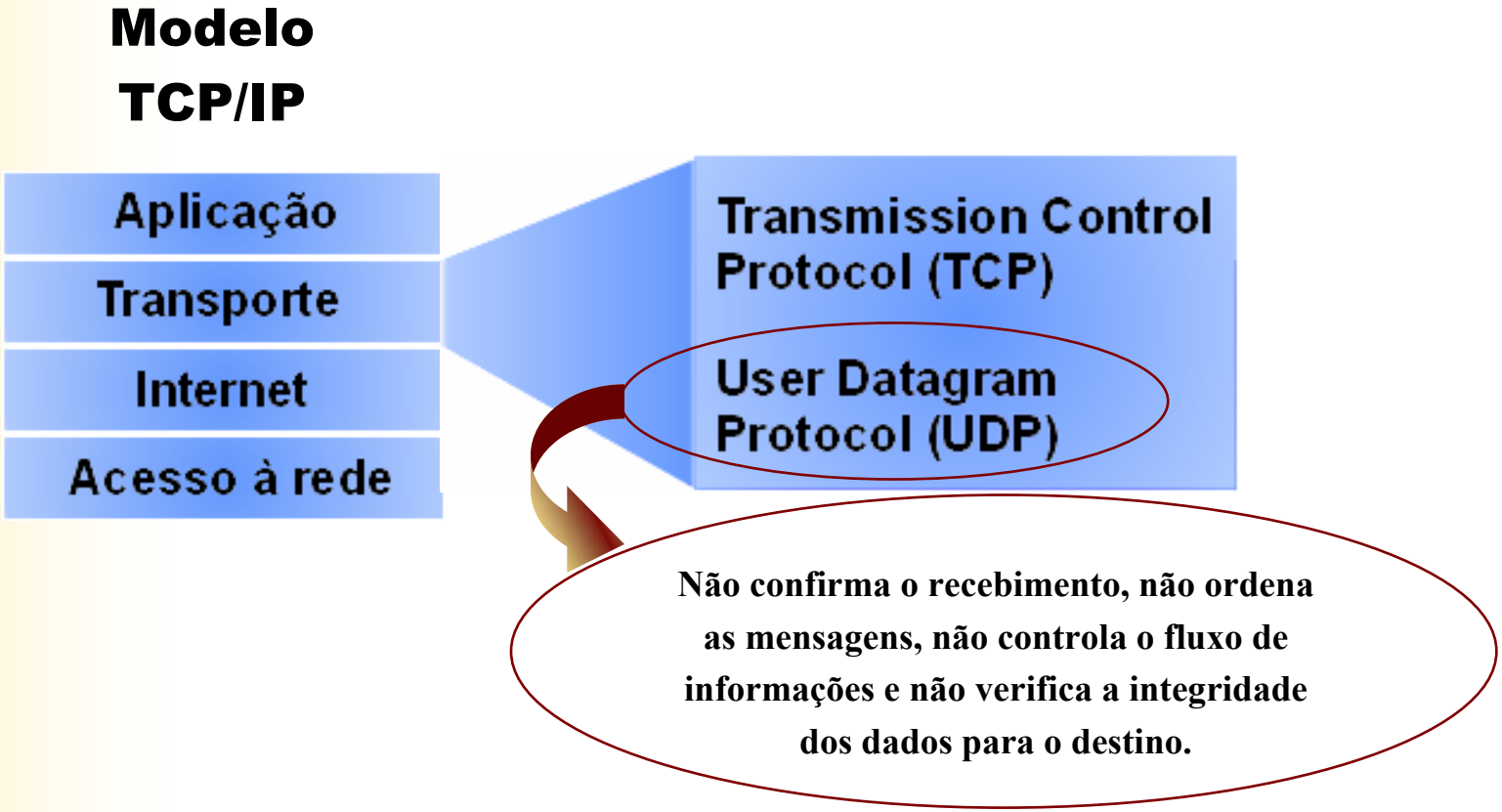
Tópicos da Apresentação:

