PROCESSO SELETIVO - Grupo de Resposta a Incidentes de Segurança

Nome: Fernanda Veiga Gomes da Fonseca
TAG - Redes - Entrega: 15/03/2020

1-

No modelo OSI, há sete camadas de abstração que representam funções de cada componente em uma rede: física, enlace, rede, transporte, sessão, apresentação e aplicação.

Camada física: descreve as interfaces do meio físico, tratando da modulação e codificação, transmissão e recepção dos bits “brutos”.

Camada de enlace: responsável pela transferência de dados entre elementos de rede vizinhos, ou seja, pela recepção, delimitação e transmissão de quadros, estabelecendo um protocolo de comunicação entre eles (Ethernet, WiFi).

Camada de rede: lida com o encaminhamento e roteamento de datagramas, podendo realizar fragmentação e remontagem dos pacotes. É responsável pelo endereçamento dos pacotes, convertendo o endereço IP em MAC, utilizado na camada de enlace.

Camada de transporte: lida com a comunicação entre sistemas finais na rede, tratando de segmentos de forma orientada à conexão (TCP) ou não (UDP).

Camada de sessão: define a forma de transmissão de dados entre aplicações em máquinas diferentes.

Camada de apresentação: pode converter o padrão de caracteres, comprimir os dados e criptografá-los.

Camada de aplicação: identifica as aplicações utilizadas, definindo os protocolos necessários (HTTP, SMTP, POP3, FTP).

2-

Domínio de broadcast: segmento lógico de uma rede que um dispositivo conectado à rede é capaz de se comunicar com outro sem a necessidade de utilizar um dispositivo de roteamento.

Domínio de colisão: segmento lógico de uma rede onde os pacotes transmitidos por dispositivos nele podem colidir uns com os outros. Colisões são frequentes em topologias de barramento ou em topologias formadas pela interligaçao das estações através de hubs.

3-

Domínios de broadcast:

1- R1-S1 + S1-PC1 + S1-PC2

2- R1-PC3

3- R2-H1 + H1-PC4 + H1-PC5

Domínios de colisão:

1- R1-S1

2- S1-PC1

3- S1-PC2

4- R1-PC3

5- R2-R1

6- R2-H1

7- H1-PC4 + H1-PC5 (OBS: No hub, o dispositivo também pertence ao domínio de colisão, não apenas as conexões.)

4-

Primeiro, o computador A envia uma requisição ARP, gerando uma tabela de encaminhamento. Então, procura pelo endereço MAC do computador B, porém não o encontra. Assim, deve enviar uma mensagem com o IP B encapsulada em uma mensagem com o IP de R1 e MAC eth0 de R1. Em seguida, R1 envia uma requisição ARP para montar sua tabela de encaminhamento e, como não encontra B, envia uma mensagem ainda com IP B encapsulada em uma mensagem com IP R2 e MAC eth0 de R2. Quando a mensagem chega a R2, o mesmo processo acontece, porém ele possui o computador B relacionado em sua tabela. Dessa forma, envia os dados originais de A para B utilizando IP B e MAC B. A confirmação do recebimento enviada para o computador A segue uma lógica semelhante (forma resumida: IP R2 + MAC eth1 R2 + IP A + dados, IP R1 + MAC eth1 R1 + IP A + dados, IP A + MAC A + dados).

5-

Como o endereço do computador A é local, quando a mensagem enviada a R1 chegar no mesmo, o IP de A deve ser resolvido pelo NAT antes de a próxima mensagem ser enviada para R2. As etapas seguintes do envio e as etapas da confirmação enviada por B serão iguais às apontadas anteriormente.

6-

O protocolo TCP estabelece conexões em três etapas, conhecidas como “three-way handshake”. Primeiro, o cliente envia um segmento de controle “SYN” para o servidor, especificando o seu número de sequência inicial (não há envio de dados). Em seguida, o servidor responde com um segmento de controle “SYN+ACK”, indicando que recebeu o segmento do cliente (“ACK”) e definindo seu número de número de sequência inicial (“SYN”). Por último, o cliente responde com um segmento “ACK”, snalizando que recebeu o segmento.

7-

São padrões de placas utilizadas em dispositivos de uma rede. O padrão MDI é usado em dispositivos de borda (por exemplo, roteadores), enquanto o padrão MDI-X, em dispositivos intermediários (hubs, switches). Se a comunicação ocorrer entre dispositivos com padrões diferentes, o mesmo padrão de cabeamento das extremidades pode ser utilizado (T568A ou T568B), porque o local de transmissão de um é equivalente ao local de recepção do outro. Entretanto, se a comunicação ocorrer entre dispositivos de mesmo tipo (entre computadores, por exemplo), deve ser utilizada a “comunicação cross” (por exemplo, de um lado seria T568A e do outro, T568B).

8-

Caso 1: Os dispositivos possuem padrões de placa diferentes. Por isso, o padrão de cabeamento é igual nas extremidades (T568A ou T568B).

Caso 2: Os dispositivos possuem o mesmo padrão de placa. Por isso, o padrão de cabeamento é diferente nas extremidades (“comunicação cross”).

