Inatel
Instituto Nacional de Telecomunicações

T202 – B/C
Redes de Computadores

04 – Protocolos de Aplicação II
(Principais protocolos)

Prof. Edson J. C. Gimenez
soned@inatel.br

2024/Sem2

Referência principal:

- ✓ Kurose & Ross. Redes de Computadores e a Internet: uma abordagem top-down. Capítulo 2.

Outras referências:

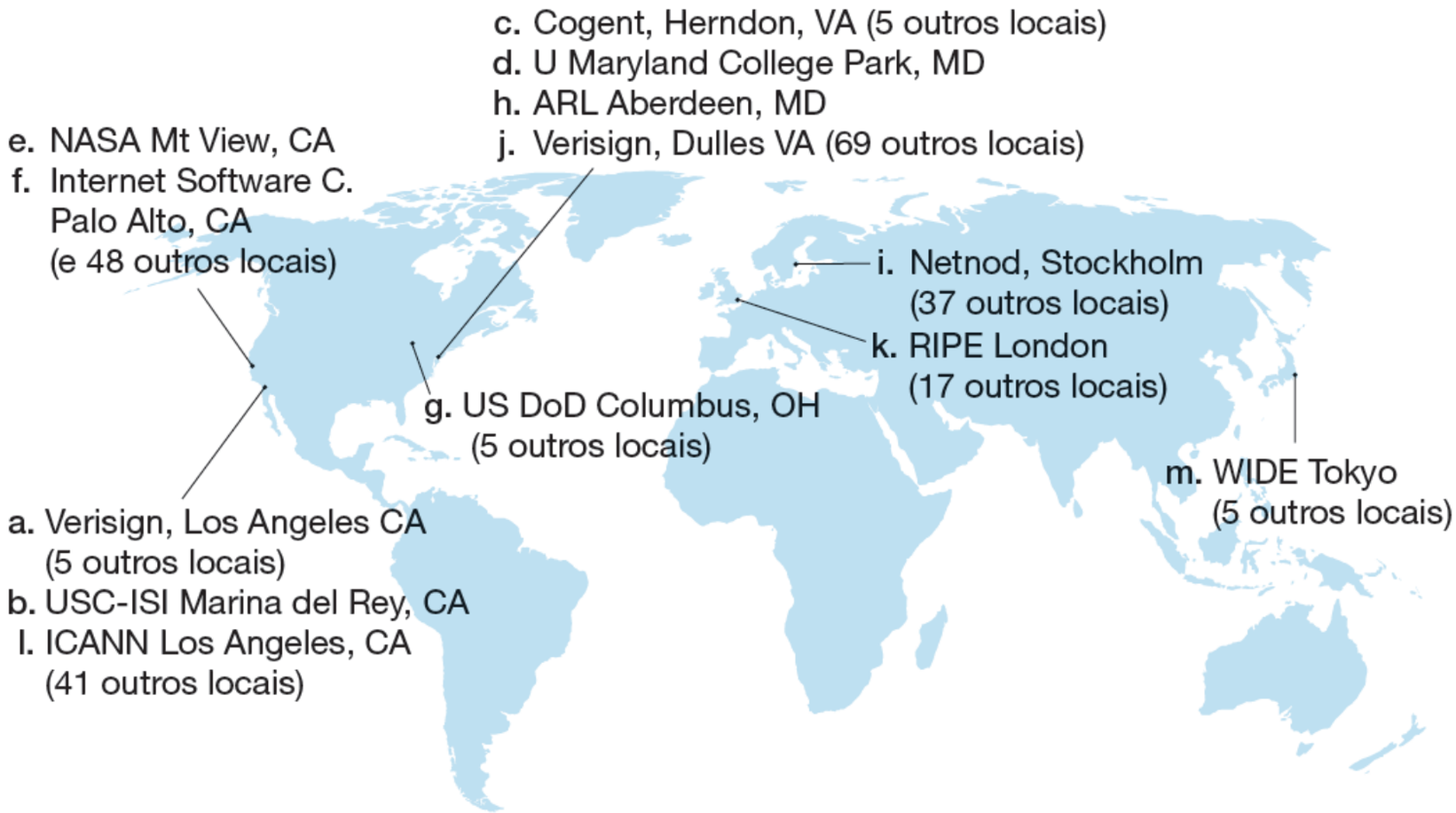
- ✓ Tanenbaum & Wetherall. Redes de Computadores; capítulo 7.
- ✓ Farrel. A Internet e seu Protocolos: uma Análise Comparativa; capítulo 12.
- ✓ Forouzan & Mosharraf. Redes de Computadores: uma abordagem top-down; capítulo 2.
- ✓ Comer. Interligação de Redes com TCP/IP; volume 1; capítulos 23 a 27 e 29.

