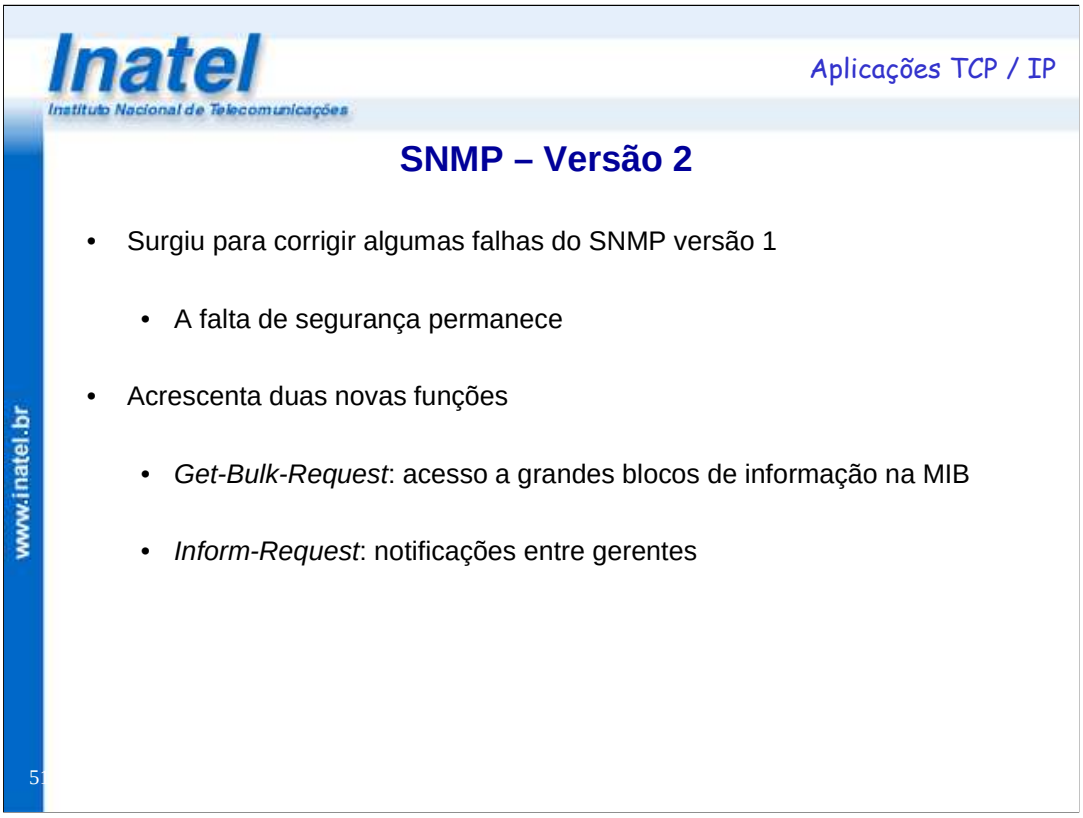
• *Get-Response*: Esta função é usada como resposta das 3 funções anteriores.

• *Trap*: Esta função é usada pelo equipamento gerenciado para notificar ao gerente a ocorrência de um evento que necessita de tratamento por parte do gerente. Nos procedimentos de gerencia o gerente consulta a MIB em intervalos de tempo regulares. A função *Trap* permite que seja enviada uma notificação ao gerente para que sejam tomadas ações antes do intervalo regular de leitura.

SNMP – Versão 1

Formato da Mensagem *Get-Next-Request*

GET-NEXT var: obj(5) 1 3 6 1 2 1 val: empty(0)	Qual é a primeira variável em sua MIB?
RESPONSE var: obj 1 3 6 1 2 1 1 1 0 val: string "Sun SNMP Agent, SPARCStation 1+, Company Property Number 123456"	sysDescr Esta é uma SPARCStaion Sun
GET-NEXT var: obj 1 3 6 1 2 1 1 1 0 val: empty	O que vem após o sysDescr?
RESPONSE var: obj 1 3 6 1 2 1 1 2 0 val: obj 1 3 6 1 4 1 42 2 1 1	sysObjectID O identificador determinado pelo fabricante
GET-NEXT var: obj(8) 1 3 6 1 2 1 1 2 0 val: empty(0)	O que vem após o sysObjectID?
RESPONSE var: obj(8) 1 3 6 1 2 1 1 3 0 val: time(3) 0x0da372	sysUpTime 893,810 centenas de segundos (cerca de 2,5 minutos) desde o inicianlização
GET-NEXT var: obj(8) 1 3 6 1 2 1 1 3 0 val: empty(0)	O quem após o sysUpTime?
. . .	Continua e passa por sysContact, sysName e sysLocation.
GET-NEXT var: obj 1 3 6 1 2 1 1 6 0 val: empty	O que vem após sysLocation?
RESPONSE var: obj 1 3 6 1 2 1 1 7 0 val: int 0x48	sysServices O código hexadecimal 48 indica que é um host que executa serviços de aplicação.
GET-NEXT var: obj 1 3 6 1 2 1 1 7 0 val: empty	O que vem após sysServices?
RESPONSE var: obj 1 3 6 1 2 1 2 1 0 val: int 0x02	ifNumber Há duas interfaces para este dispositivo