Considerando que o padrão MDI pode ser identificado nos dispositivos A, R1, R2 e B, enquanto que o padrão MDI-X é visto em S1 e S2, as conexões seguem uma das lógicas acima. A-S1: caso 1, S1-S2: caso 2, S2-R1: caso 1, R1-R2: caso 2 e R2-B: caso 2.

9-

1. 10110001.00100000.10101000.11011111 (IP)
   11111111.11111111.11111111.11111000 (máscara)

Classe B

Rede: 177.32.168.216 (10110001.00100000.10101000.11011000)

Hosts: 177.32.168.217 a 177.32.168.222

Broadcast: 177.32.168.223
(10110001.00100000.10101000.11011111)

2. 11001100.00010100.10001111.00000000 (IP)
   11111111.11111111.11000000.00000000 (máscara)

Classe C

Rede: 204.20.128.0 (11001100.00010100.10000000.00000000)

Hosts: 204.20.128.1 a 204.20.191.254

Broadcast: 204.20.191.255
(11001100.00010100.10111111.11111111)

3. 00100100.01001000.01101101.00011000 (IP)
   11111111.11111110.00000000.00000000 (máscara)

Classe A

Rede: 36.72.0.0 (00100100.01001000.00000000.00000000)

Hosts: 36.72.0.1 a 36.73.255.254

Broadcast: 36.73.255.255
(00100100.01001001.11111111.11111111)

4. 00000111.00011010.00000000.01000000 (IP)
   11111111.11111111.11111111.11000000 (máscara)

Classe A

Rede: 7.26.0.64 (00000111.00011010.00000000.01000000)

Hosts: 7.26.0.65 a 7.26.0.126

Broadcast: 7.26.0.127

(00000111.00011010.00000000.01111111)

5. 11001000.11001001.10101101.10111011 (IP)

11111111.11111111.11111111.11111100 (máscara)

Classe C

Rede: 200.201.173.184 (11001000.11001001.10101101.10111000)

Hosts: 200.201.173.185 a 200.201.173.186

Broadcast: 200.201.173.187

(11001000.11001001.10101101.10111011)

10-

1. Uma vez que a rede é dada por 240.128.192.128, os possíveis hosts estão no intervalo de 240.128.192.129 a 240.128.192.158. Logo, os endereços estão na mesma rede.

2. Uma vez que a rede é dada por 87.42.141.136, os possíveis hosts estão no intervalo de 87.42.141.137 a 87.42.141.143. Logo, os endereços estão na mesma rede.

3. Uma vez que a rede é dada por 98.0.0.0, os possíveis hosts estão no intervalo de 98.0.0.1 a 92.63.255.254. Logo, os endereços estão na mesma rede.

11-

Rede 1: 187.1.0.0/25 -> 2^7 - 2 = 126 hosts **< 120 OK**

Rede 2: 187.2.0.0/25 -> 2^7 - 2 = 126 hosts **< 120 OK**

Rede 3: 187.3.0.0/27 -> 2^5 - 2 = 30 hosts **< 25 OK**

Rede 4: 187.4.0.0/23 -> 2^9 - 2 = 510 hosts **< 500 OK**

Rede 5: 187.5.0.0/23 -> 2^9 - 2 = 510 hosts **< 500 OK**

Rede 6: 187.6.0.0/26 -> 2^6 - 2 = 62 hosts **< 60 OK**

Rede 7: 187.7.0.0/30 -> 2^2 - 2 = 2 placas de rede **OK**

Rede 8: 187.8.0.0/30 -> 2^2 - 2 = 2 placas de rede **OK**

Rede 9: 187.9.0.0/30 -> 2^2 - 2 = 2 placas de rede **OK**

Rede 10: 187.10.0.0/30 -> 2^2 - 2 = 2 placas de rede **OK**

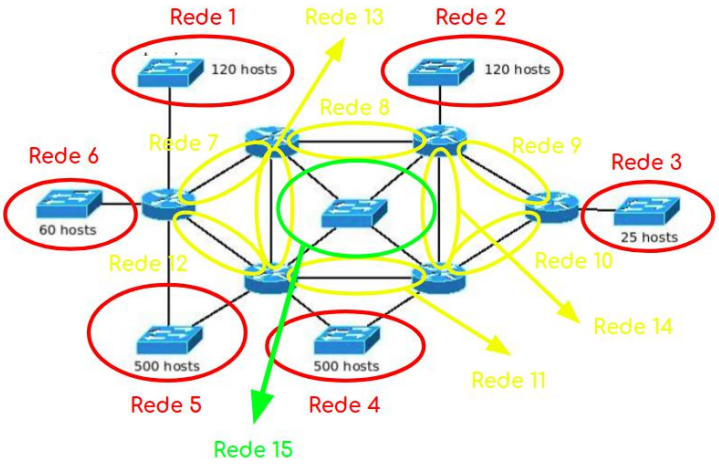
Rede 11: 187.11.0.0/30 -> 2^2 - 2 = 2 placas de rede **OK**

Rede 12: 187.12.0.0/30 -> 2^2 - 2 = 2 placas de rede **OK**

Rede 13: 187.13.0.0/30 -> 2^2 - 2 = 2 placas de rede **OK**

Rede 14: 187.14.0.0/30 -> 2^2 - 2 = 2 placas de rede **OK**

Rede 15: 187.15.0.0/29 -> 2^3 - 2 = 6 placas de rede **< 4 OK**



12-

RIP e OSPF são protocolos de roteamento intra-domínio, porém o protocolo RIP utiliza vetores de distância, além de uma tabela de roteamento, enquanto o protocolo OSPF utiliza estados de enlace, uma tabela de roteamento e uma tabela de estados de enlace. O OSPF é mais complexo, porém mais eficiente que o RIP, porque calcula a melhor rota utilizando menos mensagens. Por outro lado, o protocolo BGP é usado para roteamento inter-domínio.