DNS (Domain Name System).

- ✓ Há duas maneiras de identificar um hospedeiro:
  - um nome → inatel.br
  - um endereço IP → 131.221.240.5
- ✓ Para conciliar isso, é necessário um serviço de diretório que **traduza nomes de hospedeiro para endereços IP**. Esta é a tarefa principal do DNS.
- ✓ Assim, o servidor de nomes de domínios (DNS) pode ser visto como:
  1) Um banco de dados distribuído, executado em uma hierarquia de servidores: raiz, TLD (auto nível) e autoritativos.
  2) Um protocolo de camada de aplicação que permite que hospedeiros consultem esse banco de dados distribuído.
- ✓ Definido nas RFCs 1034 e 1035 (nov/1987), além de diversas atualizações.
- ✓ Faz uso da porta UDP 53.

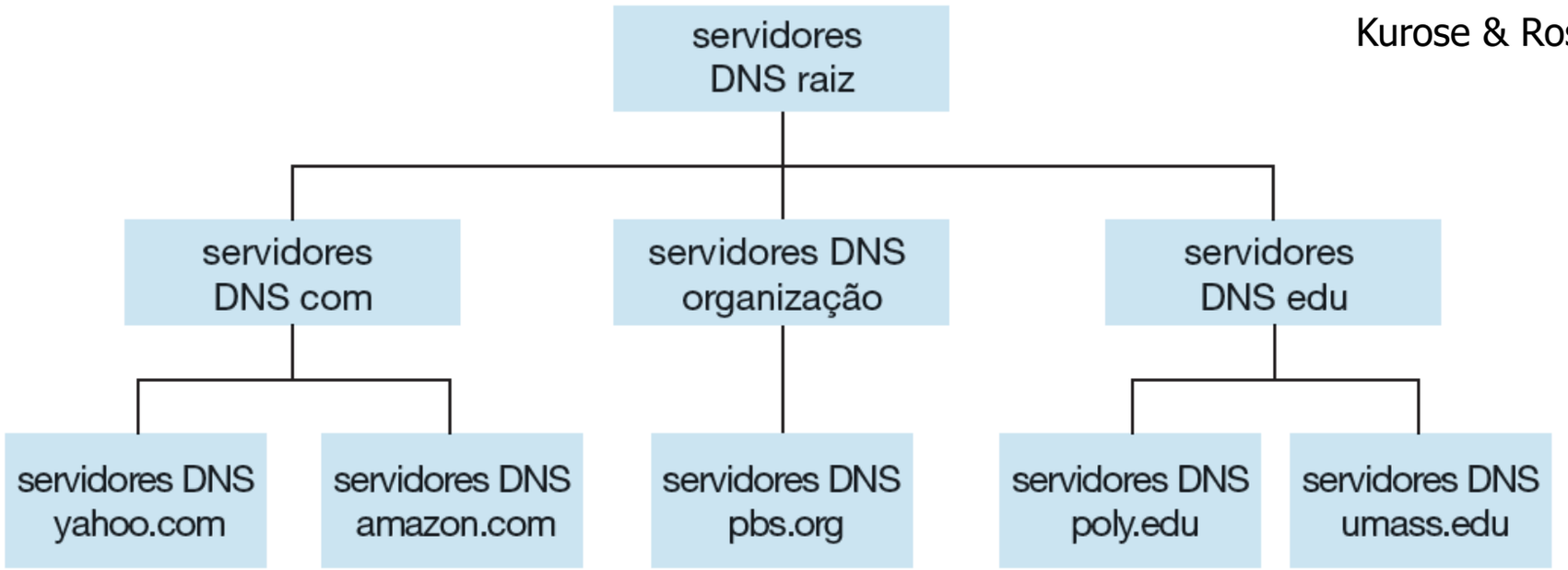
Servidores DNS raiz.

