Questions/réponses sur la fragmentation IP

Dans cet article, vous allez découvrir les 23 questions avec réponses sur la fragmentation des datagrammes IP. Avant de commencer ce questionnaire, on vous recommandons de jeter un coup d'œil sur l'article suivant :

Structure de datagramme IPLe terme « datagramme » ou « paquet » est utilisé pour décrire un bloc de données IP. Chaque datagramme IP contient un ensemble spécifique de champs dans un…Lire plus

1. Que signifie la fragmentation IP?

Réponse

La fragmentation d'un datagramme IP en deux ou plusieurs datagrammes IP de taille plus petite est appelée une fragmentation IP

2. Quand se produit la fragmentation IP?

Réponse

La fragmentation se produit lorsqu'un datagramme IP traverse un réseau dont l'unité de transmission maximale (MTU) est inférieure à la taille du datagramme. Prenons par exemple un datagramme Ethernet standard de 1500 octets. Si un datagramme de plus grande taille devait traverser un réseau Ethernet, il faudrait une fragmentation pour empêcher sa suppression quelque part sur le réseau. Les fragments poursuivre jusqu'à leur destination, où l'hôte récepteur les rassemble dans le datagramme d'origine.

3. Pourquoi un datagramme IP est-il fragmenté?

Réponse

Chaque support de transmission limite la taille maximale d'une trame (MTU) qu'il peut transmettre. Comme les datagrammes IP sont encapsulés dans des trames, la taille du datagramme IP est également limitée. Si la taille d'un datagramme IP est supérieure à cette limite, il doit être fragmenté.

4. Quelles RFC traitent la fragmentation IP?

Réponse

Les RFC 791 et RFC 815 traitent les datagrammes IP, la fragmentation et le réassemblage.

A quoi servent les RFC ?Un RFC (Request for Comments) est un document purement technique publié par l'IETF (Internet Engineering Task Force). Les RFC sont principalement utilisées pour développer un…Lire plus

5. Est-il possible de sélectionner une taille de datagramme IP pour toujours éviter la fragmentation?

Réponse

Il n'est pas possible de sélectionner une taille particulière d'un datagramme IP pour éviter toujours la fragmentation, selon le MTU. Il est toutefois possible, pour un chemin donné, de choisir une taille qui ne mène pas à la fragmentation. Cette opération s'appelle Path MTU Discovery (PMTUd) et est décrite dans la RFC 1191 qui permet de déterminer, la taille du MTU sur le chemin entre deux hôtes IP, afin d'éviter la fragmentation des paquets. Le protocole de transport TCP tente d'éviter la fragmentation à l'aide de l'option MSS (Maximum Segment Size).

6. Où un datagramme IP peut-il être fragmenté?

Réponse

Un datagramme IP peut être fragmenté sur l'hôte émetteur ou sur l'un des routeurs intermédiaires.

7. Où les fragments de datagramme IP sont-ils réassemblés?

Réponse

Les fragments IP sont réassemblés uniquement sur l’hôte de destination.

8. Comment empêcher un datagramme IP d’être fragmenté?

Réponse

La fragmentation d’un datagramme IP peut être empêchée en activant l’indicateur DF (Don’t Fragment) dans l’en-tête IP.

9. Que se passe-t-il lorsqu’un datagramme doit être fragmenté pour traverser un réseau, mais que l’indicateur DF (Don’t Fragment) dans le datagramme est défini?

Réponse

Le datagramme dont l’indicateur DF (Don’t Fragment) est défini, le datagramme est supprimé s’il doit être fragmenté pour traverser un réseau. De plus, un message d’erreur ICMP est renvoyé à l’expéditeur du datagramme.

10. Est-ce que tous les fragments d’un datagramme atteindront la destination en empruntant le même chemin?

Réponse

Les différents fragments du même datagramme IP peuvent emprunter le même ou différents chemins vers la destination.

11. Est-ce que tous les fragments d’un datagramme arriveront au système de destination dans le bon ordre?

Réponse

Les différents fragments d’un même datagramme IP peuvent arriver dans n’importe quel ordre au système de destination.

12. Qu’est-ce qui arrive au datagramme d’origine lorsqu’un ou plusieurs fragments sont perdus?

Réponse

Lorsqu’un ou plusieurs fragments d’un datagramme IP sont perdus, tout le datagramme IP est supprimé après un délai d’attente.

