1. How much traffic in bytes in total was received and transmitted in your request for the Unimelb web page? What is the percentage of traffic that originated from your computer, and what is the percentage of traffic that was sent by the remote host? ANSWER: The amount of traffic captured will depend on the network conditions, whether some packets were lost and needed to be retransmitted, whether some background network traffic was also captured, etc.
2. How do these sizes compare with the file size of the web page you downloaded? Estimate the download protocol overhead, or percentage of the download bytes taken up by protocol overhead. ANSWER: Again results may vary, but the overhead (for our purposes, which includes the headers from each of the packets and also the traffic involved with establishing and ending the connection) can be obtained by dividing the total traffic in bytes received from the previous question, by the file size of the retrieved HTML file (which is 44,220 bytes when I tried).
3. What are the protocol overheads used for? Why are they useful? Aren’t they a waste of space? ANSWER: The overheads/headers are used to allow each layer in the networking architecture perform their particular service. For example, the networking layer headers will have the source IP and destination IP addresses for that packet, which tells the intermediate hosts where the final destination of the packet is intended to be. These headers are part of how data is transferred between the networking layers, what we call ”encapsulation”, and keeps networking functions separate and modular between the layers. Arguably, the size of the information contained in the headers can be reduced by having a ”monolithic” architecture to networking, where there is only one ”layer”, but then modularity and abstraction are sacrificed, which is bad from an engineering perspective.
4. Are you able to identify other packets apart from the HTTP GET request and response packets in your capture? What might these packets be used for? ANSWER: Apart from HTTP GET and HTTP 200 OK request and response packets, other packets of interest include the SYN and SYN ACK packets at the beginning which establishes a reliable connection between two hosts (more on that when we get to TCP), and also the packets at the end when the connection is closed. The packets in the middle are the data that make up the rest of the actual web page. Because the web page is quite large, the data will be split and transferred with multiple packets. It can also be observed that between every two or three packets that are received, our computer sends an ACK or acknowledgement packet to communicate to the remote host that the packets sent were successfully received. If the remote host fails to receive these packets, then it can be assumed that they were lost in transmission and need to be resent.
5. How does do the protocol overheads relate to the networking layering architecture you have seen (or will see) in class? Is this architecture efficient? What are the advantages of this ‘layered-cake’ architecture? What are the disadvantages? ANSWER: a non-layered architecture may be more efficient, but at the cost of flexibility and modularity. Other disadvantages include a sizable overhead if the information to be transferred needs to be split across many packets. However, the advantages of modularity and abstraction (also in engineering overall) outweigh the disadvantages. Advantages include, but aren’t limited to, information hiding (i.e. if you were a network engineer, you would not need to know detailed information on the physical layer to work on improvements to another layer), and flexibility (the ability to change protocols in a certain layer, without affecting the operation of other layers).
6. Calculate the inter-arrival times (IAT) of the packets, i.e. the time between each packet arrival. Plot the number of packets against the IAT. What sort of distribution do you observe? You may need to capture many more HTTP packets (this time using a web browser, for example) for a proper distribution to be seen. ANSWER: You should observe an exponential distribution.
7. Describe the key OSI layer division principles. ANSWER: A layer should be created where a different abstraction is needed. Each layer should perform a well-defined function. The function of each layer should be chosen with a view toward defining internationally standardised protocols. The layer boundaries should be chosen to minimise the information flow across the interfaces. The number of layers should be large enough that distinct functions need not to be thrown together in the same layer out of necessity, and small enough that the architecture does not become unwieldy.
8. Give three key characteristics that affect the performance of applications on networks. ANSWER: Bandwidth; Latency; Jitter Give an example of application that has stringent requirements on each of the three main characteristics you have given above ANSWER: Bandwidth - HD video; Latency - Interactive gaming; Jitter - Real-time video
9. Briefly explain key relative advantages and disadvantages of using Fibre Optics versus Copper Wire. ANSWER: Fibre is efficient to run over longer distances, higher bandwidth, low noise, however it is expensive, requires specialists to deploy, is difficult to tape, is fragile. Copper is cheaper, lower bandwidth, no specialist skill required, more receptive to noise.
10. The transmission media used in the physical layer can be wired or wireless. Compare satellite with wired medium coaxial cable, and list both the advantages and disadvantages of these two media using bullet points. ANSWER:

