



Fundamentos de Infraestrutura da Tecnologia da Informação



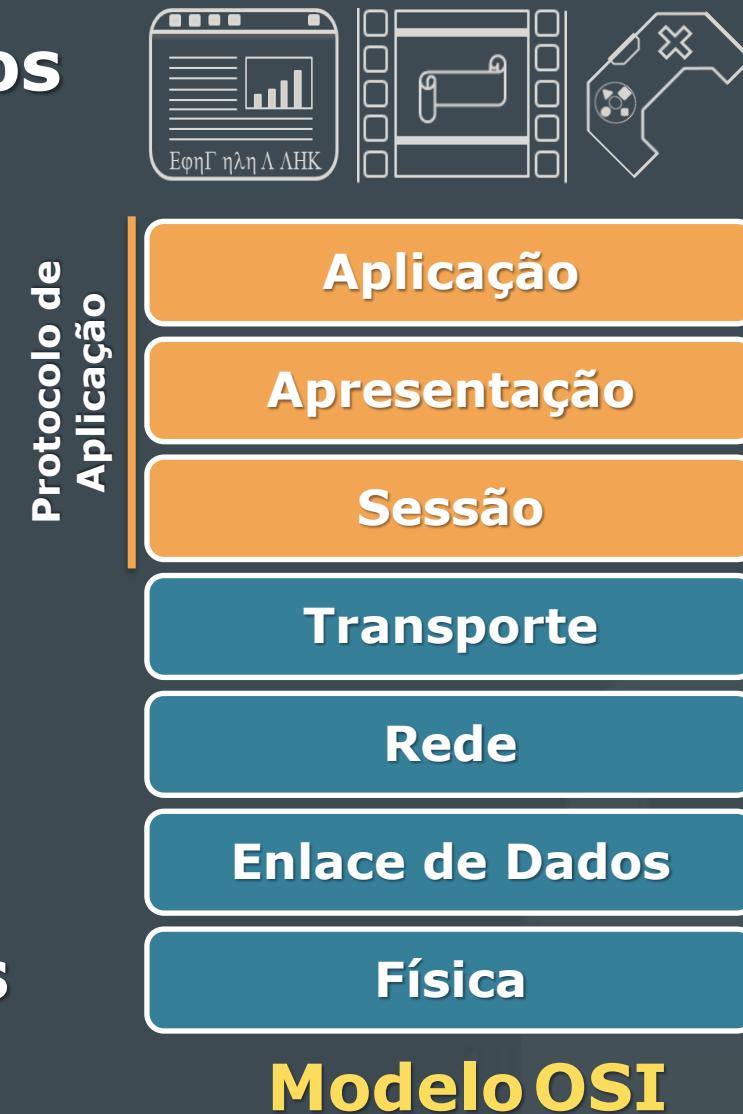
Conversa Inicial

Redes de computadores

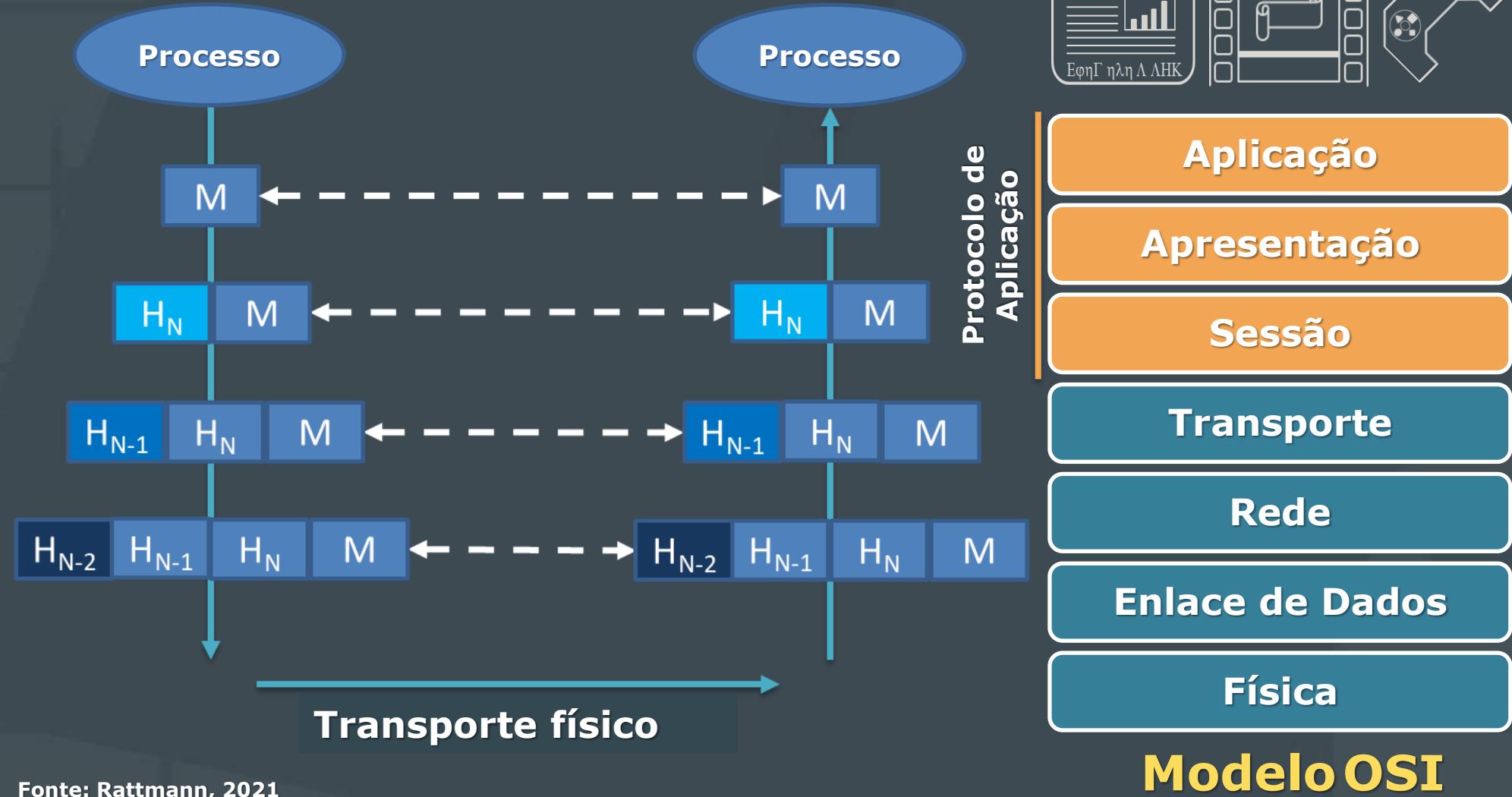
- Os protocolos de aplicação
- DNS, SMTP e TELNET
- MIB, SNMP e HTTP
- Roteamento e encaminhamento
- Firewall, IPS e VPN

Os protocolos de aplicação

- Na pilha TCP/IP, os protocolos de aplicação ocupam as três camadas mais altas do modelo OSI
- Executam as funções necessárias
 - Controle de sessão
 - Representação de dados
 - Criptografia
 - Interface com os processos de usuário



