

Aulão de Exercícios 2011

Redes de Computadores

TCP/IP

Prof. Fred Sauer, D.Sc.

3ª QUESTÃO (10 pontos)

Corpo de Engenheiros Marinha 2011

Explique as diferenças entre o protocolo UDP e TCP.

19) A partir das práticas de gerenciamento de redes baseadas no modelo de referência OSI, são problemas relacionados à camada de rede, EXCETO:

- A) Endereço IP de hospedeiro incorreto.
- B) Servidor DHCP mal configurado.
- C) Rotas estáticas mal configuradas.
- D) Saturação de recursos devido excesso de quadros de difusão.
- E) Hospedeiro com máscara de rede incorreta.

COFEN 2011

21) Na implementação de serviços em redes TCP/IP (configuração padrão), o número de porta do serviço de SMTP (Simple Mail Transfer Protocol), é:

- A) Porta 21
- B) Porta 23
- C) Porta 25
- D) Porta 27
- E) Porta 80

26) A camada de aplicação do modelo de referência OSI é a parte da arquitetura que oferece serviços de rede aos usuários finais. Das principais aplicações, temos os seguintes protocolos: SMTP, FTP, DNS, DHCP e ARP. Qual das opções a seguir descreve de forma INCORRETA a função de um dos serviços dos protocolos?

- A) SMTP – Simple Mail Transfer Protocol: fornecer o serviço de correio eletrônico.
- B) FTP – File Transfer Protocol: fornecer o serviço de transferência de arquivos.
- C) DNS – Domain Name Service: fornecer o serviço de mapeamento de nomes em números IP (e vice-versa).
- D) DHCP – Dynamic Host Configuration Protocol: oferecer configuração dinâmica de terminais, com concessão de endereços IP para hosts da rede.
- E) ARP – Address Resolution Protocol: é um protocolo para atualizar e pesquisar diretórios rodando sobre TCP/IP. Cada diretório consistindo de um conjunto de atributos com seus respectivos valores.

Respostas

- Diferenças fundamentais:
 - TCP – orientado a conexão; UDP – não orientado
 - TCP suporta:
 - Segmentação e Remontagem;
 - Multiplexação e Splitting
 - Retransmissão e ordenamento de segmentos
 - UDP suporta apenas Multiplexação e Splitting
- Questão 19 – Letra B – DHCP é Aplicação
- Questão 21 – Letra C
- Questão 26 – Letra E – ARP resolve endereços IP em MAC. A descrição é do LDAP

TRT 2011

35. Tem como principal tarefa a transformação de um canal de transmissão bruto em uma linha que pareça livre de erros não detectados. Para executar tal tarefa, faz com que o transmissor divida os dados de entrada em quadros de dados e os transmita sequencialmente, aguardando um quadro de confirmação do receptor. Um de seus protocolos é o PPP.

No modelo OSI, a descrição acima trata-se de tarefa da camada

- (A) de transporte.
- (B) física.
- (C) de rede.
- (D) de enlace.
- (E) de sessão.

37. Considere:

- I. Oferece às camadas superiores independência das tecnologias de transmissão e comutação de dados, usadas para conectar os sistemas; responsável por estabelecer, manter e terminar as conexões.
- II. Possibilita a transferência de dados confiável e transparente entre as extremidades; oferece recuperação de erro e controle de fluxo ponta a ponta.

No modelo OSI, essas funções são exercidas, respectivamente, pelas camadas:

- (A) rede e transporte.
- (B) transporte e sessão.
- (C) sessão e apresentação.
- (D) apresentação e aplicação.
- (E) transporte e enlace.

36. São protocolos da camada 3 (rede, inter-redes ou internet) do modelo TCP/IP de cinco camadas.

- (A) IPsec e DNS.
- (B) SMTP e TCP.
- (C) 802.11 Wi-Fi e SMTP.
- (D) SNMP e TCP.
- (E) IPsec e ICMP.

38. Parte do conjunto TCP/IP é um protocolo do nível de transporte que não garante entrega, nem preservação de sequência e nem proteção contra duplicação. Utilizado por algumas aplicações orientadas a transação, trata-se de

- (A) FTP.
- (B) DNS.
- (C) IP.
- (D) TCP.
- (E) UDP.

39. O protocolo usado para o gerenciamento das redes TCP/IP é o

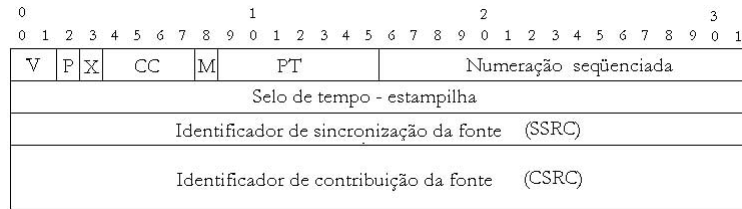
- (A) IMAP.
- (B) SNMP.
- (C) DHCP.
- (D) SMTP.
- (E) ICMP.

Respostas

- 35 – letra D – Correção de erros, “quadros” e ppp → camada de enlace
- 36 – letra E – Ainda tem o IGMP
- 37 – letra A – No IP não há conexões, mas no OSI a camada de rede tem esta função. A descrição do transporte está perfeita.
- 38 – letra E, sem comentários
- 39 – letra B
 - IMAP – Internet Message Access Protocol
 - SNMP – Simple Network Management Protocol
 - DHCP Dynamic Host Configuration Protocol
 - SMTP – Simple Mail Transfer Protocol
 - ICMP – Internet Control Message Protocol

62. A função básica do protocolo RTP (Real-time Transport Protocol) é:
- D**
- (A) fornecer informações para controle do fluxo de dados multimídia.
 - (B) padronizar a codificação de áudio e vídeo utilizando pacotes UDP.
 - (C) substituir o protocolo UDP para a transmissão de conteúdos de áudio e vídeo.
 - (D) multiplexar diversos fluxos de dados de tempo real sobre um único fluxo de pacotes UDP.
 - (E) cuidar da interface entre a camada de aplicação e camada de transporte para transmissões de dados multimídia.
63. O conjunto de normas e padrões do protocolo TCP/IP é descrito em documentos chamados de:
- E**
- (A) Reports Per Comments.
 - (B) Reports For Comments.
 - (C) Remote Procedure Calls.
 - (D) Requests Per Comments.
 - (E) Requests For Comments.