Satellite: +1.can rapidly set up anywhere/anytime communications(after satellites have been launched);+2.can broadcast to large regions;-3.limited bandwidth and interface to manage.-4expansive to deploy

Cable: +1.easy to engineer a fixed data rate over point-to-point links.+2.does not readily support mobility or broadcast. 3.higher speed over greater distances

1. Satellite VS Fiber: ANSWER:

Satellite: +1.can rapidly set up anywhere/anytime communications(after satellites have been launched);+2.can broadcast to large regions;-3.limited bandwidth and interface to manage

Fiber: +1.enormous bandwidth over long distance.-2.installation can be more expensive/difficult

1. Week8-lecture1\_\_\_ TCP Segment Header
2. Briefly explain the difference in operation and philosophy of two approaches to error handling on the data link layer ; error-correcting and error-detecting. ANSWER: Include enough information in frames to allow reconstruction/deduction of original content (error-correcting). Include enough redundancy to allow receiver to determine an error occurred and request retransmission (error-detecting).
3. Data link protocols almost always put the CRC in a trailer rather than in a header. Why do we want to do this? ANSWER: The CRC is computed during transmission and appended to the output stream as soon as the last bit goes out onto the wire. If the CRC were in the header, it would be necessary to make a pass over the frame to compute the CRC before transmitting. This would require each byte to be handled twice. Using the trailer cuts the work in half.
4. If a LAN is under high load, would it be more efficient to use a contention protocol or a collision free protocol in the MAC Sub-layer? ANSWER: Under high load a contention protocol would cause many collisions and not be effective, where a collision free protocol allows each source to use the network in turn. Therefore, a collision free protocol should be used.
5. Consider a client program that needs to run the following operations on a remote file server:
   1. List the contents of a directory b. Open a file c. Read a text file d. Display the attributes of a file For each of the above operations, indicate whether they are more likely to be delay sensitive or bandwidth sensitive. Justify your answer? ANSWER: a. Delay-sensitive; directories are typically of modest size. b. Delay-sensitive; the messages exchanged are short. c. Bandwidth-sensitive, particularly for large files. d. Delay-sensitive; a file’s attributes are typically much smaller than the file itself.
6. Give the name of one sliding window protocols and briefly explain how that protocol works at Data Link Layer using an example figure where a transmission error occurs. ANSWER: Selective Repeat
7. With respect to routing packets in the Network Layer, explain the difference between a connectionless and connection-oriented service? ANSWER: Connectionless: packets are injected into the network individually and routed independently of each other. No advance setup is needed Connection-oriented: If connection-oriented service is used, a path from the source router all the way to the destination router must be established before any data packets can be sent. This connection is called a VC (virtual circuit).
8. Explain the purpose of subnetting. ANSWER: Subnetting allows networks to be split into several parts for internal uses whilst acting like a single network for external use.
9. Give an example for policy choice at the Transport layer that can affect network congestion. ANSWER: E.g. Flow control policy - small congestion windows reduce the data rate and avoid congestion.
10. a. A common approach to removing jitter in streaming audio is to buffer incoming packets at the receiver. Briefly explain a key problem using this approach for video conferencing. ANSWER: Videoconferencing is a 2-way interactive service. Buffering introduces delay into the service, which is a nuisance for interactive services.
11. Briefly explain what do we need low water mark and high water mark in media player buffer management? ANSWER: Low water mark: Safety margin, to avoid a stall. When this threshold is reached, media player requests media server to resume data transmission. High water mark: Can pause server (or go ahead and save to disk). When this threshold is reached, media player requests media server to stop data transmission temporarily to avoid buffer overflow.
12. 图示, 工程绘图

    描述已自动生成
13. Name two services that DNS provides ANSWER: 1.Hostname to IP address translation 2.Load Balancing
14. Is a DNS server a client, a server, or both? Briefly justify your answer. ANSWER: Both, since it can act as a server if the requested domain name is in its database, or as a client if it needs to ask another server to resolve the name.
15. An encrypted file needs to be accessed in non-sequential order. Which cipher mode is best suited to encrypting this file, and briefly explain why. ANSWER: Counter mode is the best option, since each block can be encrypted or decrypted based on its location in the files using a counter. Other techniques required decryption of all preceding blocks in the file. Give at least three key properties of a message digest. ANSWER: easy to compute MD(P) given P; impractical to compute P given MD(P);given P, impractical to find P' such that MD(P') = MD(P);also, a single bit change in P creates a very different message digest
16. Briefly explain Dijkstra’s algorithm in computing the set of optimal routes to all destinations from a given source. ANSWER:Dijkstra's algorithm can be use to compute a sink tree on the graph. Each link is assigned a non-negative weight/distance;Shortest path is the one with lowest total weight from the source to a destination (Using weights of 1 gives paths with fewest hops)