Fonte: Rattmann, 2021



Fonte: Rattmann, 2021

Fonte: Rattmann, 2021

Modelo OSI

Aplicações e protocolos

Aplicação	Protocolo da camada de aplicação	Protocolo de transporte subjacente
Correio eletrônico	SMTP	TCP
Acesso a terminal remoto	Telnet	TCP
Web	HTTP	TCP
Transferência de arquivo	FTP	TCP
Servidor de arquivo remoto	NFS	Tipicamente UDP
Recepção de multimídia	Tipicamente proprietário	UDP ou TCP
Telefonia por internet	Tipicamente proprietário	UDP ou TCP
Gerenciamento de rede	SNMP	Tipicamente UDP
Protocolo de roteamento	RIP	Tipicamente UDP
Tradução de nome	DNS	Tipicamente UDP

Fonte: Elaborado por Rattmann, 2021, com base em Kurose, 2013 (Pearson)

DNS, SMTP e TELNET

Serviço DNS

- Necessário para gerenciar uma grande quantidade de endereços eletrônicos que são criados diariamente e muito frequentemente alterados
 - Nome versus endereço
 - Controle distribuído e hierárquico

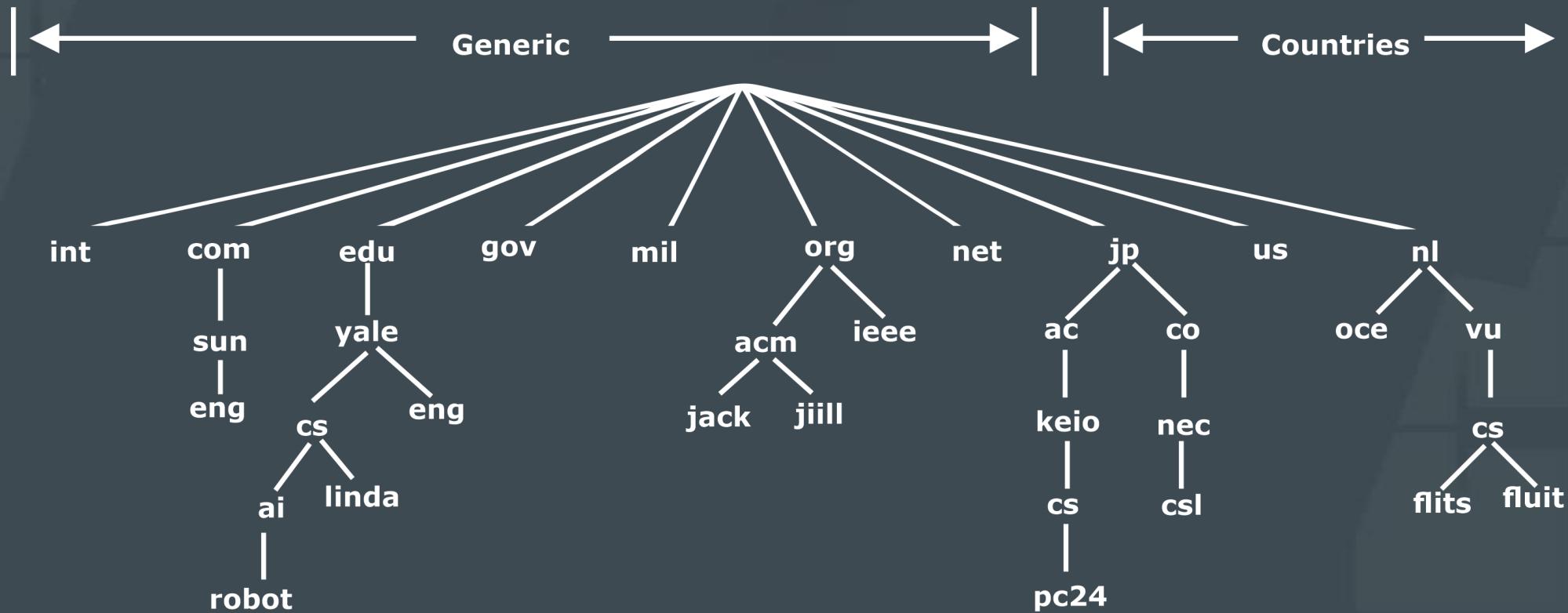
www.local.com > IP?



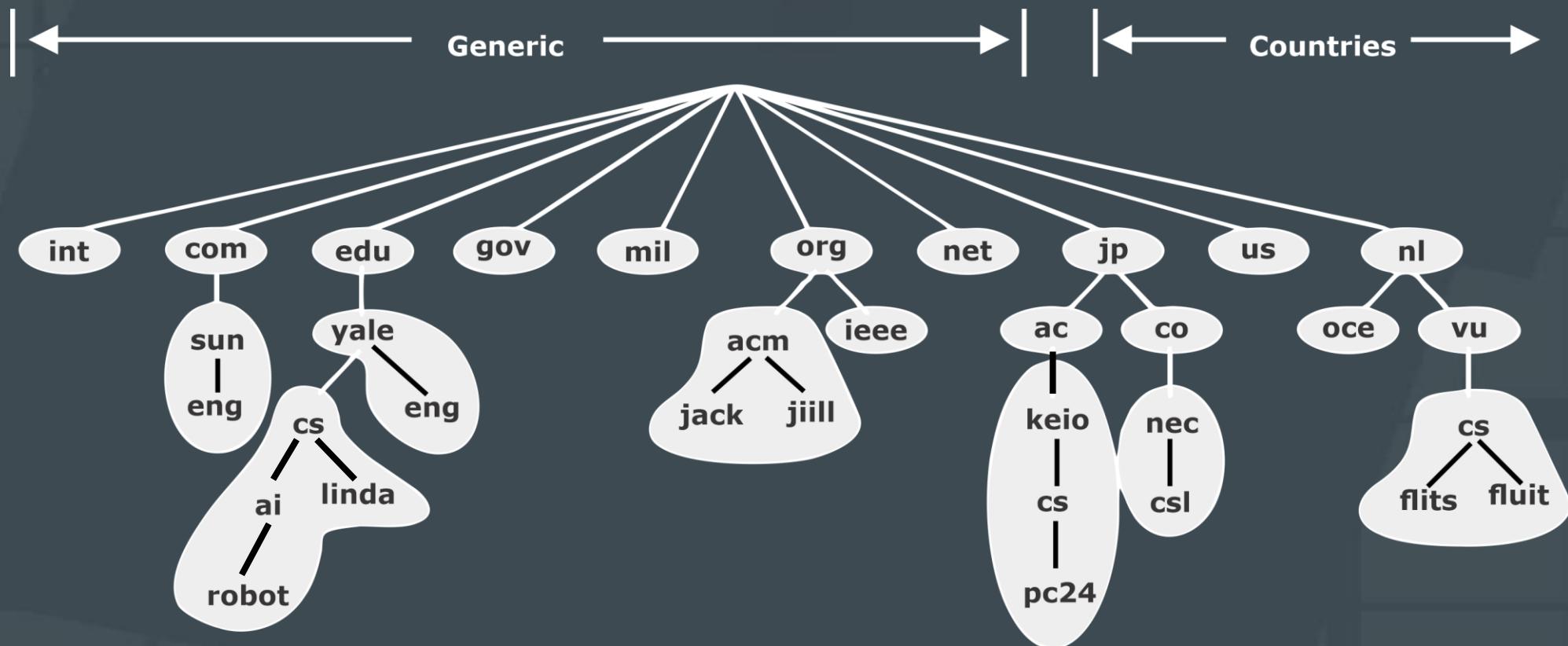
Fonte: Rattmann, 2021

- Encontra o endereço IP do URL
 - ✓ **URL (*Uniform Resource Locator*)**
- Organizado por estrutura em árvore
- Separado por zonas
- Busca recursiva ou alternativa