- ✓ Na Internet há 13 servidores DNS raiz (denominados de A à M), a maior parte deles localizados na América do Norte.
  - Na realidade, cada um é um conglomerado de servidores replicados, para fins de segurança e confiabilidade.



- ✓ Servidores DNS de Domínio de Alto Nível (TLD).
  - São responsáveis por domínios de alto nível como *com*, *org*, *net*, *edu* e *gov*, e por todos os domínios de alto nível de países (*uk*, *fr*, *br,* etc.*)*
- ✓ Servidores DNS autoritativos.
  - São responsáveis por abrigar os registros DNS acessíveis publicamente de uma organização
- ✓ Há ainda os servidores DNS locais, que não pertencem propriamente à hierarquia de servidores DNS

Exemplo hierarquia de servidores DNS:



Kurose & Ross

Serviço de diretório na Internet

Operação básica: cis.poly.edu deseja obter o end. IP de gaia.umas.edu:

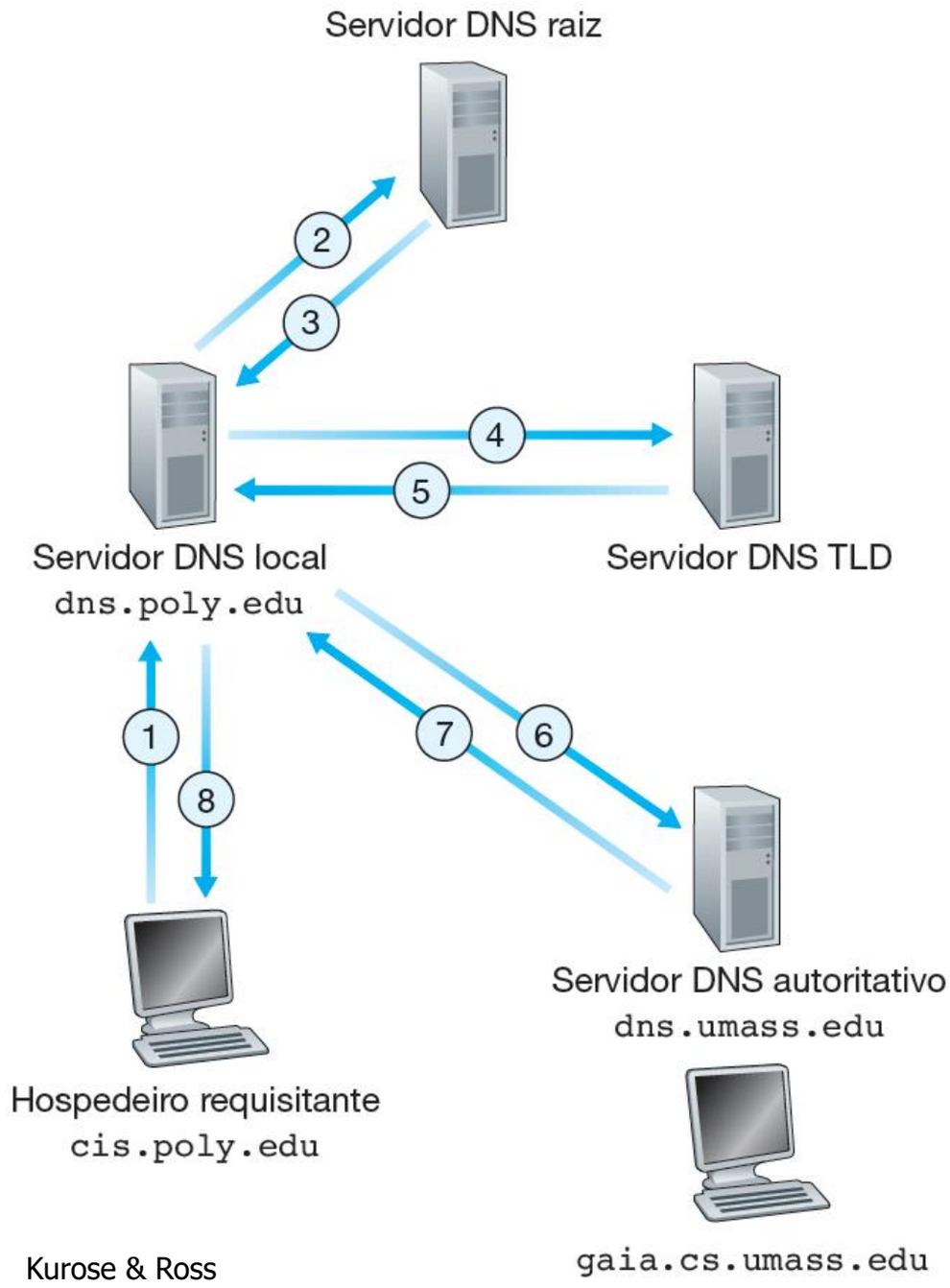
(1) cis.poly.edu consulta seu servidor local (dns.poly.edu).