RTP



- **Numeração sequenciada:** o RTP atribui número de ordem aos pacotes. Isto pode ser usado para verificação das perdas, sequenciamento e possível redirecionamento de pacotes pelas aplicações.
- **Selo de temporização (estampilha - *timestamp*):** possibilita a correta temporização dos pacotes contendo áudio e/ou vídeo.
- **Envio de pacotes sem retransmissão:** característica fundamental das transmissões em multimídia, pequenas perdas não comprometem a qualidade do envio e a não retransmissão torna o sistema mais ágil. O RTP apenas permite ao receptor verificar a existência das perdas e ou atrasos.
- **Identificação de origem:** Necessário para indicar quem enviou o pacote. Numa conferência multicast, um mesmo fluxo pode ter várias origens.
- **Identificação de conteúdo:** permite a alteração dinâmica dos vocoders em redes sem garantia de QoS em função das perdas e do atraso a fim de melhorar a qualidade final acústica.
- **Sincronismo:** pacotes de um mesma corrente podem sofrer diferentes atrasos. A variação deste atraso é prejudicial à reprodução da mídia. Buffers adicionais podem então ser utilizados para eliminar a diferença entre os atrasos (jitter). Esses mecanismos processam de informações de tempo de cada pacote. O RTP provê esta informação.

Apesar de todas essas vantagens, o RTP ainda não possui componentes de segurança e nem monitora a transmissão nem a recepção dos pacotes. Essa última tarefa é realizada pelo RTCP

31

Para os protocolos utilizados em redes de computadores, analise as afirmativas a seguir.

- I – Um determinado host A está recebendo dados de um host B em uma taxa mais alta do que pode processar, e para reduzir a taxa de transmissão, o host A pode enviar para o host B uma mensagem ICMP source quench.
- II – Para um host determinar um endereço Ethernet, a partir de um endereço IP, deve enviar uma mensagem ARP Request.
- III – No protocolo SNMP, a MIB é um componente de hardware independente utilizado para realizar funções complexas de gerenciamento de rede.

D

Está(ão) correta(s) a(s) afirmativa(s)

- | | |
|------------------|---------------------|
| (A) I, apenas. | (B) II, apenas. |
| (C) III, apenas. | (D) I e II, apenas. |
| (E) I, II e III. | |

Type	Name	Reference
0	Echo Reply	[RFC792]
1	Unassigned	[JBP]
2	Unassigned	[JBP]
3	Destination Unreachable	[RFC792]
4	Source Quench	[RFC792]
5	Redirect	[RFC792]
6	Alternate Host Address	[JBP]
7	Unassigned	[JBP]
8	Echo	[RFC792]
9	Router Advertisement	[RFC1256]
10	Router Selection	[RFC1256]
11	Time Exceeded	[RFC792]
12	Parameter Problem	[RFC792]
13	Timestamp	[RFC792]
14	Timestamp Reply	[RFC792]
15	Information Request	[RFC792]
16	Information Reply	[RFC792]
17	Address Mask Request	[RFC950]
18	Address Mask Reply	[RFC950]
19	Reserved (for Security)	[Solo]
20-29	Reserved (for Robustness Experiment)	[ZSu]
30	Traceroute	[RFC1393]
31	Datagram Conversion Error	[RFC1475]
32	Mobile Host Redirect	[David Johnson]
33	IPv6 Where-Are-You	[Bill Simpson]
34	IPv6 I-Am-Here	[Bill Simpson]
35	Mobile Registration Request	[Bill Simpson]
36	Mobile Registration Reply	[Bill Simpson]
37-255	Reserved	[JBP]
40	Authentication Failures	[RFC2521]

5	Redirect	[RFC792]
Codes		
0	Redirect Datagram for the Network (or subnet)	
1	Redirect Datagram for the Host	
2	Redirect Datagram for the Type of Service and Network	
3	Redirect Datagram for the Type of Service and Host	
Destination Unreachable	[RFC792]	
Codes		
0	Net Unreachable	[RFC792]
1	Host Unreachable	[RFC792]
2	Protocol Unreachable	[RFC792]
3	Port Unreachable	[RFC792]
4	Fragmentation Needed and Don't Fragment was Set	[RFC792]
5	Source Route Failed	[RFC792]
6	Destination Network Unknown	[RFC1122]
7	Destination Host Unknown	[RFC1122]
8	Source Host Isolated	[RFC1122]
9	Communication with Destination Network is Administratively Prohibited	[RFC1122]
10	Communication with Destination Host is Administratively Prohibited	[RFC1122]
11	Destination Network Unreachable for Type of Service	[RFC1122]
12	Destination Host Unreachable for Type of Service	[RFC1122]
13	Communication Administratively Prohibited	[RFC1812]
14	Host Precedence Violation	[RFC1812]
15	Precedence cutoff in effect	[RFC1812]
11	Time Exceeded	[RFC792]
Codes		
0	Time to Live exceeded in Transit	
1	Fragment Reassembly Time Exceeded	
12	Parameter Problem	[RFC792]
Codes		
0	Pointer indicates the error	
1	Missing a Required Option	[RFC1108]
2	Bad Length	

32

A figura abaixo ilustra o cabeçalho de um datagrama IP (IPv4).

Versão	Comprimento do Cabeçalho	Tipo de Serviço	Comprimento do Datagrama					
Identificador			Flags	Deslocamento de Fragmentação				
Tempo de Vida	Protocolo		Bits para verificação da Integridade do Cabeçalho					
Endereço IP da Fonte								
Endereço IP do Destino								
Opções								

Quais dos campos do cabeçalho indicam, respectivamente, a qual datagrama pertence um fragmento recém chegado ao host de destino e a que processo de transporte a camada de rede deve entregar o datagrama, uma vez completo?