Parte do espaço de nome de internet



Zonas não sobrepostas de resolução da internet



Consulta no DNS

- Formato do registro de recurso armazenado no banco de dados distribuído do sistema DNS
- Domain_name Time_to_live Class Type Value

Tipo	Significado	Valor
SOA	Início de autoridade	Parâmetros para esta zona
A	Endereço IP de um host	Inteiro 32 bits
MX	Troca de mensagens de correio	Prioridade, domínio disponível a aceitar correio eletrônico
NS	Servidor de nomes	Nome de um servidor para este domínio
CNAME	Nome canônico	Nome de domínio
PTR	Ponteiro	Nome alternativo de um endereço IP
HINFO	Descrição de Host	CPU e SO em ASCII
TXT	Texto	Texto ASCII não interpretado
Classe	Significado	Valor
IN	Internet	Informações relacionadas à Internet

Requisição DNS



Requisição

Source fe80::e1c5:d74c:676:9ab9	Destination fe80::c23d:d9ff:fea4:20c0	Protocol DNS	Length 89	Info Standard query 0x47cf A IN c.msn.com
------------------------------------	--	-----------------	--------------	--

Resposta

Source fe80::c23d:d9ff:fea4:20c0	Destination fe80::e1c5:d74c:676:9ab9	Protocol DNS	Length 153	Info Standard query response 0x47cf A c.msn.com CNAME c-msn-com-nsatc.trafficmanager.net A 20.36.253.92
-------------------------------------	---	-----------------	---------------	--

Protocolo DNS

Requisição DNS – ETH/IPv6/UDP/DNS

0000	c0 3d d9 a4 20 c0 98 83 89 8d 60 0b 86 dd 60 08	Ethernet
0010	d7 e6 00 23 11 40 fe 80 00 00 00 00 00 00 e1 c5	
0020	d7 4c 06 76 9a b9 fe 80 00 00 00 00 00 00 c2 3d	IPv6
0030	d9 ff fe a4 20 c0 e4 be 00 35 00 23 d1 ee 47 cf	
0040	01 00 00 01 00 00 00 00 00 00 01 63 03 6d 73 6e	Identification Query
0050	>03 63 6f 6d 00 00 01 00 00 01	Standard query Type (A) Class (IN)

Ethernet
IPv6
UDP
DNS

Fonte:
Rattmann, 2021

1º Octeto	2º Octeto	3º Octeto	4º Octeto
Identificação		Flags	
Número de Perguntas		Número de RRs de resposta	
Números de RRS autoritativos		Número de RRs adicionais	
Perguntas (número variável de perguntas)			
Respostas (número variável de respostas)			
Autoridade (número variável de registros de recursos)			
Informações adicionais (número variável de registros de recursos)			

- 12 octetos
- Nome, tipo de campo para consulta
 - RRs de resposta à consulta
 - Registros para servidores com autoridade
 - Informação adicional “útil” que pode ser usada

Fonte: Elaborado por Rattmann, 2021, com base em Kurose, 2013 (Pearson)

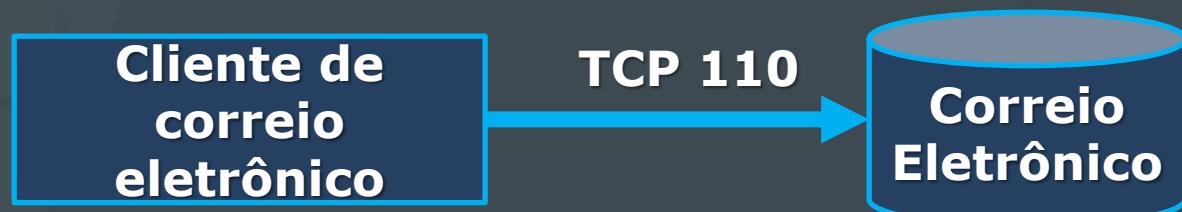
SMTP

- *Simple Mail Transfer Protocol*
- TCP 25
- Protocolo simples em modo texto
- HELO, MAIL, RCPT, DATA, QUIT



C: HELO abcd.com	S: 220 xyz.com SMTP service ready
C: MAIL FROM: <elinor@abcd.com>	S: 250 xyz.com says hello to abcd.com
C: RCPT TO: carolyn@xyz.com	S: 250 sender ok
C: DATA	S: 250 recipient ok
C: < *** Todo conteúdo do email *** >	S: 354 Send Mail; end with "." on a line itself
C: .	S: 250 message accepted
C: QUIT	S: 221 xyz.com closing connection

SMTP/POP3



- Máquinas sempre ativas
- Mensagens grandes > 64 kB
- Ajustes de Timeout
- Lista de distribuição cruzada entre servidores
- Clientes Internet via ISP

- ISP (caixa postal)
- POP3
 - RFC 1939
 - TCP 110
 - Sequência
 - ✓ Autorização
 - ✓ Transações
 - ✓ Atualização

SMTP/POP3/IMAP

- **POP3**

- **Baixa as mensagens do servidor**
- **Mantém mensagens em vários clientes**

■ IMAP

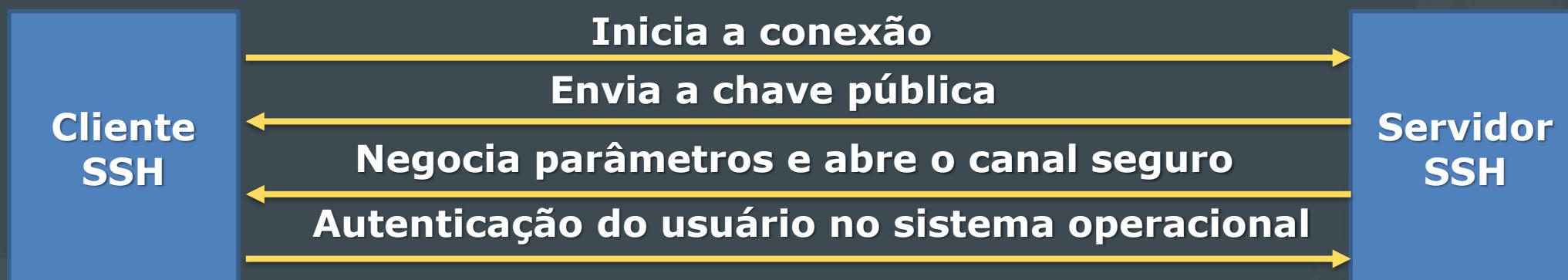
- Manipula mensagens no servidor
- RFC 2060
- TCP/143
- Filtros e regras para correspondências
- Filtros por atributos
- Download de mensagens parciais