(2) dns.poly.edu consulta o servidor raiz, que (3) retorna uma lista de servidores TLD responsáveis por .edu.

(4) dns.poly.edu consulta um servidor TLD responsável por .edu, que (5) retorna o endereço IP de um servidor autoritativo do sufixo umas.edu.

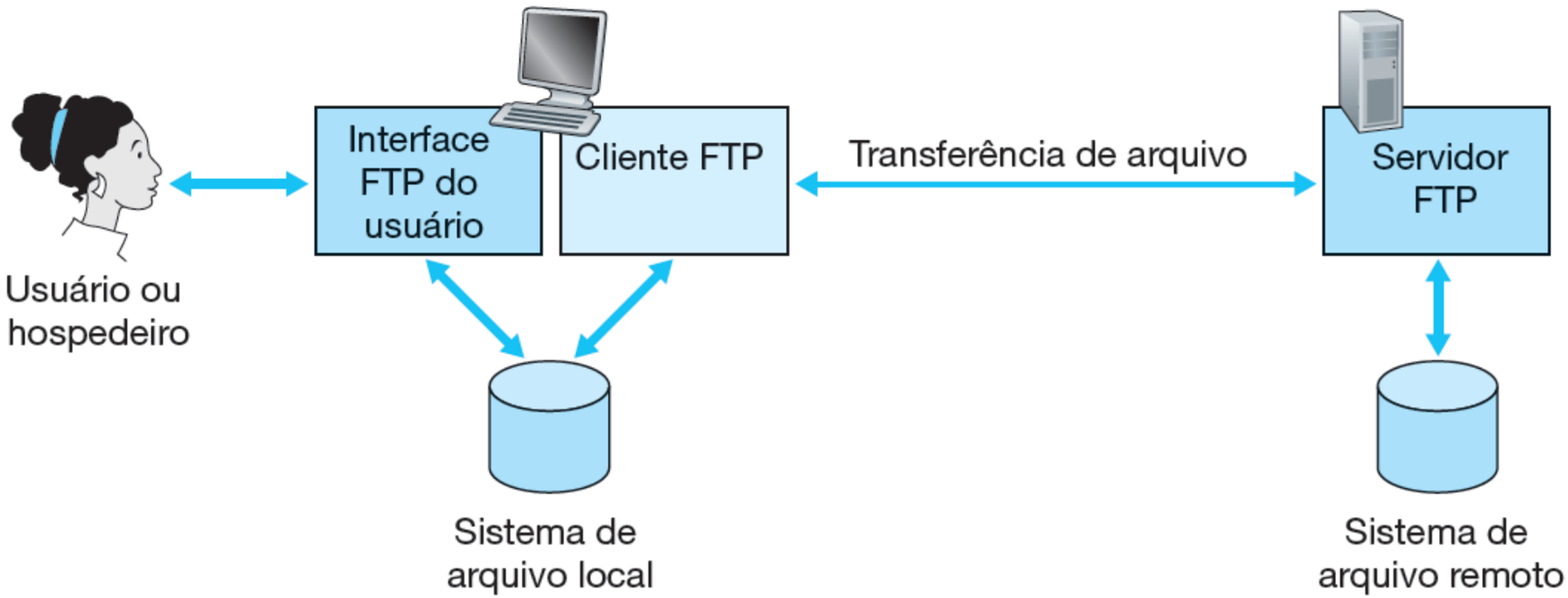
(6) dns.poly.edu consulta o servidor dns.umas.edu, que (7) responde com o endereço IP de gaia.cs.umas.edu.