Algorithm: Start with the source, set distance at other nodes to infinity Relax distance to other nodes;Pick the lowest distance node, add it to sink tree;Repeat until all nodes are in the sink tree

1. 图示, 表格

   描述已自动生成Suppose the algorithms used to implement the operations at layer k is changed, how does it impact the operations at layers k - 1 and k + 1?

ANSWER: Both layer k-1 and k+1 will not be affected by layer k in this case, because changing the algorithm is just modifying how the service is implemented, but not changing the service itself. Hence, layer k-1 and k+1 are not affected. Suppose there is a change in the service provided by layer k, how does it impact operations at layers k – 1 and k + 1? ANSWER: If the service at layer k has a change, it means service provided by layer k will have an impact on layer k+1. Since the definition of service tells us service provides set of primitives only to the upper layer, there is no impact on the operations at layer k-1.

1. At Transport layer we use segments to send data across. Argue for using larger segments by discussing briefly why larger segments could be beneficial. Then also argue why using small segments may be beneficial. ANSWER: Segmentation is the process that chops data stream into several consecutive smaller segments, which is then encapsulated into IP packets. For different size of segments the transport layer choose will have a significant impact on efficiency and reliability of transmission. For larger segments, the benefits lie in two aspects. One is to save resources on both source and destination hosts to segment larger segments into small pieces, and then reassembly them together. On the other hand, we do not take too much the ordering of the different segments into consideration, because of relatively smaller number of segments to be reordered to guarantee reliability. In terms of packet loss that needs retransmission, it is the smaller segments that has a distinctive advantage. Compared with the larger segment, which needs to retransmit the entire large segment, segment with the smaller size cost less to maintain stability and reliability of transmission. Besides, small-sized segments can reduce the pressure of network layer, because network layer do not need to further segment those packets.
2. Suppose an end-to-end network connection is using the TCP protocol on ethernet service. What is the maximum data size from an application that can be transmitted in one TCP segment, including overheads from TCP and IPv4 but excluding the overhead(s) imposed by the data link layer? How will your answer change if the transport layer protocol is UDP instead of TCP? ANSWER: The maximum data size is 1,500 bytes (20 bytes IPv4 header + 20 bytes TCP header + 1,460 TCP payload from application) when using the TCP protocol on ethernet.If the transport layer protocol is UDP, my answer will still be 1,500 bytes. (20 bytes IPv4 header + 8 bytes UDP header + 1472 bytes UDP payload from application)
3. Congestion and buffer windows are used at sender and receiver ends to avoid network issues in TCP transport protocol. Describe: 1) What are the roles of these windows on sender and receiver sides? ANSWER: On the sender side, congestion window is for congestion control, to reduce sender’s transmission rate when network congestion happens. The size of congestion window (cwnd) is the number of bytes the sender could have in the network at any time, which is based on the network capacity.On the receiver side, the buffer window (or rwnd) is for flow control, to inform sender of the remaining buffer size. It specifies the number of bytes that the receiver can buffer, which shows the receiver capacity.Both windows are tracked in parallel, and the maximum transmission rate is the smaller of the two windows. 2)What are the implications of using large vs. small window sizes on sender and receiver sides? If congestion window is set too large, it could be beyond the current network capacity and then congestion could happen within the network; if congestion window is too small then it could waste (not fully use) the network capacity or bandwidth. If receiver window is set too large, then buffer overflow could happen and the receiver might have to discard some data; if receiver window is too small, it could waste (not fully use) the receiver’s buffer capacity.
4. Cookies vs sessions:

Answer: Sessions:1.(positions)sessions information regarding visitor’s interaction stored at the server side :up to some hours.2.(lifetime)When user closes the website ,the session ends.3.(size):sessions information size can be large. Cookies : 1.(positions) scookies are transferred between server and client ,cookie information stored at both client and server.2.(lifetime)maintain client information until deleted 3.(size):cookies information size limited