TELNET/SSH

■ TELNET

- Permite o acesso remoto, modo terminal
- Comunicação bidirecional, em modo texto
- RFC 854
- TCP 23
- Envio caractere a caractere, ecoado pelo servidor
- Texto enviado sem criptografia

- **SSH (*Secure Shell*)**
- Utiliza criptografia na comunicação
- RFC 4251/4252/4253
- TCP 22
- Putty, WinSCP, OpenSSH



Fonte: Elaborado por Rattmann, 2021, com base em SSH.com, 2021

MIB, SNMP e HTTP

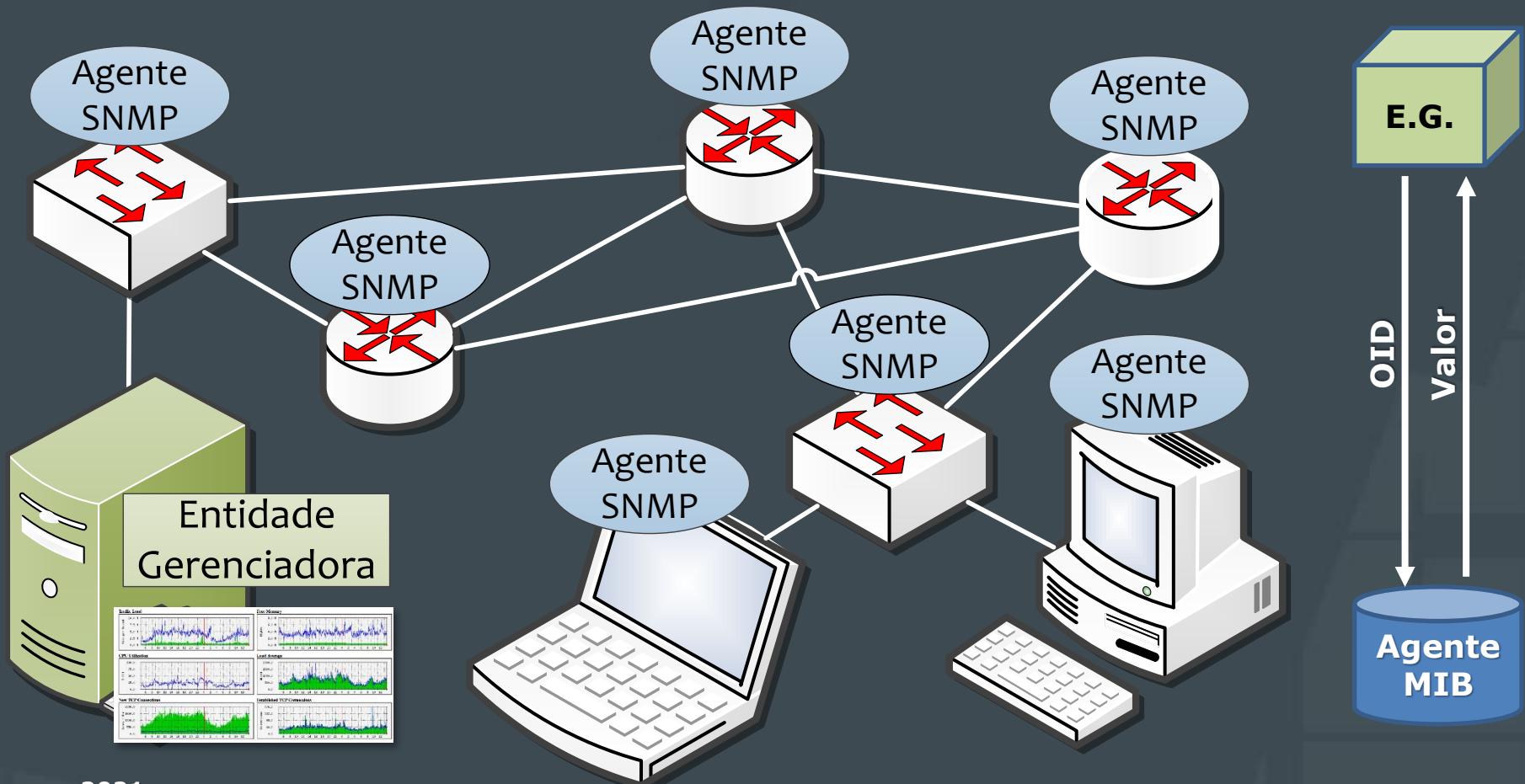
SNMP/MIB

- Banco de Dados de Objetos
 - OID: Object ID
- Leitura/escrita em variáveis
 - GetRequest/SetRequest
- Envio de eventos (Trap)
- Segurança
 - Comunidades de acesso
 - Usuário/senha SNMP V.3
- NMS (*Network Management System*)