- (A) Flags e Tipo de Serviço.
- (B) Tempo de Vida e Deslocamento de Fragmentação.
- (C) Identificador e Protocolo.
- (D) Identificador e Deslocamento de Fragmentação.
- (E) Tipos de Serviço e Identificador.

C

33

O processo de traceroute consiste em obter o caminho que um pacote atravessa por uma rede de computadores até chegar ao destinatário. O traceroute também ajuda a detectar onde ocorrem os congestionamentos na rede, já que é dado, no relatório, o(a)

- (A) número de pacotes enviados com erro.
- (B) tamanho dos pacotes que sofreram colisão.
- (C) total de tabelas de roteamento percorridas entre a origem e o destino.
- (D) latência até cada máquina interveniente.
- (E) banda ocupada pelos pacotes enviados para a máquina destino.

D

```
C:\Documents and Settings\Sauer>tracert www.velex.com.br
Rastreando a rota para www.velex.com.br [200.223.247.67]
com no máximo 30 saltos:
 1  *      *      *      *      Esgotado o tempo limite do pedido.
 2  *      *      *      *      Esgotado o tempo limite do pedido.
 3  164 ms  188 ms  195 ms      xe-0-0-0-531-arc-rj-rot1-01.telemar.net.br [200.164.45.187]
 4  160 ms  160 ms  196 ms      200223045166.host.telemar.net.br [200.223.45.166]
 5  165 ms  197 ms  200 ms      gigabitethernet6-0-0-mpi-ng-man-sw13-01.telemar.net.br [200.195.78.29]
 6  173 ms  179 ms  177 ms      20118104206.host.telemar.net.br [201.18.104.206]
 7  *      *      *      *      Esgotado o tempo limite do pedido.
```

53

A transmissão de áudio e vídeo em tempo real, através da Internet, enfrenta uma série de obstáculos que dificultam o atendimento aos requisitos de QoS. Para minimizar o efeito destes obstáculos é possível utilizar técnicas de processamento de sinais e determinados protocolos de comunicação. A técnica ou protocolo que **NÃO** é indicado para este tipo de aplicação é(são)

- (A) o protocolo UDP, em vez do TCP.
- (B) os protocolos de roteamento que levem em conta a prioridade dos pacotes.
- (C) os algoritmos para controle de fluxo e de congestionamento na rede.
- (D) os códigos corretores de erro do tipo FEC.
- (E) as técnicas de codificação de fonte com boas características de desempenho, como grande compressão e pequenas perdas.

C

55

O SIP (Session Initiation Protocol) é um protocolo, que utiliza o modelo requisição-resposta, similar ao HTTP, para iniciar sessões de comunicação interativa entre utilizadores. No contexto deste protocolo, o método ACK é utilizado para

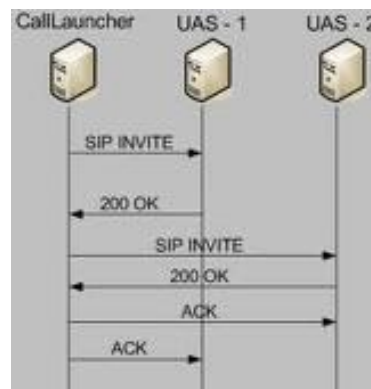
- (A) solicitar a inicialização de uma sessão.
- (B) solicitar o término de uma sessão.
- (C) confirmar que uma sessão foi inicializada.
- (D) consultar um host sobre seus recursos.
- (E) cancelar uma solicitação pendente.

C

- FEC – Forward Error Correction – Envio antecipado de bits adicionais aos dados visando uma possível correção sem retransmissão

– Ex.: Hamming, Viterbi, Reed-Solomon

- Método ACK



62

A arquitetura Diffserv é capaz de prover QoS em redes IP. Com relação a esta arquitetura, considere as afirmativas abaixo.

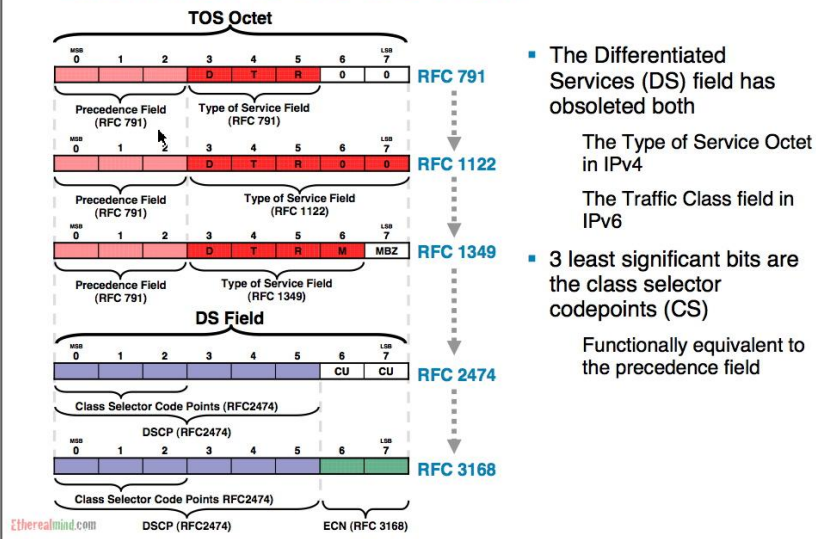
- I – O campo Differentiated Services (DS) no pacote Ipv6 é marcado com um padrão binário específico chamado DSCP (DS Codepoint) e é utilizado para indicar como os roteadores devem tratar o pacote em termos de QoS.
- II – O tratamento de QoS dado a cada pacote, em cada roteador da rede, é denominado Per Hop Behavior (PHB), e cada roteador de um domínio Diffserv tem sua tabela própria para a determinação do PHB em função do DSCP do pacote.
- III – O conjunto de fluxos de tráfegos pertencentes à mesma classe de serviço é denominado, na nomenclatura Diffserv sobre MPLS, Behavior Aggregates (BA).