13-

Vazão = tamanho da janela / latência

Tamanho da janela = 3***(64*8)** + 2*(32*8) = 2048 kbits

Vazão = 2048 kbits / (15*0,001) segundos ≃ 137 Mbits/s

14-

“Número de sequência”: número de bytes acumulados desde o envio do primeiro segmento. “Número de reconhecimento”: número de sequência do próximo byte esperado. “Tamanho da janela”: número de bytes que podem ser aceitos pelo remetente do segmento (cresce à medida que são recebidos ACKs). “URG”: indica se há urgência no ponteiro correspondente. “ACK”: indica se o campo do número de reconhecimento é válido. “PSH”: indica que deve ocorrer envio imediato para a aplicação. “RST”: “reseta” a conexão. “SYN”: indica a sincronização dos números de sequência. “FIN”: indica que foi enviado o último pacote.

15-

Os dados enviados são “repetidos” pelas respostas ACK, ou seja, após o envio de um segmento com um número de reconhecimento, a resposta corresponderá a um segmento com número de sequência igual ao número de reconhecimento recebido incrementado de uma unidade. Já o número de reconhecimento da resposta será o número de sequência recebido incrementado de uma unidade, pois indica o próximo segmento esperado.

16-

Quando um segmento é transmitido, é iniciado um contador. Caso o número de reconhecimento correspondente for recebido, esse contador é reiniciado antes de ser enviado o próximo segmento. Caso esse contador chegue a um valor máximo (timeout), serão enviados números de reconhecimento duplicados nas próximas transmissões para indicar que o segmento não foi recebido. Caso o mesmo valor seja enviado três vezes, ocorre retransmissão (apenas do segmento perdido ou de todos os segmentos a partir do segmento perdido).

17-

Quando um remetente recebe três vezes um número de sequência duplicado, conclui-se que o segmento foi perdido. Um remetente com

a poliica de “fast retransmit” retransmitirá o segmento imediatamente, sem esperar por outro timeout.

18-

O controle de congestionamento no TCP é composto por três etapas: partida lenta, prevenção de congestionamento e recuperação rápida. Inicialmente, o tamanho da janela está limitado a 1 MSS, mesmo que a largura de banda disponível seja muito maior que MSS/RTT. A taxa inicial é baixa, mas a cada “ACK” recebido, o tamanho da janela é duplicado, crescendo de forma exponencial. Caso o tamanho da janela chegue a um limiar “threshold” e já tenha ocorrido um timeout, o tamanho da janela crescerá de forma diferente no modo de prevenção de congestionamento (abordagem conservadora).

19-

A importância do comportamento serrilhado é que a largura de banda é testada aos poucos, isto é, o tamanho da janela é dinâmico, pois está em função do congestionamento detectado na rede. Dessa forma, são evitadas perdas logo no início da transmissão e a transmissão não é completamente interrompida em caso de congestionamento na rede. Também, essa política garante justiça na alocação de banda.

21-

Um sistema autônomo é uma unidade que contém redes e roteadores sob mesma administração, conectados à Internet através de um ponto comum (backbone). Internamente, os roteadores se comunicam através de um protocolo interno (IGP), como RIP e OSPF, por exemplo, definindo rotas internas. Para a comunicação com outros sistemas autônomos, é utilizado um protocolo EGP.

22-

Formato da mensagem: IP destino | MAC destino | IP origem | MAC origem

Requisição: IP B | 111...1 | IP A | MAC A (a requisição ARP ocorre em broadcast)

Resposta: IP A | MAC A | IP B | MAC B

23-

Algoritmo que organiza o compartilhamento de um canal em redes Ethernet, definindo que a transmissão deve ocorrer quando o meio estiver disponível. Assim, previne, detecta e trata das situações em que duas estações disputam o acesso ao meio simultaneamente.

24-

O envio de pacotes na rede percorre camadas de abstração, nas quais o pacote é analisado segundo um protocolo específico. Por isso, as informações de cada protocolo necessárias são encapsuladas antes de o pacote passar pela rede. À medida que o pacote percorre as camadas de rede, ele recebe ou “perde” cabeçalhos e outras informações.

25-

Estabelece regras de comunicação e formato de mensagens entre entidades na rede. Pode cumprir requisitos como comunicação confiável, sem falhas, com qualidade e segura. Quanto mais requisitos são previstos pelo protocolo, maior é a sua complexidade.