profit_image/adobe stock

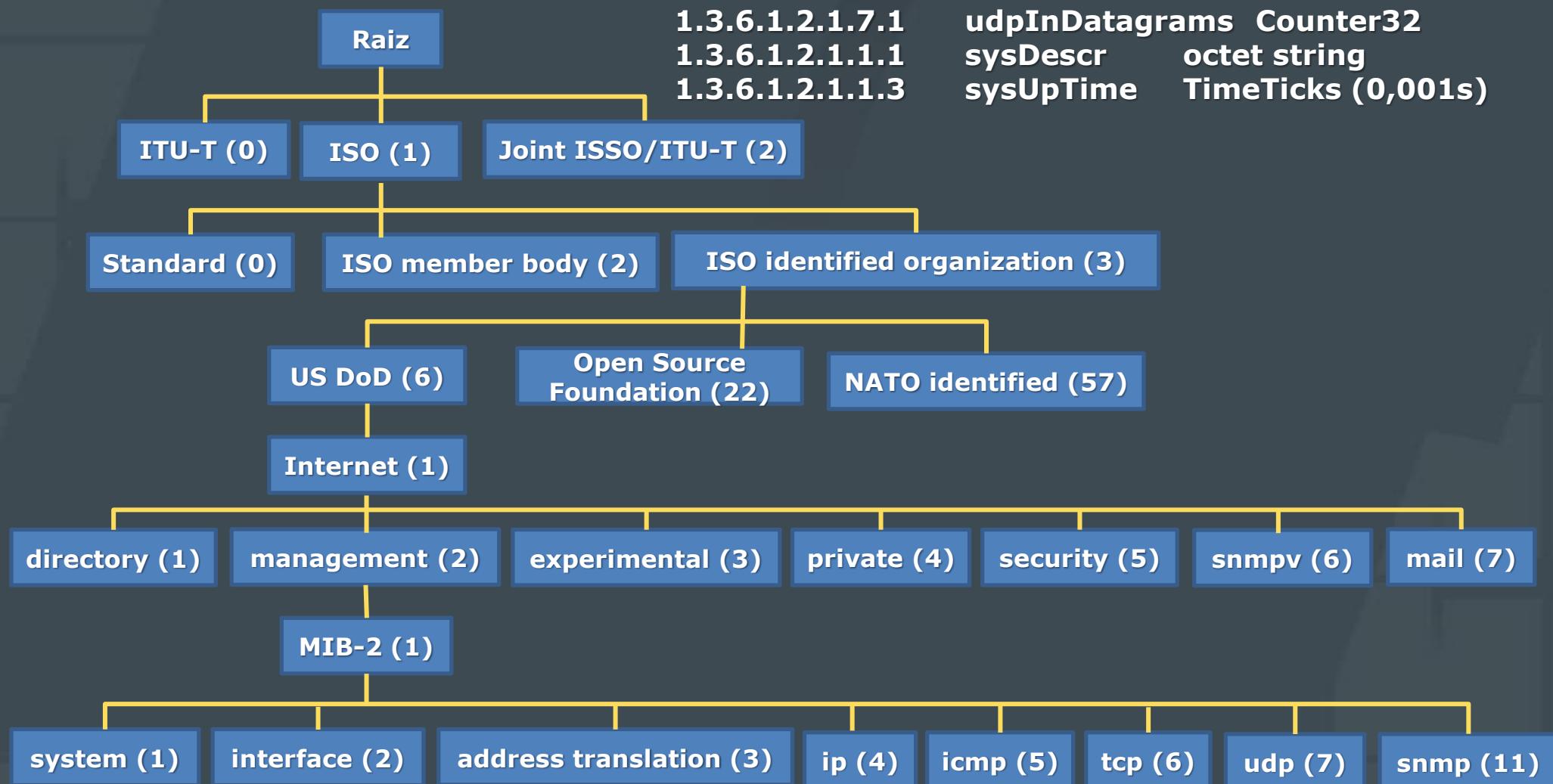
Arquitetura de gerenciamento SNMP



Fonte: Rattmann, 2021

MIB/OID

- Objetos organizadas em árvore
 - CPU
 - ✓ Ocupação
 - Memória
 - ✓ Utilização
 - Interface
 - ✓ Erros
 - ✓ Tráfego



Fonte: Rattmann, 2021

GET SNMP

Ethernet	IPv4
UDP	SNMP

0000	50	57	9c	a0	c3	9d	98	83	89	8d	60	0b	08	00	45	00
0010	00	49	f0	b7	00	00	80	11	aa	3d	c0	a8	0f	37	c0	a8
0020	0f	27	c5	6f	00	a1	00	35	0c	2d	30	2b	02	01	00	04
0030	05	65	70	73	6f	6e	a1	1f	02	01	02	02	01	00	02	01
0040	00	30	14	30	12	06	0e	2b	06	01	04	01	89	60	01	02
0050	02	01	01	01	02	05	00									

1.3.

PW.....`...E.
.I.....=....7..
.'.o...5.-0+....
.epson.....
.0.0...+....`...
.....

Cabeçalho comum SNMP			Cabeçalho GET/SET			Variáveis pra GET/SET				
versão	comunidade	Tipo PDU (0-3)	ID de requisição	Estado de erro (0-5)	Índice de erro	nome	valor	nome	valor	...

Source: 192.168.15.55

Destination: 192.168.15.39

Protocol: SNMP

Length: 87

Info: get-next-request 1.3.6.1.4.1.1248.1.2.2.1.1.1.2

Integer: 0x02; Octet String: 0x04; Null: 0x05; Object ID: 0x06;
Sequence: 0x30; GetRequest: 0xA0; SetRequest: 0xA3;

ASN.1/BER – (TLV)

Tipo	Tamanho	Dados
Integer: 0x02	0x01	0x00

Abstract Syntax Notation One
Basic Encoding Rules
Tag-Length-Value

Centro de gerenciamento de rede

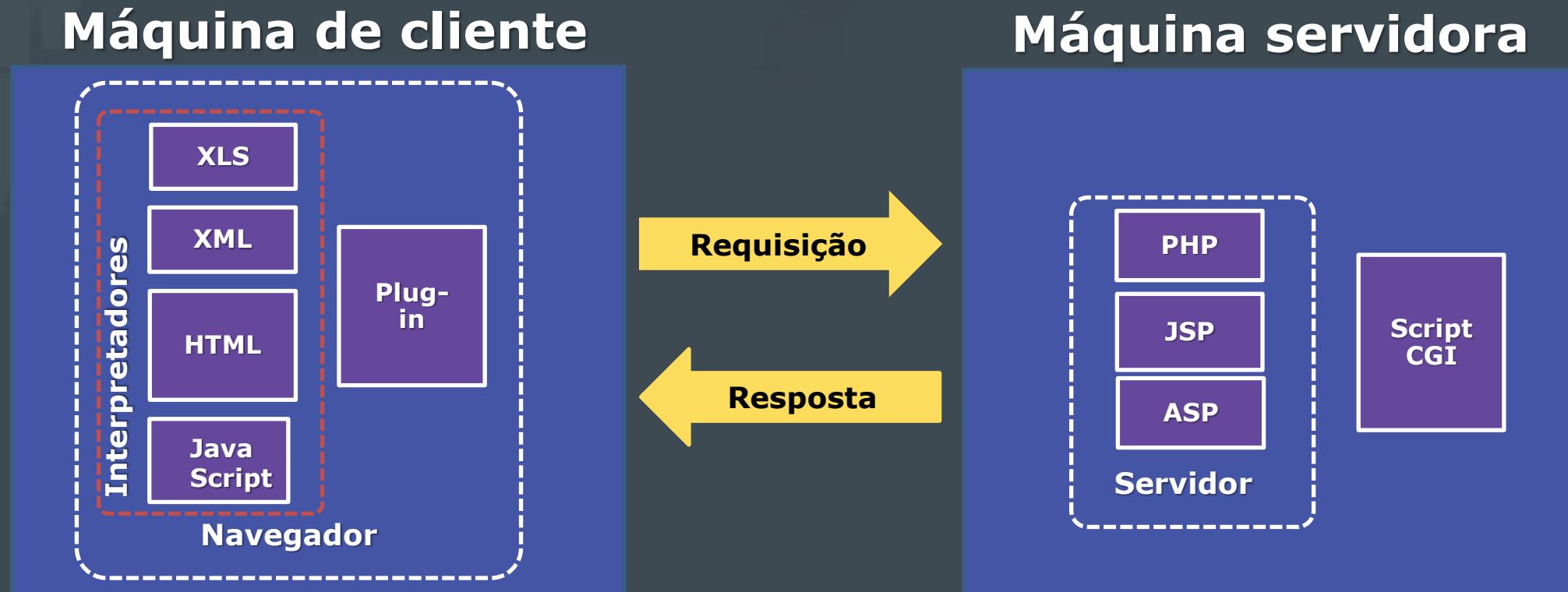


tonsnoei / adobe stock

HTTP (*HyperText Transfer Protocol*)

- **Hipertexto**
 - Arquivo texto no formato HTML
 - Objetos referenciados via URL
- **Sistema Cliente-Servidor**
 - Interação por mensagens HTTP
- **RFC 1945; RFC 2616**
 - Formato das mensagens
 - Requisição/resposta