Está(ão) correta(s) a(s) afirmativa(s)

- (A) I, apenas.
- (B) II, apenas.
- (C) III, apenas.
- (D) I e II, apenas.
- (E) I, II e III.

E

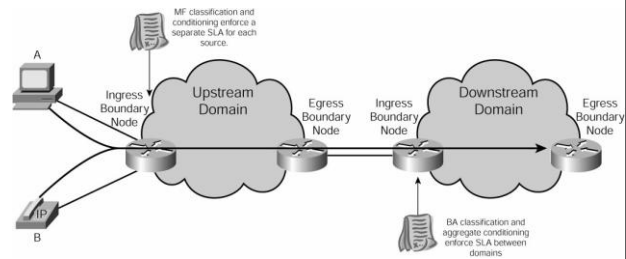
Evolution to the DS Field



DiffServ Terminology

The DiffServ architecture introduces many new terms. This section presents a simplified definition of a selected few of them. The upcoming sections explain the terms in more detail. RFC 2475 and 3260 introduce the complete list of terms:

- **Domain** A network with a common DiffServ implementation (usually under the same administrative control).
- **Region** A group of contiguous DiffServ domains.
- **Egress node** Last node traversed by a packet before leaving a DiffServ domain.
- **Ingress node** First node traversed by a packet when entering a DiffServ domain.
- **Interior node** Node in a DiffServ domain that is not an egress or ingress node.
- **DiffServ field** Header field where packets carry their DiffServ marking. This field corresponds to the six most significant bits of the second byte in the IP header (formerly, IPv4 TOS [Type-of-Service octet and IPv6 Traffic Class octet]).
- **Differentiated Services Code Point (DSCP)** A specific value assigned to the DiffServ field.
- **Behavior aggregate (BA)** Collection of packets traversing a DiffServ node with the same DSCP.
- **Ordered aggregate (OA)** A set of BAs for which a DiffServ node must guarantee not to reorder packets.
- **BA classifier** Classifier that selects packets based on DSCP.
- **Multifield (MF) classifier** Classifier that selects a packet based on multiple fields in the packet header (for example, source address, destination address, protocol, and protocol port).
- **Per-hop behavior (PHB)** Forwarding behavior or service that a BA receives at a node.
- **Per-hop behavior group** One or more PHBs that are implemented simultaneously and define a set of related forwarding behaviors.
- **PHB scheduling class (PSC)** A set of PHBs for which a DiffServ node must guarantee not to reorder packets.
- **Traffic profile** Description of a traffic pattern over time. Generally, in terms of a token bucket (rate and burst).
- **Marking** Setting the DSCP in a packet.
- **Metering** Measuring of a traffic profile over time.
- **Policing** Discarding of packet to enforce conformance to a traffic profile.
- **Shaping** Buffering of packets to enforce conformance to a traffic profile.
- **Service level agreement (SLA)** Parameters that describe a service contract between a DiffServ domain and a domain customer.
- **Traffic-conditioning specification** Parameters that implement a service level specification.
- **Traffic-conditioning** The process of enforcing a traffic conditioning specification through control functions such as marking, metering, policing, and shaping.



32

A SSL (Secure Sockets Layer), um pacote de segurança que fornece criptografia de dados e autenticação entre um cliente e um servidor Web,

- (A) exige que ambos, cliente e servidor, possuam certificados digitais.
- (B) opera na camada física do TCP/IP construindo uma conexão segura entre cliente e servidor.
- (C) garante a privacidade e a autenticação do cliente, mas não garante a integridade da mensagem.
- (D) se restringe aos navegadores utilizados para navegar na Internet.
- (E) utiliza uma combinação de tecnologias de chave secreta e pública para garantir a segurança dos dados transmitidos.

E

39

Após enviar um datagrama para um servidor na Internet, uma estação recebeu uma mensagem ICMP TIME EXCEEDED. Significa que

- (A) a taxa de transmissão da estação deve ser diminuída.
- (B) o campo TTL (Time to Live) do datagrama assumiu o valor 0.
- (C) o servidor de destino não foi localizado na rede.
- (D) os datagramas enviados como retorno pelo servidor estão corrompidos.
- (E) os datagramas estão sendo gerados com erro porque existe um bug no *software* da estação.

B**45**

Um analista precisa modificar o endereço MAC de uma estação conectada à rede local. Para realizar essa tarefa ele deve

- (A) solicitar que o servidor de DHCP envie um novo endereço IP para a estação.
- (B) editar o endereço na BIOS da estação e reinicializar a estação.
- (C) trocar a placa de rede da estação.
- (D) trocar a porta de conexão da estação ao hub da rede.
- (E) limpar a tabela CAM do switch da rede.

C

47

Campo X	Delimitador de Início de Frame	Endereço de Destino	Endereço de Origem	Tipo ou tamanho	Dados	Preenchimento	Sequência de verificação de quadros
7 bytes	1 byte	6 bytes	6 bytes	2 bytes	0 a 1500 bytes	0 a 46 bytes	4 bytes

A figura acima apresenta um quadro Ethernet/802.3.
O campo identificado por Campo X é o(a)

- (A) preâmbulo.
- (B) endereço MAC.
- (C) máscara de rede.
- (D) classe da rede.
- (E) porta de destino.