13. Quelle est la taille minimale d’un fragment IP?

Réponse

La taille minimale d’un fragment IP est la taille minimale d’un en-tête IP plus huit octets de données. La plupart des périphériques de type pare-feu suppriment le fragment IP initial (offset 0) qui ne contient pas assez de données pour contenir les en-têtes de transport. En d’autres termes, le fragment IP nécessite normalement 20 octets de données en plus de l’en-tête IP afin de traverser un pare-feu si l’offset est égal à 0.

14. Quelles sont les limitations sur la taille d’un fragment?

Réponse

La taille d’un fragment de datagramme IP est limitée par :

- **La quantité de données restantes dans le datagramme d’origine**
- **Le MTU du réseau**
- **Doit être un multiple de 8, sauf le dernier fragment.**

QCM sur l’en-tête IP et la fragmentation IPQCM en réseau informatique avec la correction pour la préparation des concours, des tests, aux examens et aux certifications. Cette partie de (QCM) est basé…Lire plus

15. Comment différencie-t-on un fragment de datagramme IP d’un datagramme IP non fragmenté?

Réponse

Un datagramme IP complet est différencié d’un fragment IP à l’aide du champ offset et l’indicateur MF (More Fragments). Pour un datagramme IP non fragmenté, l’offset de fragment sera nul et l’indicateur MF (More Fragments) sera mis à zéro.

16. Comment les fragments d’un seul datagramme IP sont-ils identifiés?

Réponse

Le champ « Identificateur » dans l’en-tête IP est utilisé pour identifier les fragments d’un datagramme IP unique. La valeur de ce champ est définie par le système d’origine. Il est unique pour la source et la destination tant que le datagramme est actif.

17. Comment le dernier fragment d’un datagramme IP est-il identifié?

Réponse

Le dernier fragment d’un datagramme IP est identifié à l’aide de l’indicateur « More Fragments » (MF). L’indicateur « More Fragment » (MF) est défini sur zéro pour le dernier fragment.

18. Comment la longueur totale du datagramme IP est-elle calculée à partir des fragments IP reçus?

Réponse

En utilisant le champ offset du fragment et la longueur du dernier fragment, la longueur totale du datagramme IP est calculée.

19. Comment un datagramme IP est-il fragmenté?

Réponse

Dans l’exemple suivant, un datagramme IP est fragmenté en deux fragments. Ce même algorithme peut être utilisé pour fragmenter le datagramme en « n » fragments.

- **La couche IP crée deux nouveaux datagrammes IP, dont la longueur répond aux exigences du réseau dans lequel le datagramme d’origine va être envoyé.**
- **L’en-tête IP du datagramme IP d’origine est copié dans les deux nouveaux datagrammes.**
- **Les données du datagramme IP d’origine sont divisées en deux sur une limite de 8 octets. Le nombre de blocs de 8 octets dans la première partie est appelé « Number of Fragment Blocks » (NFB) ou Nombre de blocs de fragments.**
- **La première partie des données est placée dans le premier nouveau datagramme IP.**
- **Le champ de longueur du premier nouveau datagramme IP est défini sur la longueur du premier datagramme.**
- **Le champ de décalage de fragment(Offset) dans le premier datagramme IP est défini sur la valeur de ce champ dans le datagramme d’origine.**
- **Le champ « more fragments » (MF) du premier datagramme IP est défini sur un.**
- **La deuxième partie des données est placée dans le deuxième nouveau datagramme IP.**
- **Le champ de longueur du deuxième nouveau datagramme IP est défini sur la longueur du deuxième datagramme.**
- **Le champ « More Fragments » (MF) du deuxième datagramme IP est défini sur la même valeur que le datagramme IP d’origine.**
- **Le champ de décalage de fragment(Offset) dans le deuxième datagramme IP est défini sur la valeur de ce champ dans le datagramme d’origine plus**

NFB.