1. DNS：Answer:iterated query( done by local DNS server)1.Root DNS server Query2.TLD DNS server Query 3.authoritative DNS server
2. What does iterative mode of execution when querying a DNS mean? Where is it used? What is the recursive mode? Please explain with an example. Ans. Iterative queries are requests that are propagated from one name server to another, gathering partial results in the form of which name server might know the location of the authoritative record till we reach that location. At which point, we return the final answer (Resource record mapping) to our end user who requested the domain initially, this is referred to as recursive, where we return the final answer only to the end user and not partial answers. Recursive queries are when a local PC/device delegates to local server the DNS query to recursively follow-up the query with other servers in the DNS system.
3. Reduced overhead: Persistent HTTP connections allow multiple requests and responses to be sent over a single connection. This eliminates the need to establish and tear down a new connection for each resource (e.g., images) on the web page. As a result, the client can avoid the overhead associated with establishing and maintaining multiple connections, resulting in faster and more efficient communication.
4. Faster page load times: With a persistent connection, subsequent requests for resources (such as images) can be sent immediately after the initial request without waiting for connection setup. This enables parallel downloading of multiple resources, leading to faster overall page load times. The client can start rendering the web page and displaying its content incrementally as each resource is received, providing a better user experience.
5. Better resource utilization: Persistent connections allow the server to reuse the same connection for multiple requests from the same client. This reduces the server's overhead in establishing new connections for each resource request and can result in better resource utilization on the server side, especially when handling multiple simultaneous client requests.
6. Connection latency: Establishing a new connection for each resource can introduce additional latency, particularly if the client and server are geographically distant. By using a persistent connection, the client can avoid the overhead of repeated connection establishment, reducing the latency between making the initial request and receiving subsequent resources.
7. HTTP/2 and pipelining benefits: Persistent connections align well with the features offered by newer HTTP versions like HTTP/2. HTTP/2 supports multiplexing, allowing multiple resources to be requested and received concurrently over a single connection. Additionally, HTTP/2 supports request prioritization, enabling the client to prioritize critical resources for faster delivery. These features further enhance the benefits of using a persistent connection.
8. Persistent VS non-persistent Answer:1. Reduce Latency: For each new TCP connection, there is a need for a three-way handshake to establish the connection, which can introduce additional latency. A persistent connection avoids this overhead, as multiple requests can be sent over a single established connection.2. Less Resource-Intensive: Each new TCP connection requires resources on both the client and server to track and manage the connection. With many connections, this can add up to significant overhead. Using a single, persistent connection reduces this resource usage.3. Improved Network Utilization: In TCP, the slow-start mechanism increases the data transmission rate over time to prevent network congestion. Each new connection must go through this slow-start phase, whereas a persistent connection can continue sending larger amounts of data more quickly.4. HTTP Pipelining: Persistent connections also allow the use of HTTP pipelining, where multiple HTTP requests can be sent on a single TCP connection without waiting for the corresponding responses. This can improve page load times.
9. Identify 2 ways in which the OSI reference model and the TCP/IP reference model are the same,and 2 different ways.

Similarities:1.stacking of layered protocols.2.similar functionality in each of the layers.3.layers above transport layer relate to applicationsDifferences:1. TCP/IP does not distinguish between services, interfaces and protocols.2.TCP/IP does not clearly separate physical and data link functions