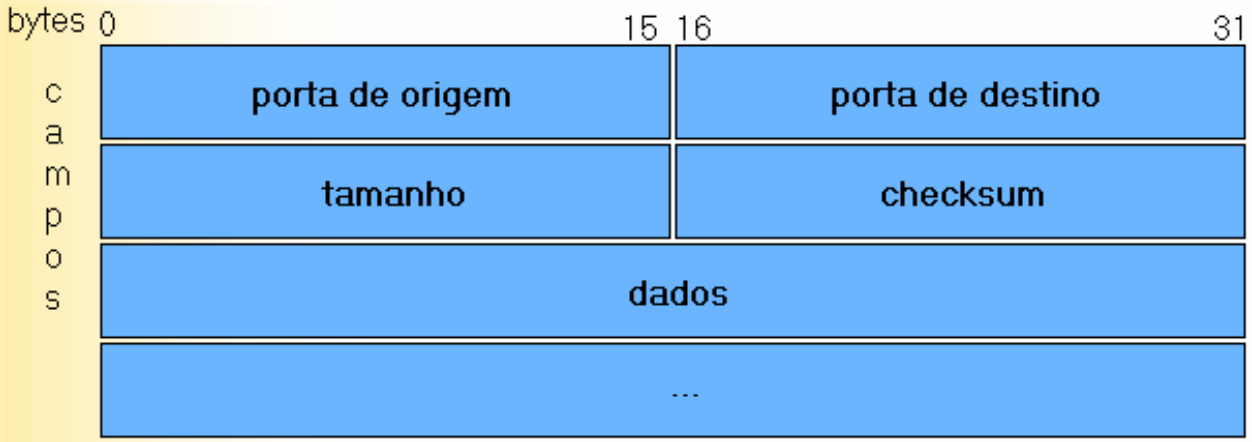
- Características Gerais do Protocolo UDP
  - Visão Geral da Camada de Transporte
  - Para que usamos o UDP se existe o TCP?
- Protocolos que Utilizam o UDP
- Vulnerabilidades do UDP
- Conclusões

Visão Geral da Camada de Transporte:

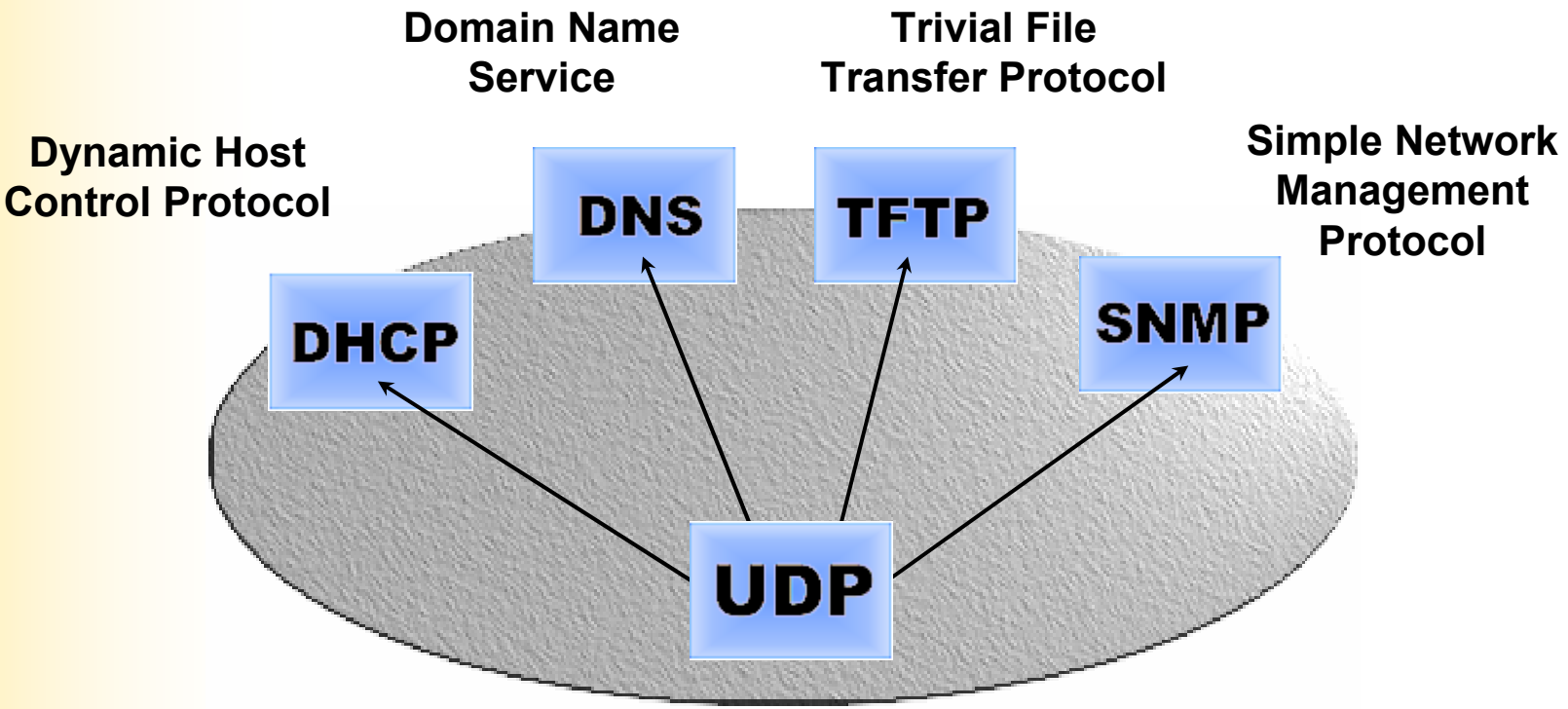


Para que usamos o UDP se existe o TCP?

Formato do Datagrama UDP:



Protocolos que usam UDP:



Vulnerabilidades do Protocolo UDP – parte 1/3

Alguns Tipos de Ataques:

"IP Spoofing" – falsificação de IP.

SYN Flood – o *hacker* pode lançar um processo que cause sobrecarga na máquina servidora.

Fraggle – causador de chuva de pacotes UDP para um lista de *broadcast.*

New Teardrop – diminui a parte de dados do UDP, falsificando-o, assim ele causa o travamento das máquinas.

Vulnerabilidades do Protocolo UDP – parte 2/3

Worm W32.SQLExp.

Alvos: Microsoft SQL Server 2000 e também o Microsoft Desktop Engine (MSDE) 2000.

Ação: O worm envia 376 bytes para a porta UDP, a porta de SQL Server Resolution Service.

Método: envia uma cópia de si mesmo para o SQL Server Resolution Service, o qual monitora a porta 1434 do UDP. Gera endereços IP aleatórios. Abre um soquete no computador infectado e tenta enviar uma cópia de si mesmo repetidamente à porta 1434 do UDP nos endereços IP que gerou, usando uma porta de fonte temporária.

Resultado: Como o worm não ataca os hosts seletivamente na sub-rede, o resultado é uma grande quantidade de trânsito.

Vulnerabilidades do Protocolo UDP – parte 3/3

Algumas Fragilidades:

NFS *(Network File System)* – Este protocolo utiliza o UDP para a solicitação da criação, remoção e escrita de arquivos.

RIP *(Routing Information Protocol)* – Os roteadores utilizam este protocolo para detectar o melhor caminho. O problema é que os pacotes RIP são pacotes UDP, enviados para a porta 513 e que não são checadas.

Referências

www.modulo.com - Módulo Security: *"Aspectos de Segurança no Protocolo IP"*

www.redbooks.ibm.com - RedBooks IBM: *"TCP/IP Tutorial and Technical Overview"*

CCNA – Cisco Certified Network Associate

www.symantec.com.br