Exercices corrigés adressage IP – Partie 1La meilleur façon pour apprendre à utiliser les sous-réseaux est de pratiquer des exercices comme ceci. Voici certaines questions que vous pouvez avoir dans des…Lire plus

20. Comment un système de destination réassemble les fragments d'un datagramme IP?

Réponse

- **Lorsqu'un hôte reçoit un fragment IP, il le stocke dans un buffer de réassemblage basé sur son champ de décalage de fragment(offset).**
- **Une fois que tous les fragments du datagramme IP d'origine sont reçus, le datagramme est traité.**
- **À la réception du premier fragment, un compteur ou « timer » de réassemblage est lancée.**
- **Si le timer de réassemblage expire avant la réception de tous les fragments, le datagramme est supprimé.**

21. Quels champs sont modifiés dans un en-tête IP en raison de la fragmentation?

Réponse

Les champs d'en-tête IP suivants sont modifiés en raison de la fragmentation IP:

- **Longueur totale**
- **Longueur d'en-tête (IHL)**
- **Flag « More Fragments »**
- **Position du fragment (Offset)**

- **Checksum de l’entête**
- **Options**

22. Qu’est-ce qui arrive au champ d’options IP lorsqu’un datagramme IP est fragmenté?

Réponse

Selon l’option choisie, elle est copiée dans tous les fragments ou uniquement dans le premier fragment.

23. Quelles options IP sont copiées sur tous les fragments d’un datagramme IP?

Réponse

Si le bit le plus significatif dans le type d’option est défini (c’est-à-dire la valeur un), cette option est alors copiée dans tous les fragments. S’il n’est pas défini (c’est-à-dire, la valeur zéro), il est copié uniquement dans le premier fragment.

- QCM Réseau – Partie 1
- QCM Réseau – Partie 2
- QCM Réseau – Partie 3
- QCM Réseau – Partie 4
- QCM Réseau – Partie 5
- QCM Réseau – Partie 6
- QCM Réseau – Partie 7
- QCM Réseau – Partie 8
- QCM Réseau – Partie 9
- QCM Réseau – Partie 10
- QCM Réseau – DNS – Partie 1
- QCM Réseau – DNS – Partie 2
- QCM Réseau – DNS – Partie 3
- QCM Réseau – DNS – Partie 4
- QCM Réseau Informatique – Couche physique – Partie 1
- QCM Réseau Informatique – Couche physique – Partie 2
- Questions/réponses sur la fragmentation IP
- QCM sur l’en-tête IP et la fragmentation IP

- Perte de paquets
- Comment utiliser la commande Ping sous Windows
- La commande IPConfig – Windows
- Protocole UDP
- Protocole TCP
- Protocole IMAP
- Protocole POP
- Protocole SMTP
- Protocole HTTP
- Protocole FTP
- Protocole ICMP
- Protocole ARP
- VLSM – Réseau
- Les modes de transmission
- Techniques de détection d'erreur
- Les 7 couches du modèle OSI
- Fragmentation ipv4
- Structure de datagramme IP
- Encapsulation et décapsulation TCP/IP
- Les normes IEEE 802
- La technologie FDDI (Fiber Distributed Data Interface)
- Différents types de câblage informatique
- NIC – Carte réseau – Informatique
- Qu'est ce qu'un répéteur ?
- Qu'est ce qu'un Hub (concentrateur) ?
- Qu'est ce qu'un pont réseau (Bridge) ?
- Qu'est ce qu'un commutateur réseau (Switch) ?
- Qu'est ce qu'un routeur ?
- L'adressage CIDR
- Topologie du Réseau Informatique
- Topologie réseau en étoile
- Topologie de réseau maillée
- Topologie réseau en anneau
- Topologie réseau en bus
- A quoi servent les RFC ?
- Classe d'adresse IP
- Adresse de diffusion
- Les avantages de IPv6
- Liste des protocoles internet
- Zone DNS
- Différence entre CSMA/CA et CSMA/CD
- Configurer une adresse ip en ligne de commande sous Linux
- 9 Commandes avec ip pour configurer l'interface réseau sous Linux
- Renommer l'interface par défaut ens33 à l'ancienne eth0 sur Ubuntu 16.04
- 15 Commandes avec ifconfig pour configurer l'interface réseau sous Linux
- 7 exemples avec la commande Dig pour interroger DNS
- 11 exemples avec la commande Tcpdump pour débugger son réseau
- 10 commandes indispensables pour l'administration réseau sous Linux
- 15 commandes Netstat pour la gestion de réseau sous Linux
- Exercices corrigés adressage IP – Partie 1
- Exercices corrigés adressage IP – Partie 2