(8) dns.poly.edu envia ao cis.poly.edu o endereço IP solicitado, e armazena uma cópia para futuras solicitações.



File Transfer Protocol

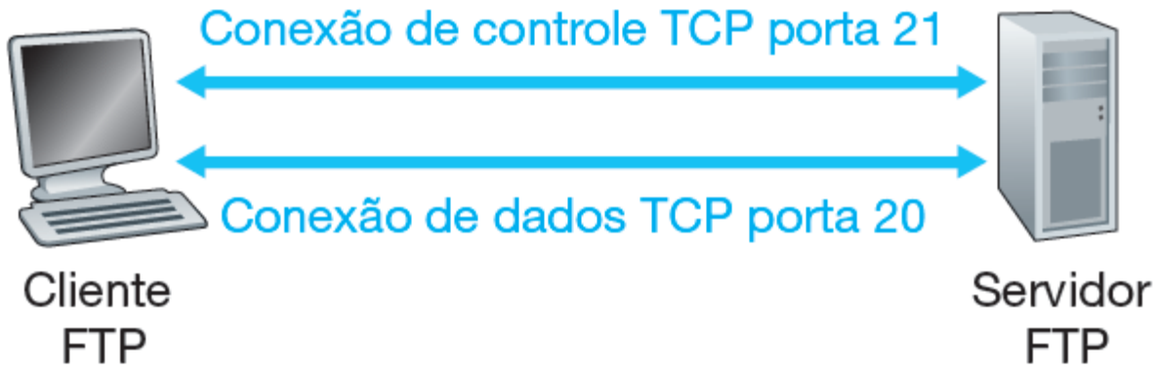
- ✓ Definido na RFC 959 (maio/1983), e atualizações, permite transferências de arquivos entre um cliente e um servidor.
- ✓ A transferência de dados pode acontecer em ambas as direções.
  - ▫ O cliente pode baixar dados do servidor ou o cliente pode fazer upload (enviar) de dados para o servidor.



Kurose & Ross

File Transfer Protocol

- ✓ O FTP faz uso de duas conexões: uma para controle e uma para dados
- ✓ Controle de tráfego (porta TCP 21): para comandos do cliente e respostas do servidor; permanecendo aberta durante toda sessão.
- ✓ Dados (porta TCP 20): para a transferência de dados propriamente; sendo que uma nova conexão é criada para cada novo arquivo a ser transferido.



Kurose & Ross

Operação FTP

- ✓ O cliente FTP (usuário) inicia primeiro uma conexão TCP de controle com o servidor, porta numero 21 do servidor, e envia por essa conexão de controle sua identificação e senha, além de comandos para mudar o diretório remoto.
- ✓ Quando o lado servidor recebe (pela conexão de controle) um comando para uma transferência de arquivo (de ou para o hospedeiro remoto), abre uma conexão TCP de dados (porta 20).
- ✓ O FTP envia pela conexão de dados o arquivo solicitado e em seguida fecha a conexão.
- ✓ Se durante a mesma sessão, o usuário quiser transferir outro arquivo, o FTP abrirá outra conexão de dados.
- ✓ Observa-se que a conexão de controle permanece aberta durante toda a sessão do usuário, mas uma nova conexão de dados é criada para cada arquivo transferido dentro de uma sessão.