Formas de exibir conteúdo



Fonte: Elaborado por Rattmann, 2021, com base em Tanenbaum, 2003

HTTP 1.1

- RFC 2616
- TCP Porta 80

Método	Descrição
GET	Solicita a leitura de uma página Web
HEAD	Solicita a leitura de um cabeçalho de página Web
PUT	Solicita o armazenamento de uma página Web
POST	Acrescenta a um recurso (por exemplo, uma página Web)
DELETE	Remove a página Web
TRACE	Ecoa a solicitação recebida
CONNECT	Reservado para uso futuro
OPTIONS	Consulta certas opções

Código	Significado
1xx	Informação
2xx	Sucesso
3xx	Redirecionamento
4xx	Erro do cliente
5xx	Erro de servidor

Exemplos:

100: O servidor concorda em atender

200: Requisição bem-sucedida

204: Sem conteúdo

301: A página foi movida

403: Página proibida

503: Tente mais tarde

Requisição HTTP

0000	ac 16 2d 2f 23 5d 98 83 89 8d 60 0b 08 00 45 00	...-/#]....`....E.
0010	00 71 f7 fd 40 00 80 06 62 39 c0 a8 0f 37 c0 a8	.q..@...b9...7..
0020	0f c8 fc 89 1f 90 c3 f0 13 0e 56 c9 c8 0b 50 18V...P.
0030	43 62 bb e9 00 00 47 45 54 20 2f 44 65 76 4d 67	Cb....GET /DevMg
0040	6d 74 2f 50 72 6f 64 75 63 74 53 74 61 74 75 73	mt/ProductStatus
0050	44 79 6e 2e 78 6d 6c 20 48 54 54 50 2f 31 2e 31	Dyn.xml HTTP/1.1
0060	0d 0a 48 4f 53 54 3a 20 31 39 32 2e 31 36 38 2e	.HOST: 192.168.
0070	31 35 2e 32 30 30 3a 38 30 38 30 0d 0a 0d 0a	15.200:8080....

**GET /DevMgmt/ProductStatusDyn.xml HTTP/1.1
HOST: 192.168.15.200:8080**

Ethernet

IPv4

TCP

HTTP

Resposta HTTP

0000	98	83	89	8d	60	0b	ac	16	2d	2f	23	5d	08	00	45	00
0010	01	60	01	3a	00	00	40	06	d8	0e	c0	a8	0f	c8	c0	a8
0020	0f	37	1f	90	ef	ae	d7	34	52	3d	22	2a	81	ac	50	18
0030	20	75	40	20	00	00	48	54	54	50	2f	31	2e	31	20	32
0040	30	30	20	4f	4b	0d	0a	53	65	72	76	65	72	3a	20	48
0050	50	20	48	54	54	50	20	53	65	72	76	65	72	3b	20	48
0060	50	20	44	65	73	6b	6a	65	74	20	34	36	32	30	20	73
0070	65	72	69	65	73	20	2d	20	43	5a	32	38	34	41	3b	20
0080	53	65	72	69	61	6c	20	4e	75	6d	62	65	72	3a	20	43
0090	4e	39	34	37	31	35	32	37	56	30	36	54	4e	3b	20	43

....`....-/#]..E.
.~.:..@.....
.7.....4R="*..P.
u@ ..HTTP/1.1 2
00 OK..Server: H
P HTTP Server; H
P Deskjet 4620 s
eries - CZ284A;
Serial Number: C
N9471527V06TN; C

...

HTTP/1.1 200 OK

Server: HP HTTP Server; HP Deskjet 4620 series - CZ284A;
Serial Number: CN9471527V06TN; Cesar_wl_ia_pp_usr_hf Built:Thu Apr 14, 2016
12:28:23PM {CAP1FN1616AR, ASIC id 0x00340100}

Content-Type: text/xml

Transfer-Encoding: chunked

Cache-Control: must-revalidate, max-age=0

Pragma: no-cache

...