- Exercices corrigés adressage IP – Partie 3
- Comment installer Cisco Packet Tracer 7.0 sur Windows 7,8,10 – 32/64 bits
- Table de routage
- Adresse Mac
- Adresse IP
- Calculer des sous réseaux, le nombres d'hôtes, la plage d'adresses IP et le Broadcast
- Différence entre CCNA et CCNP
- Différences entre circuits virtuels et datagrammes
- Différence entre intranet et extranet
- Différence entre vlan statique et dynamique
- Différence entre internet et ethernet
- Différence entre socket client et socket serveur
- Différence entre POP et POP3
- Différence entre les câbles Cat6 et Cat5E
- Différence entre Hub et Switch
- Différence entre HTTP et WWW
- Différence entre OSPF et BGP
- Différence entre IGRP et EIGRP
- Différence entre SIP et VoIP
- Différence entre Ripv1 et Ripv2
- Différence entre ip publique et privée
- Différence entre LAN et VLAN
- Différence entre Fast ethernet et Gigabit ethernet
- Différence entre SAN et NAS
- Différence entre la topologie en étoile et en anneau
- Différence entre Fibre optique et Cable coaxial
- Différence entre Répéteur et Amplificateur
- Différence entre adresse ip statique et dynamique
- Différence entre routage statique et dynamique
- Différence entre NAT et PAT
- Différence entre DNS et DHCP
- Différence entre BOOTP et DHCP
- Différence entre la compression avec perte et la compression sans perte
- Différence entre FTP et SFTP
- Différence entre le débit binaire et le débit en bauds
- Différence entre le Pont(Bridge) et le Commutateur(Switch)
- Différence entre Broadcast et Multicast
- Différence entre mode connecté et non connecté
- Différence entre les réseaux client-serveur et peer-to-peer
- Différence entre SMTP et POP3
- Différence entre une Trame et un Paquet
- Différence entre Pont et Routeur
- Différence entre UTP et STP
- Différence entre Cc et Cci
- Différence entre HTTP et FTP
- Différence entre modem et routeur
- Différence entre la commutation de circuit et commutation de paquets
- Différence entre un switch et un routeur
- Différence entre l'adresse MAC et l'adresse IP

- Différence entre unicast et multicast
- Différence entre un Pont et une Passerelle – Réseau informatique
- Différence entre le modèle TCP / IP et le modèle OSI
- Différence entre LAN, MAN et WAN
- Différence entre Internet et Intranet
- Différence entre SLIP et PPP
- Différence entre FTP et TFTP
- Différence entre HTTP et HTTPS
- Différence entre les protocoles TCP et UDP
- Différence entre POP et IMAP
- Différence entre LDAP et Active Directory
- Différence entre les en-têtes IPv4 et IPv6
- Différence entre ARP et RARP
- Différence entre SNMP v2 et v3
- Différence entre SNMP v1 et v2
- Différence entre les protocoles à état de liens et vecteur de distance
- Différence entre SSH et Telnet
- Différence entre EIGRP et OSPF
- Différence entre RIP et OSPF
- Différence entre MAP et Diameter
- Différence entre IBGP et EBGP
- Différence entre TCP et IP
- Différence entre FTP mode passif et actif

QCMs qui pourraient vous intéresser :

- Questions techniques sur MYSQL
- QCM MySQL Corrigé – Optimisation de requêtes
- QCM Base de données avec correction
- QCM sur PHP
- QCM Symfony
- QCM AngularJS
- QCM React
- QCM HTML / CSS
- QCM Java – Programmation Orientée Objet
- QCM Python
- QCM Cloud Computing
- QCM Framework Spring
- QCM Javascript
- QCM jQuery
- QCM Oracle
- QCM sur GIT – Gestionnaire de version
- QCM Linux – Gestion de processus
- QCM Réseau
- QCM Architecture des ordinateurs
- QCM Securité informatique
- QCM En Informatique Générale
- QCM en C
- QCM en C#
- QCM sur l'algorithmique
- QCM Word

- QCM Excel
- QCM PowerPoint
- QCM Access