Comandos típicos FTP:

- *USER username*: enviar a identificação do usuário ao servidor.
- *PASS password*: enviar a senha do usuário ao servidor
- *LIST*: pedir ao servidor que envie uma lista com todos os arquivos existentes no atual diretório remoto. A lista de arquivos e enviada por meio de uma conexão de dados, e não pela conexão de controle.
- *RETR filename*: solicita ao hospedeiro remoto que abra uma conexão de dados e envie o arquivo requisitado por essa conexão.
- *STOR filename*: usado para armazenar um arquivo no diretório atual do hospedeiro remoto.
- Etc.

Obs.: cada comando é seguido de uma resposta.

Mensagens típicas de resposta:

- 331 Nome de usuário OK, senha requisitada
- 125 Conexão de dados já aberta; iniciando transferência
- 425 Não é possível abrir a conexão de dados
- 452 Erro ao escrever o arquivo

Trivial File Transfer Protocol

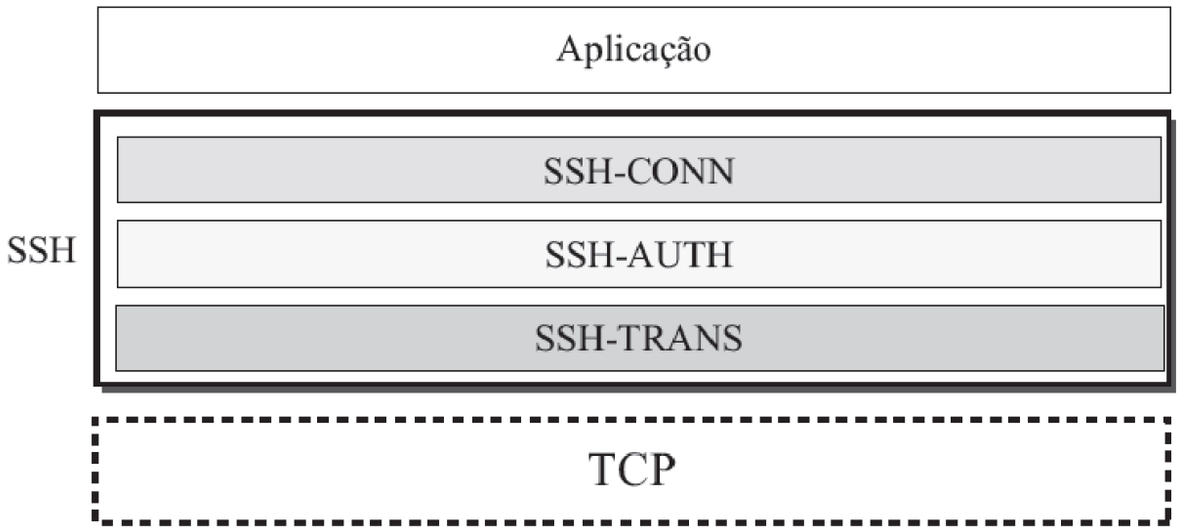
- ✓ Definido na RFC 1350 (julho/1992)
- ✓ Oferece um serviço de transferência de arquivos baseado no protocolo UDP (porta 69), portanto não orientado à conexão e não confiável.
- ✓ Desenvolvido para ser leve e de fácil implementação, sendo mais rápido que o FTP.
- ✓ Pode ler ou gravar arquivos de e para um servidor remoto porém, por ser não confiável, não possui recursos de autenticação.
- ✓ Usado, normalmente para transferência de arquivos pequenos, tais como arquivos de configuração e arquivos imagens de sistemas (sistema operacional) de equipamentos.

Telnet Protocol

- Permite acessar um dispositivo remoto, que esteja executando uma aplicação de servidor Telnet e, em seguida, acessar todos os seus recursos disponíveis.
  - Não utiliza qualquer recurso de processamento do computador cliente. O que ele faz é transmitir as teclas digitadas localmente ao dispositivo remoto e enviar a saída na tela de volta ao monitor local.
  - Todo o processamento e o armazenamento ocorrem no dispositivo remoto.
- Apesar da necessidade de autenticação para o acesso remoto, o Telnet não é um protocolo seguro.
  - Para acesso remoto no modo seguro, com autenticação e criptografia dos dados, utiliza-se o protocolo Secure Shell (SSH).
- Telnet: RFC 318 (abril/1972)
- Faz uso da porta TCP 23.