Ethernet

IPv4

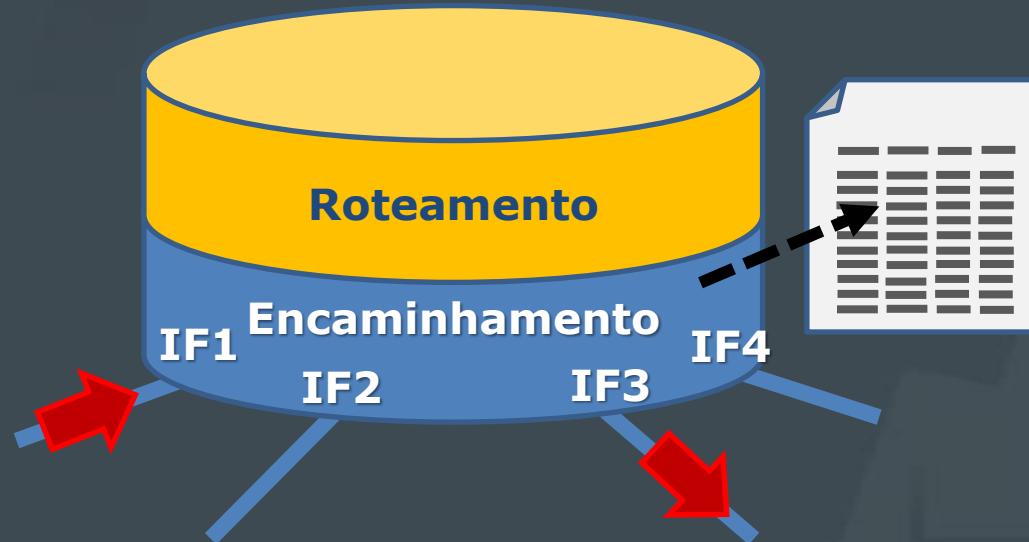
TCP

HTTP

Roteamento e encaminhamento

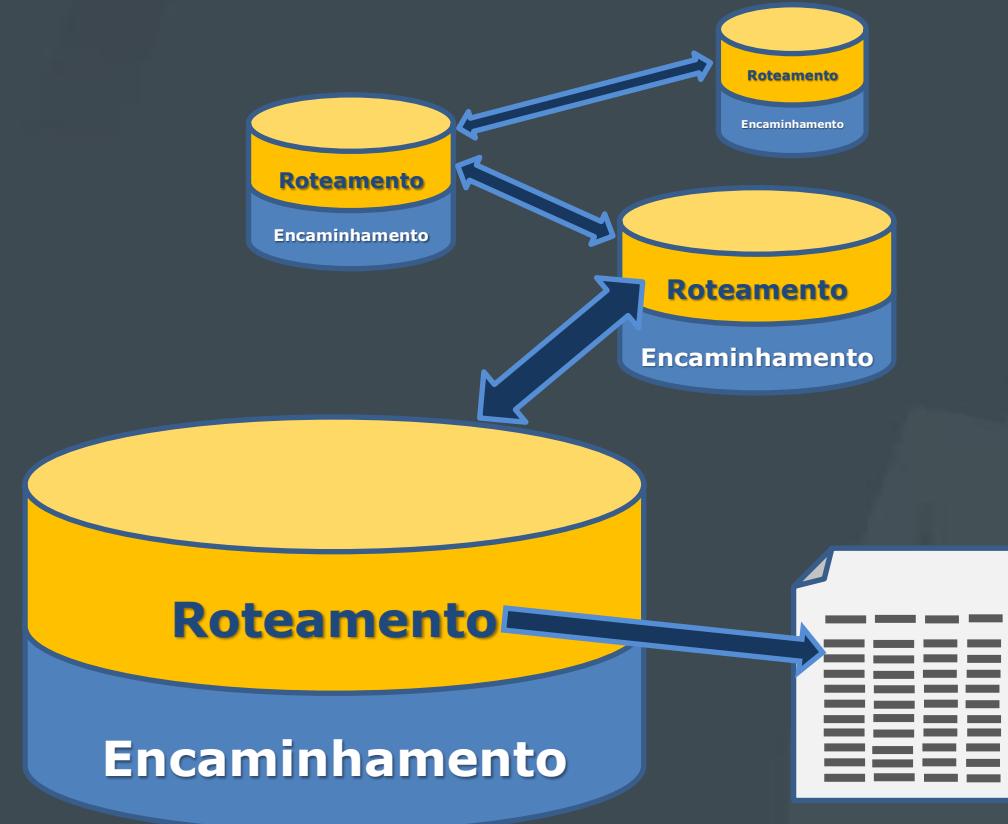
Encaminhamento

- Analisa o pacote que chega
- Utiliza a Tabela de Rotas
- Encontra a rota e identifica a interface
- Encaminha o pacote pela interface associada



Roteamento

- Mantém a Tabela de Rotas
- Mantém o registro da topologia da rede
- Ativa a melhor rota



- Utiliza dois métodos
 - Manual
 - Automático
 - ✓ Protocolos de roteamento
 - ✓ Processo comum
 - ✓ Troca de informações entre dispositivos

Melhor rota

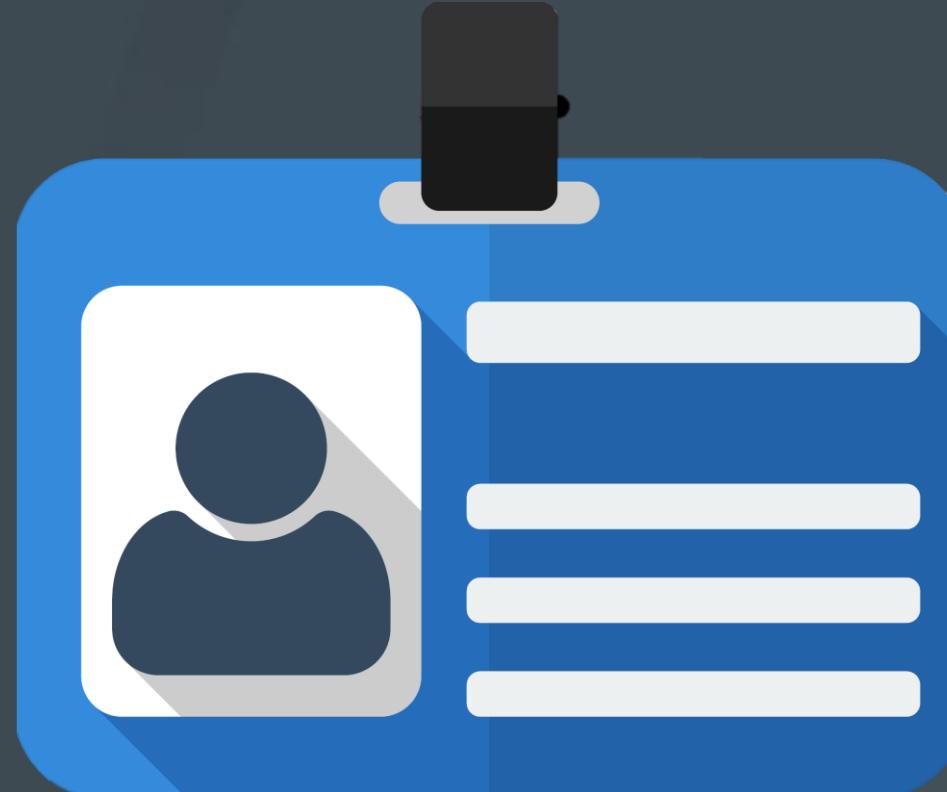
- **Protocolos de Roteamento**
 - **RIPv2 (*distance vector*)**
 - **OSPF (*link state*)**
 - **BGP (*internet*)**
- **Várias rotas para o mesmo destino**
 - **Ativação da melhor rota**
 - **As demais rotas ficam inativas**



Firewall, IDS, IPS e VPN

Segurança

- **Equipamentos**
 - Atualizados
 - Eficazes



RealVector/adobe stock

- **Atitudes**
 - **Políticas de segurança**
 - ✓ **Classificação**
 - ✓ **Procedimentos**
 - ✓ **Responsabilidade**
 - **Não compartilhamento de informação**
 - **Descarte de documentos**

Firewall

- **Rede (L4)**
 - **Regras**
 - **Nova Geração (L7)**
 - **Firewall**



Rafal Olechowski/adobe stock

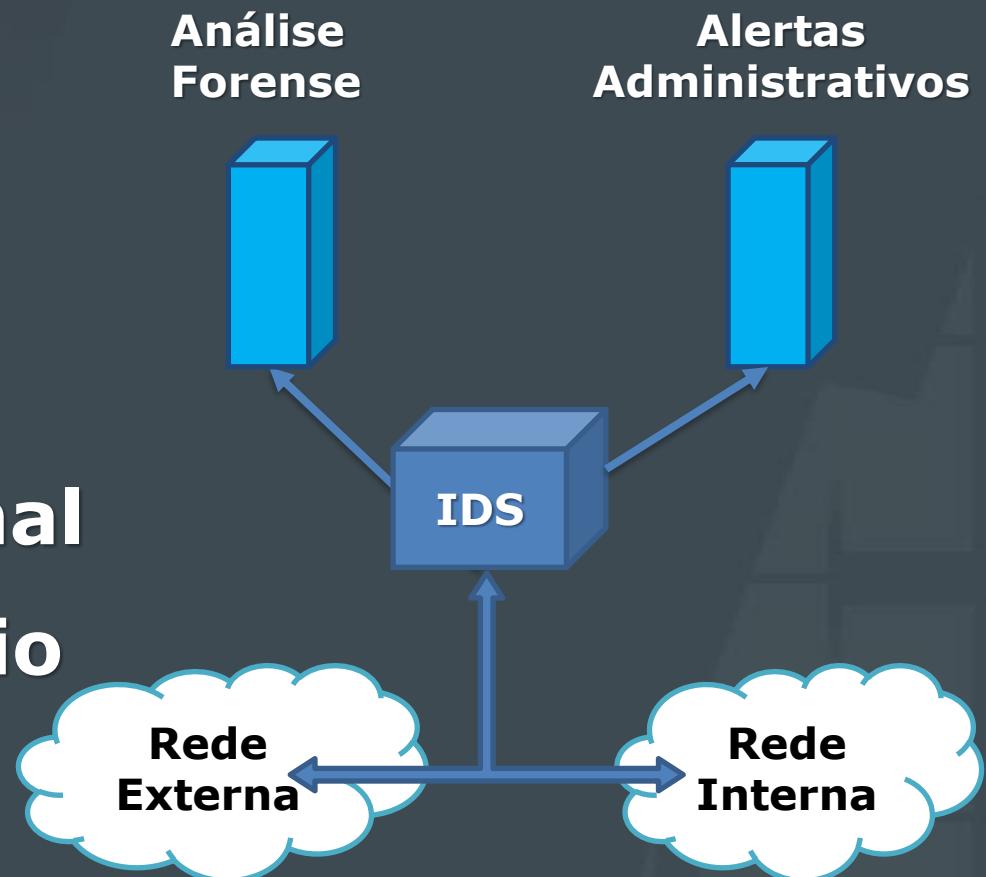
- **Filtro URL**
 - ✓ **Categorias/reputação**
- **Usuários/políticas**
 - ✓ **Grupos**
- **Controle de aplicações**
- **IPS**