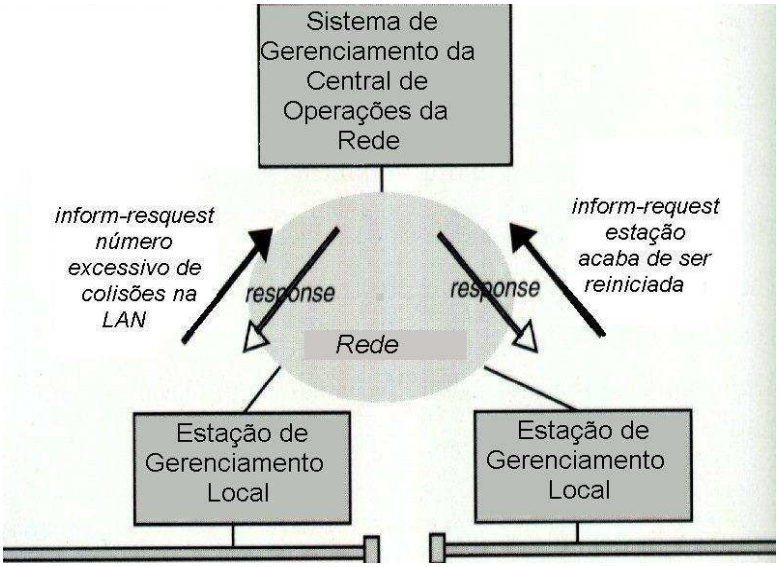
A versão 2 do protocolo SNMP acrescenta duas novas funções ao SNMP. O problema da falta de segurança não foi resolvido nesta versão (apenas na versão 3 ele é resolvido).

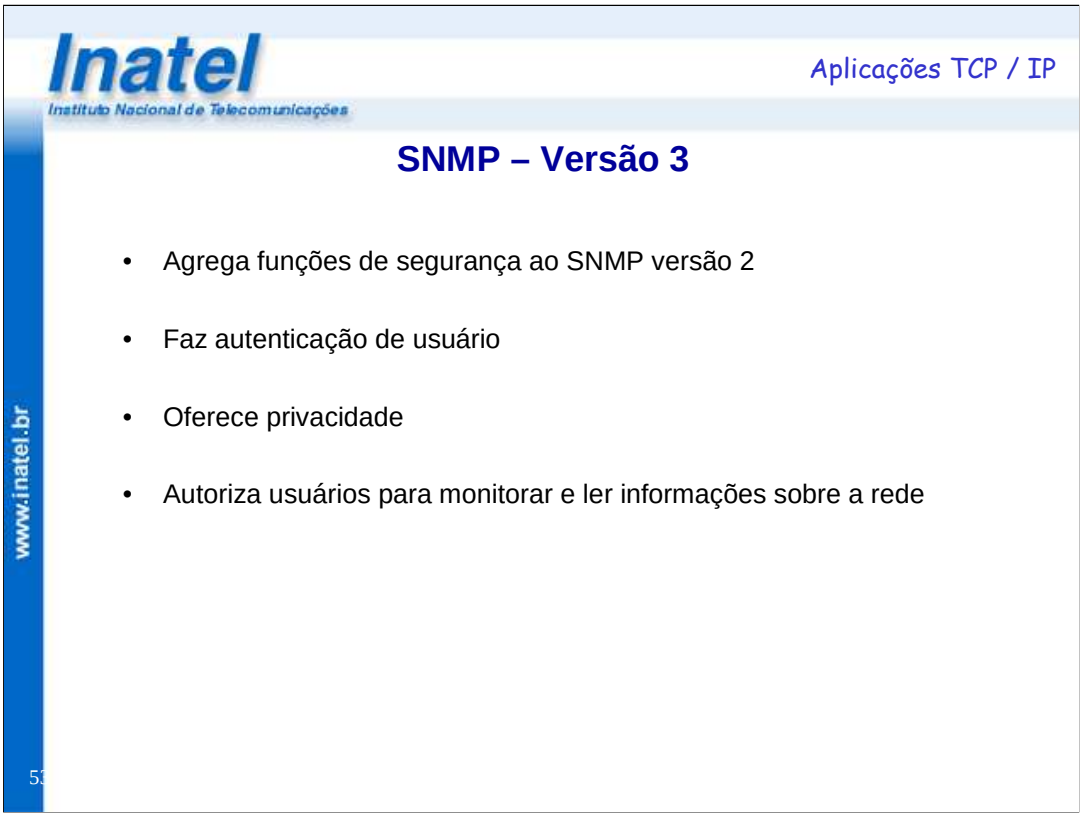
As duas novas funções são:

• *Get-Bulk-Request*: Usada para acessar grandes blocos de dados. Normalmente estes grandes blocos de dados são armazenados na forma de vetores ou matrizes. Ao invés de fazer a leitura individual de valores (com o uso do *Get-Request* ou do *Get-Next-Request*) esta função permite a transferência de um bloco de variáveis.

• *Inform-Request*: Esta função foi adicionada para permitir as implementações de gerência descentralizada. Nesta operação gerentes são responsáveis pelo monitoramento de um grupo de elementos e depois estes gerentes notificam somente os resultados ao "gerente geral" da rede.

SNMP – Versão 2





Na versão 3 do protocolo SNMP foram incluídas as funções de segurança. É possível fazer a autenticação de usuários.

Nesta versão as informações podem ser enviadas criptografadas (para garantir a privacidade) e também é possível definir usuários que poderão ter acesso a determinadas informações da MIB.