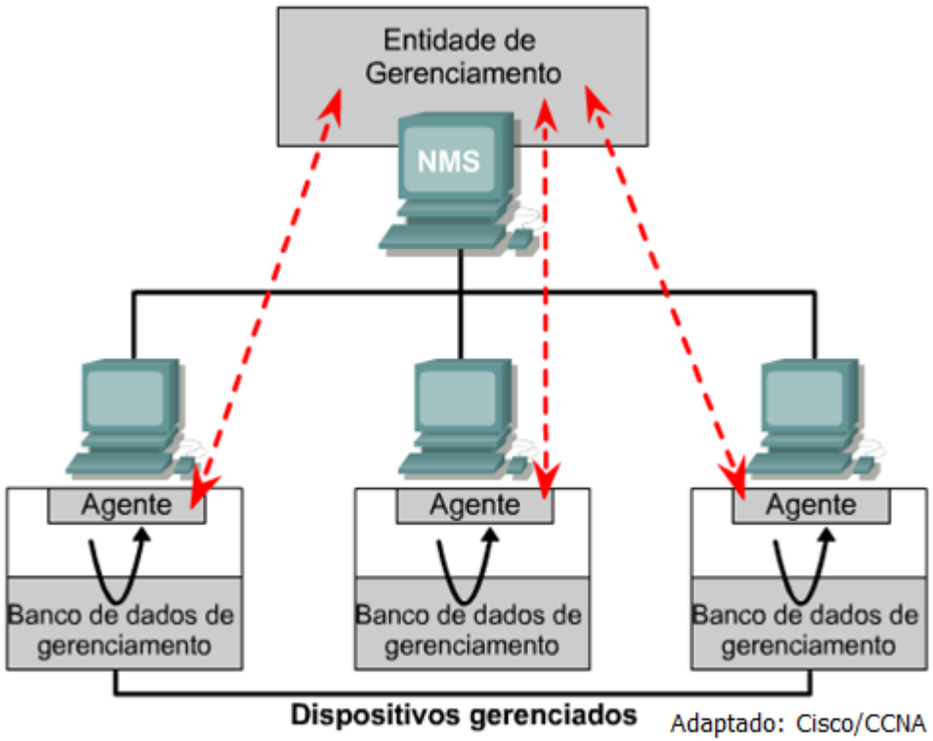
SSH (Secure Shell)

- ✓ Originalmente criado como um substituto do TELNET, podendo ser utilizado para diferentes finalidades - RFC 4251 (janeiro/2006).
- ✓ Constituído de três componentes:
  - SSH-TRANS: Permite criar um canal seguro sobre o TCP.
  - SSH-AUTH: permite a autenticação do cliente em relação ao servidor.
  - SSH-CONN: possibilita a criação de diferentes canais lógicos sobre o canal seguro já criado, permitindo a utilização de diferentes serviços, como acesso remoto, transferência de arquivos, etc.