- **Rede mais externa → rede mais interna**
 - Nega tudo
 - Exceções por regra
- **Rede mais interna → rede mais externa**
 - Permite tudo
 - Exceções por regra



IDS

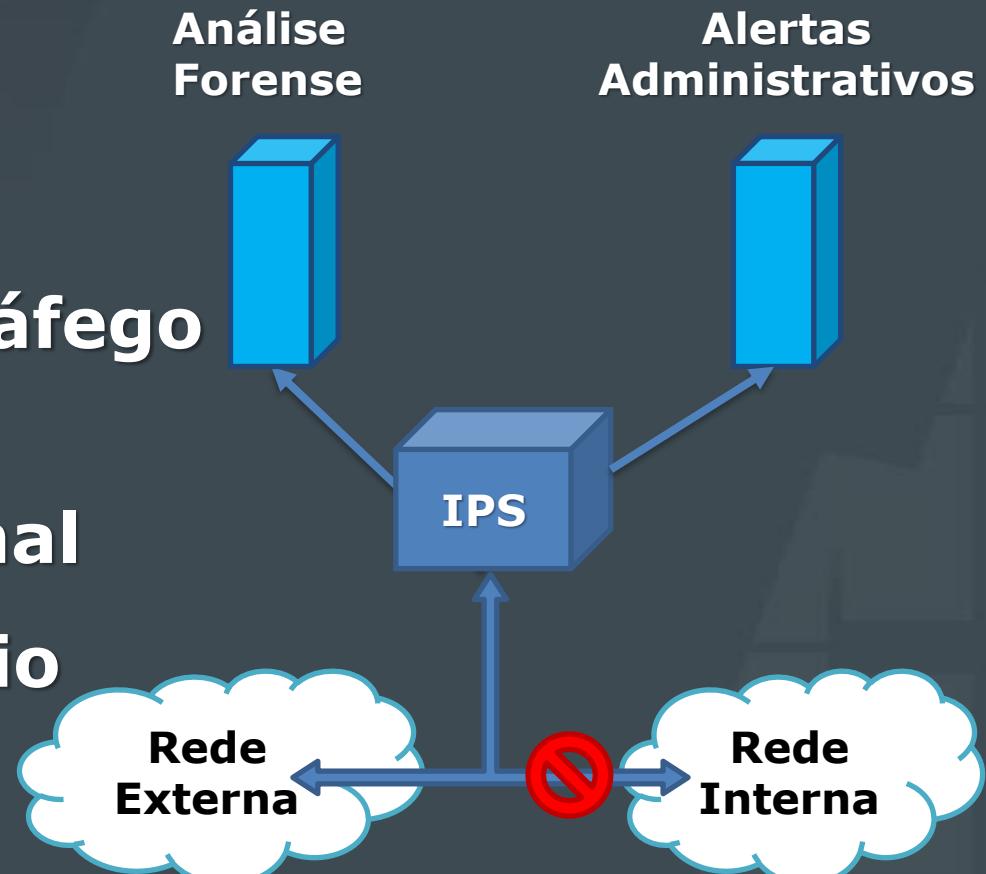
- ***Intrusion Detection System***
- Análise profunda de tráfego
- Avaliação de comportamento anormal
- Comparação por horário
- Alertas



IPS

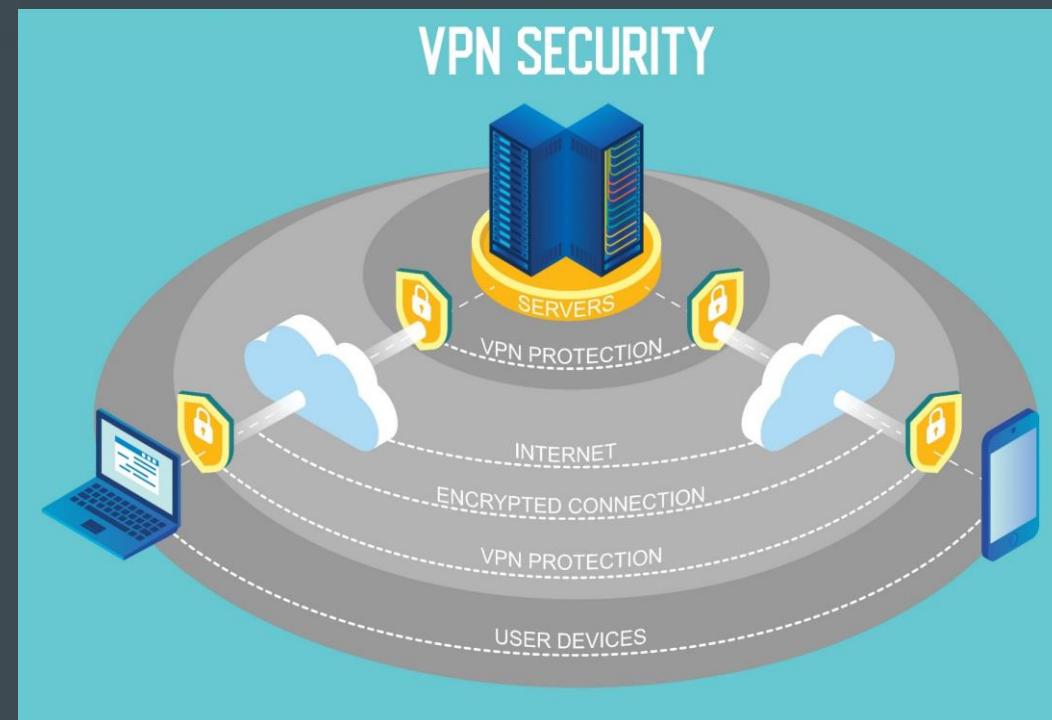
- **IPS (*Intrusion Prevent System*)**

- Análise profunda de tráfego
- Avaliação de comportamento anormal
- Comparação por horário
- Alertas
- Bloqueios



■ **VPN (*Virtual Private Network*)**

- **Conexão privada sobre rede pública**
- **Criptografia**
- **Cliente/servidor**
- **Equipamento/equipamento**



Siberian Art/adobe stock

X

Fechar