A

55

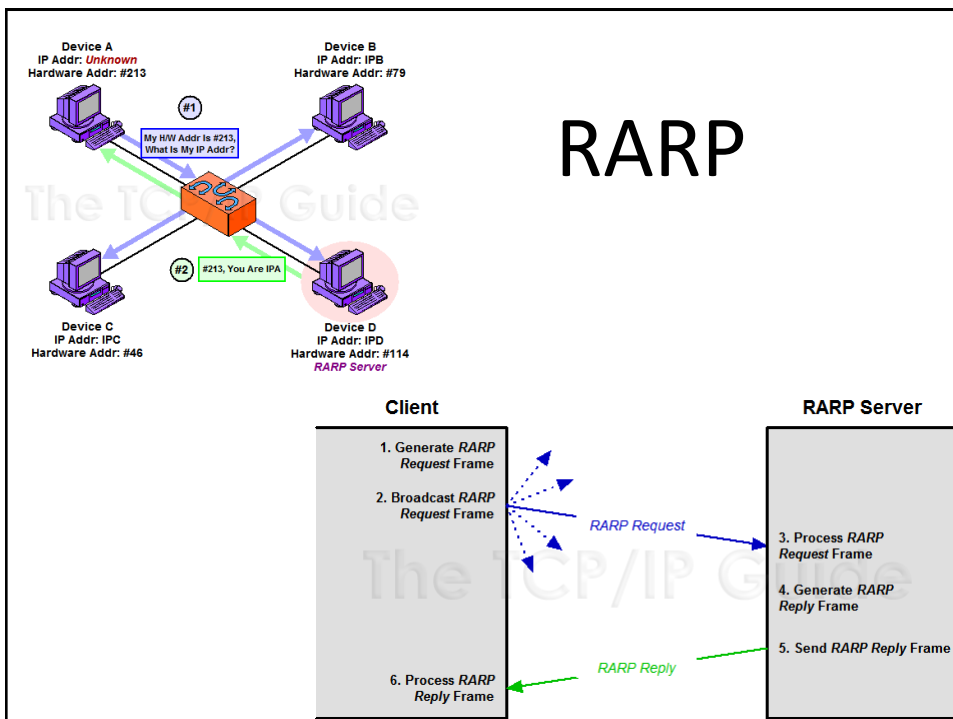
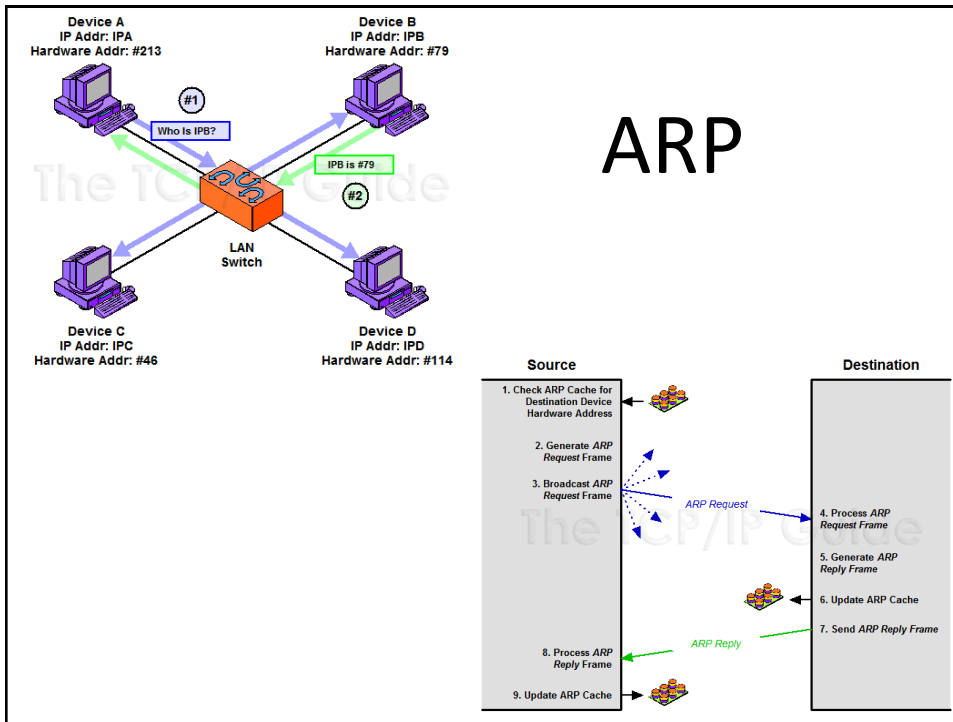
Sobre o protocolo TCP/IP, são feitas as afirmativas a seguir.

- I – O protocolo RARP (Reverse Address Resolution Protocol) pode ser utilizado por um computador sem disco rígido para obter seu endereço de IP de um servidor RARP.
- II – Se um roteador se torna muito congestionado para armazenar em buffer quaisquer outros datagramas, as mensagens de ICMP (Internet Control Messaging Protocol) podem ser utilizadas para diminuir o fluxo de datagramas desse roteador.
- III – O procedimento adotado pelo TCP/IP para detectar a perda de um pacote é o recebimento de uma mensagem de um roteador de rede informando que um pacote foi descartado.

Está(ão) correta(s) a(s) afirmativa(s)

- (A) I, apenas.
- (B) II, apenas.
- (C) III, apenas.
- (D) I e II, apenas.
- (E) I, II e III.

D



74. O protocolo L2TP utilizado na implementação de VPNs atua na camada

- (A) Física.
- (B) Rede.
- (C) Enlace.
- (D) Transporte.
- (E) Aplicação.

C

25. Considerando o modelo TCP/IP em cinco camadas, ou seja, aplicação, transporte, rede, enlace e física, os protocolos HTTP e TCP, pertencem, respectivamente, às camadas

- (A) rede e enlace.
- (B) aplicação e rede.
- (C) aplicação e transporte.
- (D) física e transporte.
- (E) transporte e rede.

C

57

Em determinada reunião técnica em uma empresa, um administrador de redes indica que, no modelo OSI, a camada responsável pela gestão de diálogos é a de

- (A) sessão.
- (B) enlace.
- (C) rede.
- (D) aplicação.
- (E) transporte.