1. Is an oil pipe a simplex system, a half-duplex system, a full duplex system or none of the above? Under which conditions?Answer：Oil can flow in either direction, but not both ways at once, therefore it cannot be full duplex.Depending on the situation, at an oil refinery, for example, an oil pipe is simplex, as the oil only flows in one direction.Theoretically oil can flow both ways, therefore it can be consider half duplex,similar to a single railroad track.
2. List two solutions that one can use for sharing a link between multiple senders and explain these solutions briefly. Answer：Time division multiplexing(Users can send according to a fixed schedule, Slotted access to the full speed of the media) and frequency division multiplexing(Users can only use specific frequencies to send their data)
3. Is the Sampling theorem true for optical fibre or only for copper wire? Answer：The Sampling theorem is a property of mathematics and has nothing to do with technology. The Sampling theorem is independent of the transmission medium. The Sampling theorem states that if you have a function which does not contain any frequency components (sines or cosines) above f, then by sampling at a frequency of 2f, you capture all the information there is.
4. Given a noiseless 4 kHz channel, what is the maximum data rate of the communication channel? Answer：A noiseless channel can carry an arbitrarily large amount of information, e.g. there can be an infinite number of signalling levels, this is because there is no noise. This is a neat observation and the level information is not restricted by the question in any way. Shannon specifies a limit on the information rate based on given noise level.
5. The bandwidth of a television video stream is 6 MHz.How many bits/sec are sent if four-level digital signals are used? Assume a noiseless channel. Answer：  
   The maximum baud rate is 12 M symbols/sec Four levels of signalling provide: log2 4 = 2 bits/symbol.Hence, the total data rate is: 12 M symbols/sec × 2 bits/symbol = 24 Mbps
6. Why would anyone like to use the Go-Back-N protocol if we already introduced a superior protocol that can repeat only the missing frames, i.e., the Selective Repeat protocol?Answer:This is a standard case of speed vs memory in computing. Yes, Selective Repeat would be fast in recovering frames as the receiver does not throw away frames that come out of sequence but this comes with the cost that the receiver now has to have a larger than single frame size as its buffer, i.e. more memory needed**.**
7. To compare the Delay of pure ALOHA vs slotted ALOHA: Answer With slotted ALOHA, it has to wait for the next slot. On average this introduces half a slot time of delay. With pure ALOHA, transmission can start instantly. At low load with minimal collisions, pure ALOHA will have less delay. However, at higher loads, there is more probability for collisions in pure ALOHA compared to slotted ALOHA. This is because frames can collide in midway. By enforcing synchronisation, slotted ALOHA is able to achieve much greater efficiency.
8. For medium access control one can use dynamic allocation of channels in comparison to static allocation. Dynamic allocation is far more adaptive. Thus, why would anyone use static allocation mechanisms? Answer: Static allocation is still useful when the number of senders are known and fairly stable. In such a case, one does not need to deal with collision resolution etc through complex algorithms. Especially if all senders are in need of the channel regularly, why would we bother trying to allocate channels dynamically. A good example is FM radio where all channels are regularly used and fairly stable in terms of number of them and a fair static allocation would suffice.
9. Benefit and disadvantage for fragmentation:AnswerGood design paradigm and encapsulation of fragmentation within each network. Transparent fragmentation is straightforward to implement and use but has problems. For one thing, the exit router must know when it has received all the pieces, so either a count field or an ‘‘end of packet’’ bit must be provided. Also, because all packets must exit via the same router so that they can be reassembled, the routes are constrained. By not allowing some fragments to follow one route to the ultimate destination and other fragments a disjoint route, some performance may be lost. More significant is the amount of work that the router may have to do. It may need to buffer the fragments as they arrive, and decide when to throw them away if not all of the fragments arrive. Some of this work may be wasteful, too, as the packet may pass through a series of small packet networks and need to be repeatedly fragmented and reassembled.
10. 4 key aspects for security: Answer: 1.Secrecy: keeping information hidden from a general audience, i.e., except the intended party 2.Authentication: Ensuring the user you are giving the content to has the valid id/credentials 3.Non-repudiation: Proving that the content belongs to/send by a named sender 4.Integrity control: Ensuring the content is not tampered with, e.g., during transport
11. Leveraging the authentication protocol using Public-Key cryptography, we send across two additional numbers, RA and RB. Why are these needed? Why not Alice sends only her name to Bob but needs a RA as well?  
    Ans. Without RA Bob can still send back an acknowledgement but Alice cannot be sure that whether the responding person is Bob or not. The RA is needed to prove that Bob opened the initial message with his private key, saw RA, and in the response message sends it to Alice to prove this. Same is true for the role of RB.
12. 单点DNS的缺陷：Ans.：1.Single point of failure.2.Traffic congestion at server.3.Distant centralised server for remote queries. 4.Maintenance issues, not only for keeping large amount of data up to date but also the prospect of simple service maintenance could cause big disruptions. 5.May not be able to service all queries fast enough, also scaling on the computation front may be an issue.
13. What are the two missing layers of the OSI protocol that we did not see in the Internet so far? Give one service for each. Ans. Presentation and Session Layer. Services can be: formatting, encryption, compression for presentation layer and authentication, authorization, session management for the Session layer.
14. 表格

