**CS3031 – Advanced Telecommunications**

**2018 Exam Solutions**

**Question 1**

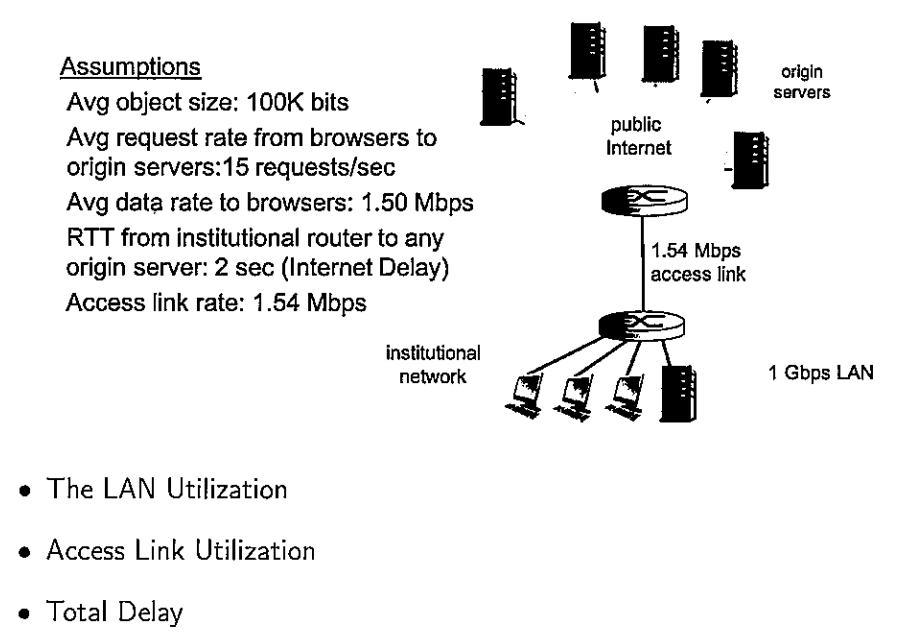
*a) What is the role of a “web proxy” in a large institutional network? What are the main advantages of installing a proxy server?*

The role of a web proxy in a large institutional network is to serve as an intermediary between incoming connections and the destination servers.

Proxy servers help improve web performance by storing a copy of frequently used webpages in a local cache on the proxy server. When a client requests a webpage stored in the proxy server’s cache, it is provided by the proxy server which is faster than relaying the request to the desired web server to fetch the page on every occurrence. Proxy servers also help improve security by filtering out some web content and malicious software.

Proxy servers also allow for requests to be blocked dynamically as well as sites, protocols and ports.

*b) Given the network and associated assumptions in the figure below calculate:*

**

* Object Size = 100K bits
* Request Rate = 15 req/s
* Data Rate to Browsers = 1.5 Mb/s
* RTT from Institution Router to Origin Server = 2 sec
* Access Link Rate = 1.54 Mb/s
* LAN Rate = 1 Gb/s

The **LAN Utilization** can be considered as:

The **Access Link Utilization** can be considered as:

The **Total Delay** can be considered as:

*Now assume that we install a web proxy server into the institutional network with a hit rate of 40%. Calculate:*



With the new cache, 40% of request are satisfied at cache, other 60% of requests are satisfied at origin, i.e 60% of requests will use access link. The **new Access Link Utilization** can be considered as:

The **new Total Delay** can be considered as:

This shows that by using a web cache you can reduce the access link utilization greatly and as a result reduce the total delay all at a much cheaper cost than expanding the access link.

*c) Describe the basic server hierarchy within the domain name system (DNS). Describe how DNSSEC validation takes place within a zone by detailing various Resource Records (RR), RRsets and Signature Keys that are required to secure a domain.*



The basic server hierarchy within the domain name system (DNS) is detailed as above.

DNSSEC provides origin authentication and integrity assurance services for DNS data. This prevents malicious attackers from spoofing DNS responses and redirecting users to malicious websites (e.g fake bank login page).

The first step towards securing a zone with DNSSEC is to group all the records with the same type into a resource record set (RRset).



Each zone in DNSSEC has a zone-signing key pair (ZSK). A zone operator creates digital signatures for each RRset using the private ZSK. Zone operators must also make their public ZSK available by adding it to their name server in a DNSKEY record. When a DNSSEC resolver requests a particular record type (e.g AAAA), the name server also returns the corresponding RRSIG.



*d) What is a “websocket” and what are its advantages over technologies such as AJAX and Comet? Why are websockets more efficient than traditional HTTP exchanges? Explain.*

Websockets allow a long-held TCP socket connection to be established between the client and server which allows bi-directional, full duplex, messages to be instantly distributed with little overhead resulting in a very low latency connection.

Websockets don’t fully replace AJAX, which should still be used for making short-lived web service calls. Unlike AJAX, WebSockets are based around an event model. The client and server can emit events and send data to each other whenever they want to. Whilst with AJAX each request must be followed by a response in a one-directional manner. Similar to AJAX, WebSockets must establish a connection with the server, however WebSockets only have to perform this once whilst with AJAX it must be done with every request causing high overhead latency.

Comet is a protocol that allows ‘**Sever push**’ behaviour wherein a server pushes events to a clients browser. It allows for the server to stream events to a client over a single persistent connection. It also allows for long polling where the browser polls the server for new events with a persistent request that is held open until it gets a response. WebSockets can be considered an extension upon Comet that allows for bi-directional pushing of events both to and from the client and server. This removes the need for long polling and significantly reduces the combined overhead of the communication.

*e) Describe in detail the main components of a X.509 certificate. Explain the “handshake” procedure used in the Secure Sockets Layer (SSL) protocol to establish a secure tunnel between web browser and server.*

The main components of a X.509 certificate are:

* Version: Which X.509 version applies to the certificate.
* Serial Number: Unique ID of cert assigned by CA.
* Algorithm Information: Information on signing algorithms used (e.g SHA-256).
* Issuer Name: Name of Certificate Authority (CA) issuing certificate.
* Validity Period: How long the cert is valid for.
* Subject Distinguished Name: Identity of the issued client.
* Subject Public Key Information: Clients public key information.



Within the Secure Socket Layer protocol (SSL) there are four main steps:

1. Server Authentication
2. Negotiation (agree on crypto algorithms)
3. Establish Keys
4. Client Authentication (optional)



1. A browser requests a secure page.
2. The web server sends its public key with its certificate.
3. The browser checks that the certificate was issued by a trusted root authority or Certificate Authority and that the certificate is still valid and that the certificate is related to the site contacted.
4. The browser then uses the public key, to encrypt a random symmetric encryption key and sends it to the server with the encrypted URL required as well as other encrypted http data.
5. The web server decrypts the symmetric encryption key using its private key and uses the symmetric key to decrypt the URL and http data.
6. The browser decrypts the http data and html document using the symmetric key and displays the information.