A

```
0.544624 00:01:01:00:01:01 > 00:03:03:03:03:03, ethertype IPv4 (0x0800), length 66: (tos 0x0, ttl 64, id 48455,
offset 0, flags [DF], proto: TCP (6), length: 52) 10.0.0.4.22 > 10.0.0.1.1821: P, cksum 0xf520 (correct),
610292262:610292274(12) ack 1867580146 win 6432
0.543601 00:03:03:03:03:03 > 00:02:02:02:02:02, ethertype IPv4 (0x0800), length 66: (tos 0x0, ttl 64, id 48455,
offset 0, flags [DF], proto: TCP (6), length: 52) 10.0.0.4.22 > 10.0.0.1.1821: P, cksum 0xf520 (correct), 0:12(12)
ack 1 win 6432
0.699554 00:02:02:02:02:02 > 00:03:03:03:03:03, ethertype IPv4 (0x0800), length 60: (tos 0x0, ttl 128, id 33657,
offset 0, flags [DF], proto: TCP (6), length: 40) 10.0.0.1.1821 > 10.0.0.4.22: ., cksum 0x6b48 (correct), ack 12
win 17197
0.666090 00:03:03:03:03:03 > 00:01:01:00:01:01, ethertype IPv4 (0x0800), length 60: (tos 0x0, ttl 128, id 33657,
offset 0, flags [DF], proto: TCP (6), length: 40) 10.0.0.1.1821 > 10.0.0.4.22: ., cksum 0x6b48 (correct), ack 12
win 17197
2.791857 00:02:02:02:02:02 > 00:03:03:03:03:03, ethertype IPv4 (0x0800), length 454: (tos 0x0, ttl 128, id 33660,
offset 0, flags [DF], proto: TCP (6), length: 440) 10.0.0.1.1821 > 10.0.0.4.22: P 1:401(400) ack 12 win 17197
2.768640 00:03:03:03:03:03 > 00:01:01:00:01:01, ethertype IPv4 (0x0800), length 454: (tos 0x0, ttl 128, id 33660,
offset 0, flags [DF], proto: TCP (6), length: 440) 10.0.0.1.1821 > 10.0.0.4.22: P 1:401(400) ack 12 win 17197
2.822118 00:01:01:00:01:01 > 00:03:03:03:03:03, ethertype IPv4 (0x0800), length 60: (tos 0x0, ttl 64, id 48456,
offset 0, flags [DF], proto: TCP (6), length: 40) 10.0.0.4.22 > 10.0.0.1.1821: ., cksum 0x8f95 (correct), ack 401
win 7504
2.793644 00:03:03:03:03:03 > 00:02:02:02:02:02, ethertype IPv4 (0x0800), length 60: (tos 0x0, ttl 64, id 48456,
offset 0, flags [DF], proto: TCP (6), length: 40) 10.0.0.4.22 > 10.0.0.1.1821: ., cksum 0x8f95 (correct), ack 401
win 7504
```

Considerando o trecho de captura apresentado acima, julgue os próximos itens.

- 66 A partir do trecho mostrado, é correto afirmar que existem eventos em que a retransmissão do TCP está atuando.
- 67 Se a máscara utilizada for /24, os *hosts* presentes na captura estarão todos na mesma rede.
- 68 Ainda que fosse necessária, a fragmentação no nível do IP não ocorreria.
- 69 A linha temporal é consistente com a ordem dos *frames* no trecho da captura em questão.

E

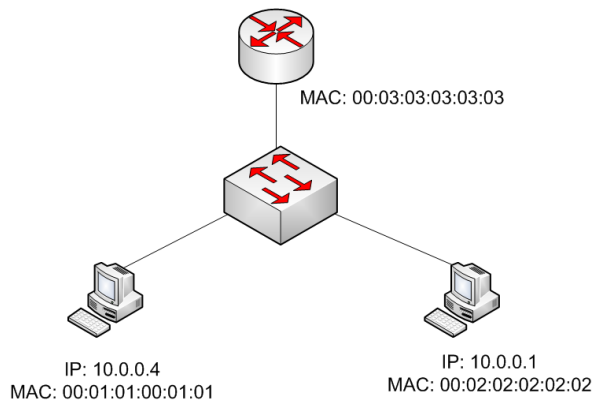
C

C

E

16:23:01.079553 churchward.erg.abdn.ac.uk.33635 > gordon.erg.abdn.ac.uk.32772: P 12765:12925(160) ack 19829 win 24820 (DF)

Timestamp 16:23:01.079553
 Source address churchward.erg.abdn.ac.uk
 Source port 33635
 Destination address gordon.erg.abdn.ac.uk
 Destination port 32772
 Indicates that the PUSH flag is set P
 Sequence number (also start byte) 12765:
 Contained data bytes from sequence number upto but not including 12925
 Number of user data bytes in datagram (160)
 Details of acknowledgements, Window size and Header flags ack 19829 win 24820 (DF)



39

Observe as afirmativas abaixo, relacionadas a datagramas IPv4.

- I – Em situações de congestionamento, os datagramas com o bit DF igual a 1 devem ser descartados.
- II – A remontagem de datagramas sempre ocorre no destino.
- III – Quando a MTU de uma rede é menor que o campo *offset* do datagrama a ser trafegado, ocorre a fragmentação.

Está(ão) correta(s) a(s) afirmativa(s)

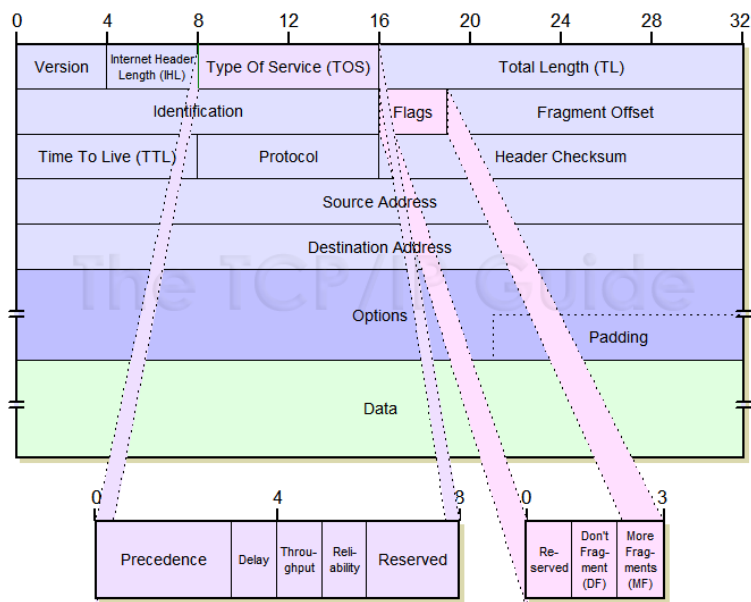
- (A) I, somente.
- (B) II, somente.
- (C) I e II, somente.
- (D) II e III, somente.
- (E) I, II e III.