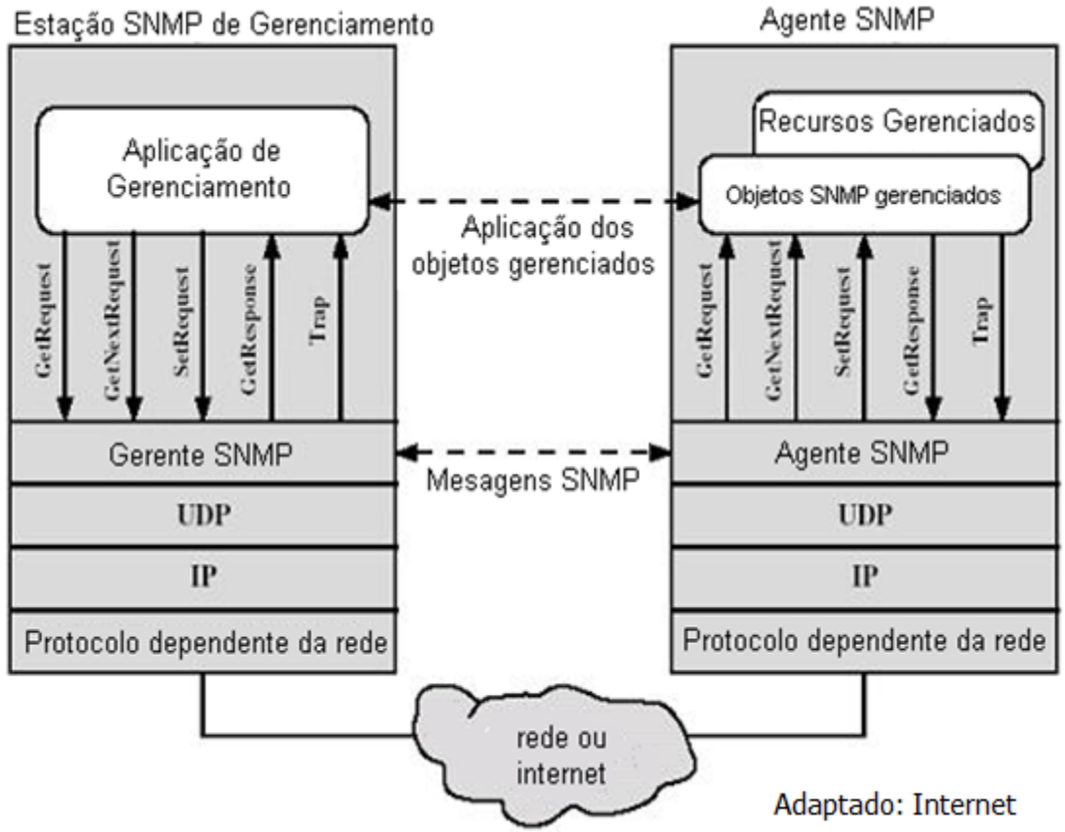


- Protocolo padrão para a troca de informações gerenciáveis entre dispositivos clientes e gerentes, em uma rede IP.
  - RFC 1098 (abril/1989) e atualizações.
- A gerência SNMP consiste dos seguintes componentes básicos:
  - **Gerente** (NMS - Network Management System): executa aplicações que monitoram e controlam os dispositivos gerenciados.
  - **Dispositivos gerenciados**: elementos de rede que contêm um agente SNMP. Coletam e armazenam informações gerenciáveis em suas MIBs, disponibilizando-as para os gerentes, quando solicitados.
  - **Agentes SNMP**: módulos de software de gerenciamento que residem nos dispositivos gerenciados. Um agente SNMP tem conhecimento local das informações gerenciáveis e as converte para uma forma compatível com o SNMP.
  - **MIB** (Management Information Base): base de dados de informações gerenciáveis, mantida nos dispositivos gerenciados.

- Por padrão, usa as portas UDP 161 pelo agente e 162 pelo gerente.
  - O gerente pode enviar solicitações de qualquer porta disponível (porta origem) para a porta destino 161 no agente, que pode gerar traps em qualquer porta disponível (porta de origem), enviando para a porta destino 162 no gerente; mas isso pode ser modificado no sistema operacional em uso.
- Pode-se encontrar ainda as portas TCP 5161 e 5162 (SNMP sobre SSH).



Adaptado: Cisco/CCNA



Adaptado: Internet

SNMP Versão 1

- Gerência única (centralizada)
- Implementa apenas 5 funções:
  - Get-Request: requisição de valores da MIB
  - Get-Next-Request: leitura de valores em seqüência
  - Set-Request: alteração de valores da MIB
  - Get-Response: resposta aos 3 comandos anteriores
  - Trap: relata eventos significantes ao gerente

SNMP Versão 2

- Permite gerência descentralizada (mais que um gerente)
- Adiciona duas novas funções:
  - Get-Bulk-Request: acesso a grandes blocos de informação na MIB
  - Inform-Request: notificações entre gerentes

SNMP Versão 3

- Agrega funções de segurança ao SNMPv2, permitindo autenticação.
- Autoriza usuários para monitorar e ler informações sobre a rede.

Nota: na verdade, essas novas versões correspondem a atualizações no protocolo.

Atividade 04 – Aplicações II