    描述已自动生成

**Compromises**: Virtual Circuit and subnets  
Memory vs bandwidth：VC’s require space in router memory but save potential overhead in full addressing of each packet and computation of path  
Setup time vs address parsing time  
VC’s require setup time and resources, but packet transmission is very fast  
Amount of memory：datagram subnets require large tables of every possible destination routes, whereas VC requires entry per link which depends on the load  
QoS and congestion avoidance：VC’s can use a tighter QoS - able to reserve CPU, bandwidth and buffer in advance  
Longevity：VC’s can exist for a long time

Vulnerability：VC’s particularly vulnerable to hardware/software crashes - all VC’s aborted and no traffic until they are rebuilt; datagram uses an alternative route

1. 表格

   描述已自动生成TCP segment header

Message Transfer  
Transfer  
SMTP (Simple Message Transfer Protocol)  
Delivery  
POP3 (Post Office Protocol 3)Download to a single device  
IMAP (Internet Message Access Protocol)Designed with multiple devices in mind

表格

描述已自动生成

计算题专题：(22年考题弄明白路由表、IP- allocation、RenoTHoa的具体区别计算、整一个表)

1. Hamming distance：
2. Hamming code: minimum number of check bits ANSWER:n data bits and k check bits,2^k >= n + k +1, if n = 16, the minimal number of k is 5

3.How can you increase the bit rate of a 1200KHz line from X bit/s to 3X bit/s without changing the frequency? ANSWER: Increase the number of bits per symbol from A bit/symbol to 3xA bits/symbol, for example, by increasing from a two-level code to a 8-level code basically. Consider a telephone line that is bandwidth limited to 4kHz. If we use 32 levels, what is the bit rate achieved to transmit data? ANSWER: 2 x 4 x log 2 of 32 gives 40kbps

3. bit-stuffing algorithm : insert 0 after 5 consecutive 1

Byte-stuffing

手机屏幕的截图

描述已自动生成

4.

表格

描述已自动生成

5.CRC：how does the receiver detect error after receiving the data? Briefly explain the process (2-3 sentences).Answer：When the receiver gets the data, it repeats the same CRC process that the sender did. The receiver divides the received data (original data + CRC) by the same generator polynomial used by the sender. If there's no error in transmission, the result of this division should be zero. If the result isn't zero, that means there was an error in transmission, and the receiver can then request the data to be sent again.

（给数据后面补最高项个数的0，然后二项除法）

6.RSA加密：

Given the RSA algorithm we studied last week, if p = 3, q = 11 and if

d = 3 and e = 7 instead of the version we saw in class, using the same

character mapping we saw in class though, where A is 01 and B is 02, and

C is 03 and so on, how would RSA work? Would it work at all? Show in

detail what numbers would be computed and transmitted at both ends of a

transmission if we want to send across a "D". Show where it fails if it

does not work properly?

Ans: It Works! p = 3, q = 11 means z is (3 - 1) x (11 - 1) = 20

d is chosen to be 3 which has no common factors with z which is good. e is 7 which means (d x e) is 3 x 7 = 21. Thus 21mod 20 is 1 which is another good choice!

n is p x q = 33

For encryption the pair to use 7,33 which is the public key ,and for decryption 3, 33 is used which is the private key!

To send "D", first we see that it has numerical value is 4 as per this question's suggestion. And 4 ^ 7 = 16384

16384 mod 33 = 16 is found next (Ok to use a calculator here but not necessary if you see 4 ^ 7 is 2 ^ 14)

16 is sent in transmission and then we take 16 ^ 3 = 4096 upon receipt, and then 4096 mod 33 to get 4 which concludes decryption, 4 is "D" in our coding. Eureka!

n=p\*q.

z=(p-1)\*(q-1)

find e such that (d\*e)mod Z=1

Public key(e,n) private key(d,n)

Encryption: cipher=(Plain^e)(mod n)

decryption: plain=(cipher^d)(mod n)

**7. TCP Tahoe 设为1 （Reno 是一个一个加1 从一半开始）**

**Tahoe：两次域值，在域值之下slow start （倍增）；域值之上 additive increase（+1）。一旦timeout occurs,把阈值设为原来的一半，窗口强制设为1MSS，进入slow start**

**Reno：增加了fast recovery，窗口强制设为原来的一半，阈值后进入**additive increase

Suppose that the TCP Tahoe congestion window was at 39 KB when the time out occurred. How big will the window size be if the next four transmission bursts are all successful and threshold was set at 20 KB?