B

- Assertiva A – Falsa. O flag DF (o do meio – ver figura) significa "*don't fragment*". Se o pacote passar por um roteador cujo MTU seja inferior ao tamanho do pacote, ele será descartado por não poder ser fragmentado. A resposta remete ao bit DE do Frame Relay, que em caso de congestionamento torna o pacote eleito para descarte.
- Assertiva B – Verdadeira. Não só a remontagem dos datagramas quanto dos segmentos de mensagem também.
- Assertiva C – Falsa. O campo *Fragment Offset* indica a posição, em número de blocos de 8 bytes, do fragmento em relação ao pacote original. O primeiro fragmento tem offset 0 (zero), o segundo tem o tamanho do primeiro fragmento / 8, o terceiro soma o offset anterior com o tamanho do segundo fragmento / 8 e assim por diante, até que o bit MF (More fragments) venha setado em 0 (zero).

Resposta certa letra B

Cabeçalho IPv4



54

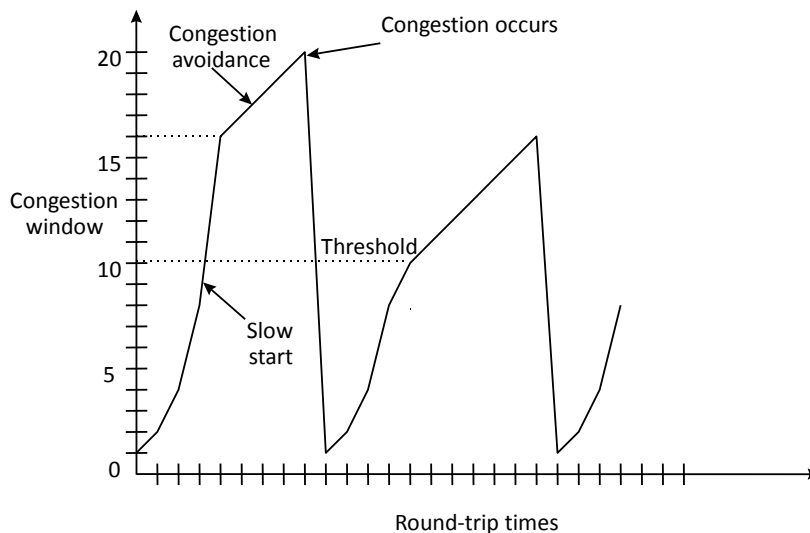
O algoritmo de *slow start* do TCP

- (A) obriga que a fonte retransmita segmentos sem que se espere pelo *timeout*, no caso de recebimento de três reconhecimentos (ACK) duplicados.
- (B) impede que segmentos cheguem fora de ordem devido a congestionamentos em *links* de baixa velocidade.
- (C) utiliza os *bits* URG e PSH para indicar retransmissões prioritárias, no caso de fontes com baixa velocidade de transmissão.
- (D) limita o tamanho da janela deslizante de recepção a 1 *byte*, durante o ciclo de vida de uma conexão TCP.
- (E) eleva, gradativamente, a taxa de transmissão de tráfego na rede até que seja atingida uma situação de equilíbrio.

E

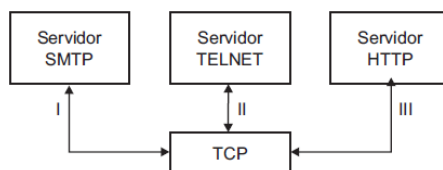
- Slow Start e Congestion Avoidance são dois algoritmos de controle de congestionamento do TCP
 - Slow Start – Ao invés de inundar a rede e o receptor de segmentos, o emissor inicia com 1 segmento e a cada ACK recebido incrementa o tamanho da janela no número de segmentos reconhecidos, fazendo um crescimento exponencial. Ao chegar no limite, entra em Congestion avoidance, que é o aumento linear do número de segmentos até que um congestionamento ocorra, reduzindo o número de segmentos por envio para 1 e reiniciando o slow start, dividindo o limite da janela por 2.
 - Resposta certa letra E

Resposta (cont)



70

O TCP tem como base a comunicação ponto a ponto entre dois *hosts* de rede. Nessa atividade, o TCP recebe os dados de programas e processa esses dados como um fluxo de *bytes*. Os *bytes* são agrupados em segmentos que o TCP numera e sequencia para entrega. Estes segmentos são mais conhecidos como Pacotes. Na comunicação, antes que dois *hosts* TCP possam trocar dados, devem primeiro estabelecer uma sessão entre si, inicializada através de um processo de *handshake*, que visa a sincronizar os números de sequência e oferece informações de controle necessárias para estabelecer uma conexão virtual entre os dois *hosts*. Os programas TCP usam números de porta reservados ou conhecidos, conforme a aplicação. Considerando essas informações, observe a figura abaixo.



