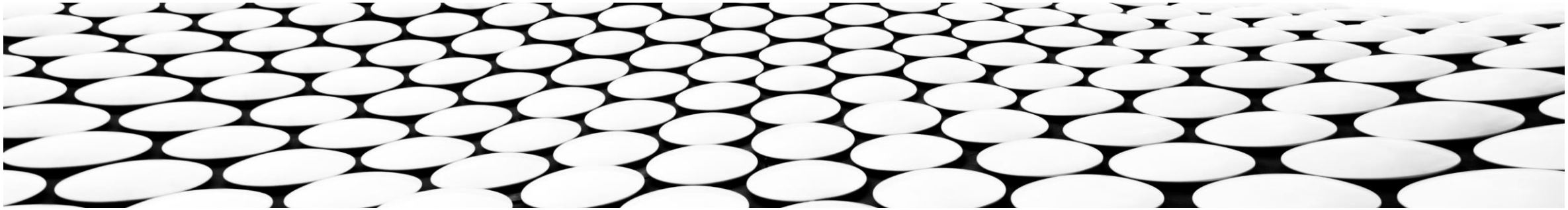
NETWORK ADMINISTRATION & SERVICES

CREATED BY :

MD. FORHAD HOSSAIN



DNS and SSH

DNS -stands for domain name system. It is an application layer protocol used to provide a human-friendly naming mechanism for internet resources. It is what ties a domain name to an IP address and allows you to access sites by name in your browser.

SSH - stands for Secure Shell.

- It is an encrypted protocol implemented in the application layer that can be used to communicate with a remote server in a secure way. Many additional technologies are built around this protocol because of its end-to-end encryption and ubiquity.

-There are many other protocols that we haven't covered that are equally important. However, this should give you a good overview of some of the fundamental technologies that make the internet and networking possible.

DNS Cache

Because of the large volume of requests generated in the DNS for the public Internet, the designers wished to provide a mechanism to reduce the load on individual DNS servers. To this end, the DNS resolution process allows for *caching* of records for a period of time after an answer. This entails the local recording and subsequent consultation of the copy instead of initiating a new request upstream. The time for which a resolver caches a DNS response is determined by a value called the time to live (TTL) associated with every record. The TTL is set by the administrator of the DNS server handing out the authoritative response.

The period of validity may vary from just seconds to days or even weeks.

DNS Security Issues

DNS was not originally designed with security in mind, and thus has a number of security issues.

- One class of vulnerabilities is DNS cache poisoning, which tricks a DNS server into believing it has received authentic information when, in reality, it has not.
- DNS responses are traditionally not cryptographically signed, leading to many attack possibilities; The Domain Name System Security Extensions (DNSSEC) modifies DNS to add support for cryptographically signed responses. There are various extensions to support securing zone transfer information as well.
- Even with encryption, a DNS server could become compromised by a virus (or for that matter a disgruntled employee) that would cause IP addresses of that server to be redirected to a malicious address with a long TTL. This could have far-reaching impact to potentially millions of Internet users if busy DNS servers cache the bad IP data. This would require manual purging of all affected DNS caches as required by the long TTL (up to 68 years).
- Some domain names can spoof other, similar-looking domain names. For example, "paypal.com" and "paypa1.com" are different names, yet users may be unable to tell the difference when the user's typeface (font) does not clearly differentiate the letter l and the numeral 1.

Thank You!