Answer：

After time out occurs, threshold will be reset to half of previous, which is 20KB (39/2 = 19.5KB≈ 20𝐾𝐵). After that slow start is reinitiated and the size of congestion window will start as 1 segment (1 KB). The process of slow start is like:

The 1st transmission: 1 segment, 1KB;  
The 2nd transmission: 2 segments, 2KB;  
The 3rd transmission: 4 segments, 4KB  
The 4th transmission: 8 segments, 8KB  
(The upcoming 5th transmission will be: 16 segments, 16KB)  
Hence, after these 4 transmissions, the congestion window size will reach 16KB (≤ threshold 20KB).

**8.stop and wait -----efficiency:**

**E=DTP/S= DTP/ (DTP+ 2DP+ DTA)文本, 信件

描述已自动生成**

**9.** binary countdown protocol

**表格

描述已自动生成**

1. **Hierarchical routing table换表（拍照画图——用excel做表）**

****

**先做简答、再做计算**

**Leaky algorithm**

**The bucket is too small, we should have had a bucket size of 200KB. The input data is 20x20=400KB, in the same time the bucket can empty only 20x10=200KB and can hold another 100KB. So another 100KB bucket size is needed to deal with 400KB in total.**

**图片包含 日程表

描述已自动生成**

**0的意思：不是最后一个代码块 1:最后一个代码块**

**一些文字和图案

描述已自动生成**

**Bit Map Protocol and Binary Countdown are both Medium Access Control (MAC) protocols used in network communications to avoid collisions and manage how nodes access the communication medium. Here's a comparison between the two:**

**Bit Map Protocol:**

**Efficiency: when the number of stations is large ,Bit Map Protocol has lower efficiency, However, efficiency can decrease with collisions that happen when two or more stations try to transmit at the same time.**

**Fairness: Bit Map Protocol is inherently fair, each station has a designated slot in the bit map.**

**Binary Countdown**

**Efficiency:Binary Countdown can be more efficient when there are a large number of stations but only a few have data to send. However, efficiency can decrease with collisions that happen when two or more stations try to transmit at the same time.**

**Fairness:Binary Countdown may not be as fair as the Bit Map Protocol. Stations with lower binary addresses have a higher chance to win the contention, making the protocol biased towards these stations.**

**In summary, the choice between Bit Map Protocol and Binary Countdown may depend on the specific needs and characteristics of the network, such as the number of stations, traffic patterns, and the importance of fairness versus efficiency.**

**Unfortunately, I cannot see any diagram or image in the text-based conversation. However, I can provide you with a comparison between Diffie-Hellman key exchange and public key cryptography, along with their assumptions and benefits:**

**Diffie-Hellman Key Exchange:**

**Assumptions:**

**The security of the Diffie-Hellman key exchange relies on the discrete logarithm problem, which assumes that computing logarithms in a finite field is computationally difficult.**

**The prime modulus and generator used in the algorithm are assumed to be known and agreed upon by both parties.**

**Benefits:**

**Diffie-Hellman allows two parties to establish a shared secret key over an insecure channel without directly exchanging the secret key.**

**It provides perfect forward secrecy, meaning that even if the secret key is compromised in the future, previous communications remain secure.**

**The algorithm is relatively simple and computationally efficient.**

**Public Key Cryptography:**

**Assumptions:**

**- The security of public key cryptography is based on the mathematical difficulty of certain computational problems, such as factoring large integers or computing discrete logarithms.**

**- The participants must have access to each other's public keys, either through a trusted third party or through a public key infrastructure (PKI).**

**Benefits:**

**- Public key cryptography provides a mechanism for secure key exchange and encryption without requiring a pre-shared secret.**

**- It enables secure communication between parties who have never communicated before, as they can securely exchange public keys.**

**- Public key cryptography supports digital signatures, allowing verification of the authenticity and integrity of messages.**

**- It facilitates the creation of secure communication channels between multiple parties, such as in secure group communication protocols.**

**In summary, Diffie-Hellman key exchange and public key cryptography are both cryptographic methods that enable secure communication. Diffie-Hellman focuses on establishing a shared secret key, while public key cryptography provides a broader range of cryptographic operations and allows for secure key exchange without a pre-existing shared secret.**