Os valores padronizados para as portas identificadas por I, II e III são, respectivamente,

- (A) 20, 21 e 80
- (B) 20, 23 e 53
- (C) 25, 20 e 53
- (D) 25, 21 e 80
- (E) 25, 23 e 80

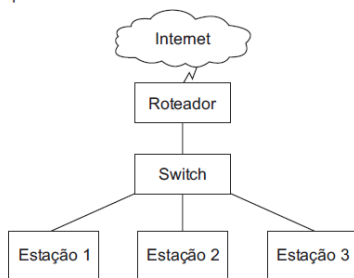
E

Resposta

- Outras portas típicas importantes (DECORAR !):
 - 20 - data e 21- control – FTP (TCP)
 - 22 – SSH (TCP)
 - 53 – DNS (UDP e TCP)
 - 67 – server e 68 – client – DHCP (UDP)
 - 69 – TFTP (UDP)
 - 110 – pop3 (TCP), 143 – IMAP4 (TCP)
 - 161 (síncrono) e 162 (assíncrono) – SNMP (UDP)
 - 443 – HTTPS (TCP)
 - RTP – porta par UDP, RTCP – porta ímpar a seguir (UDP)

38

Suponha a seguinte topologia de rede IP de uma pequena empresa:



O roteador em questão possui um endereço Internet válido em sua interface de rede externa, além de um endereço na mesma sub-rede (192.168.100.0/24) das estações em sua interface de rede interna. Para que as estações se conectem diretamente a servidores HTTP na Internet, o roteador realiza NAT. As estações estão com os sistemas operacionais:

Estação 1: Linux, Estação 2: Windows XP, Estação 3: Windows 2003.

O roteador foi acidentalmente reinicializado (*reboot*), demandando 25 segundos para retomar à operação normal. Imediatamente antes da reinicialização, cada estação efetuava *download* de arquivos via HTTP. É correto afirmar que nessa reinicialização,

- (A) todas as conexões TCP das 3 estações foram destruídas.
- (B) somente as conexões HTTP 1.1 da estação 3 sobreviveram.
- (C) somente as conexões HTTP 1.1 das estações 1, 2 e 3 sobreviveram.
- (D) somente as conexões TCP da estação 1 sobreviveram.
- (E) nenhuma conexão TCP foi destruída.

A

Resposta

- Letra A. Como o NAT está em uso, a conexão fim-a-fim é da estação com o roteador, que faz uma conexão fim-a-fim com o destino final. Como o roteador caiu, todos os processos foram reiniciados, perdendo o conteúdo das janelas e todo o controle da conexão virtual.

53

Que camada no modelo OSI é responsável por converter diferentes representações de números inteiros na comunicação entre dois sistemas distintos?

- (A) Apresentação
- (B) Sessão
- (C) Transporte
- (D) Padronização
- (E) Aplicação

A

Resposta

- FERTSAA !!!!
 - Física – interpretar e representar bits
 - Enlace – agrupar os bits em quadros, detectar erros e descartar quadros corrompidos
 - Rede – endereçamento lógico e roteamento do pacote.
 - Transporte – Garantir confiabilidade na comunicação fim-a-fim dos segmentos de mensagem
 - Sessão – controlar a comunicação entre os processos das máquinas fim-a-fim
 - Apresentação – Traduções de códigos, criptografia e compactação
 - Aplicação – Oferecer uma interface ao usuário
- Resposta certa letra A

1

A respeito de rede de computadores, relacione as características aos protocolos abaixo.

Características	Protocolo
I – Oferece serviço que permite acessar servidores remotos, como email e sites na web, sem ter que saber o endereço IP do servidor. Basta saber o nome do site, pois o serviço realiza a tradução.	P - DNS Q - FTP R - HTTP S - IPSEC T - SMTP U - SSH V - TELNET
II – Oferece serviço para execução de shell remoto, sem criptografar os comandos trafegados.	
III – Oferece serviço para execução de shell remoto, criptografando os comandos trafegados.	

Estão corretas as associações:

- (A) I - P , II - V , III - S
 (B) I - P , II - V , III - U
 (C) I - R , II - V , III - S
 (D) I - T , II - Q , III - U
 (E) I - T , II - Q , III - S

B

18-Em relação ao protocolo TCP/IP é correto afirmar que

- a) um endereço IP especifica um computador individual.
- b) um endereço IP não especifica uma conexão com uma rede.
- c) os endereços internet podem ser usados para se referir a redes.
- d) os endereços internet não podem ser usados para se referir a *hosts* individuais.
- e) os endereços internet podem ser usados para se referir a redes e a *hosts* individuais.

E

46- Os níveis do modelo de referência OSI são os seguintes, na ordem apresentada:

- a) Protótipo, Físico, Sistema, Rede, Sessão, Categoria, Transporte.
- b) Físico, Lógico, Rede, Transação, Sessão, Implantação, Aplicação.
- c) Físico, Enlace, Lógico, Transporte, Rede, Implementação, Sessão.
- d) Físico, Enlace, Rede, Transporte, Sessão, Apresentação, Aplicação.
- e) Inicial, Físico, *Hardware*, Transporte, Interação, Apresentação, Segurança.

D

47- A função do nível físico do modelo OSI é

- a) fornecer mecanismos de verificação utilizados pelo nível posterior.
- b) permitir o fluxo de bits agregados segundo critérios estabelecidos pela topologia da rede.
- c) permitir o envio de uma cadeia de *bytes* pela rede, verificando seu significado e sua composição em *bits*.
- d) controlar o envio de mensagens pela rede, preocupando-se com o seu significado e com a forma como esses *bits* são agregados.
- e) permitir o envio de uma cadeia de *bits* pela rede sem se preocupar com o seu significado ou com a forma como esses *bits* são agregados.

E

48- Quanto às funções multiplexação e o *splitting*, é correto afirmar que

- a) são importantes em um dos níveis do modelo OSI.
- b) apenas uma delas pertence a um dos níveis do modelo OSI.
- c) não estão contempladas em nenhum dos níveis do modelo OSI.
- d) são o mesmo que chaveamento e roteamento, respectivamente.
- e) equivalem a gerenciamento de *token* e controle de diálogo, respectivamente.

A

52- Quanto ao Protocolo TCP, é correto afirmar que

- a) exige um serviço de rede confiável para operar.
- b) um *socket* identifica biunivocamente um usuário TCP em toda inter-rede.
- c) as conexões são *half-duplex*, ou seja transportam dados em apenas uma direção.
- d) foi projetado para funcionar em um serviço de rede conectado e com confirmações.
- e) foi projetado para funcionar em um serviço de rede sem conexão e sem confirmação.

E