Nogas, Jean, R. BSIT 3A/CAL Activity#2 IAS1

A. List all TCP/IP Protocols, their uses, and the ports.

TCP/ IP Protocols	Ports	Use
1. HTTP (Hypertext Transfer Protocol)	80 (HTTP) and 443 (HTTPS)	Hypertext Transfer Protocol (HTTP) is a method for encoding and transporting information between a client (such as a web browser) and a web server. HTTP is the primary protocol for transmission of information across the Internet.
2. FTP (File Transfer Protocol)	21 (Control), 20 (Data)	FTP (File Transfer Protocol) is a standard network protocol used for the transfer of files from one host to another over a TCP-based network, such as the Internet.
3. SSH (Secure Shell)	22	The Secure Shell (SSH) protocol is a method for securely sending commands to a computer over an unsecured network. SSH uses cryptography to authenticate and encrypt connections between devices.
4. SMTP (Simple Mail Transfer Protocol)	25	The Simple Mail Transfer Protocol (SMTP) is a technical standard for transmitting electronic mail (email) over a network.
5. POP3 (Post Office Protocol version 3)	110	Post Office Protocol 3, or POP3, is the most commonly used protocol for receiving email over the internet.
6. IMAP (Internet Message Access Protocol)	143	Internet Message Access Protocol (IMAP) is a protocol for accessing email or bulletin board messages from a (possibly shared) mail server or service.
7. DNS (Domain Name System)	53	The purpose of DNS is to translate a domain name into the appropriate IP address.

8. DHCP (Dynamic Host Configuration Protocol)	67 (Server), 68 (Client)	Dynamic Host Configuration Protocol (DHCP) is used to dynamically assign Internet Protocol (IP) addresses to each host on your organization's network.
9. SNMP (Simple Network Management Protocol)	161 (SNMP), 162 (SNMP traps)	SNMP is used for communication between routers, switches, firewalls, load balancers, servers, CCTV cameras, and wireless devices
10. HTTPS (Hypertext Transfer Protocol Secure)	443	HTTPS prevents eavesdropping between web browsers and web servers and establishes secure communications.
11. Telnet	23	Telnet can be used to test or troubleshoot remote web or mail servers, as well as for remote access to MUDs (multi-user dungeon games) and trusted internal networks.
12. LDAP (Lightweight Directory Access Protocol)	389	Lightweight directory access protocol (LDAP) is a protocol that helps users find data about organizations, persons, and more.
13. RDP (Remote Desktop Protocol)	3389	Remote Desktop Protocol (RDP), a secure network communication protocol offered by Microsoft, allows users to execute remote operations on other computers.
14. NTP (Network Time Protocol)	123	The Network Time Protocol (NTP) is widely deployed in the Internet to synchronize computer clocks to each other and to international standards via telephone modem, radio and satellite.

B. **List all error messages in your browsers in 100s, 200s, 300s, 400s, and 500s**

List of HTTP Status Codes

100 Status Codes – Informational Responses

- 100: Continue. This code means the server in question has received your browser's request headers and is now ready for the request body to be sent.
- 101: Switching Protocols. Your browser has asked the server to change protocols and the server has agreed.
- 103: Early hints. This returns some response headers before the final HTTP message.

200 Status Codes – Success Responses

- 200: OK. The standard response for successful HTTP requests.
- 201: Created. The request has been fulfilled.
- 202: Accepted. The request has been accepted for processing, but the processing has not been completed. The request may or may not be acted upon and may be disallowed when the processing does occur.
- 203: Non-Authoritative Information. This code appears when a proxy is in use and means the proxy server received HTTP Code 200, everything is okay, from the origin server, but has modified the response before passing it on to your browser session.
- 204: No Content. This code means the server has successfully processed the request, but it's not going to return any content.
- 205: Reset Content. This is similar to the 204 code in that the server has successfully processed the request, but it's not going to return any content and the document view will be reset.
- 206: Partial Content. You may see this status code if your HTTP client uses range headers. This enables the browser to perform tasks like resuming paused downloads and splitting

downloads into multiple streams. This code is sent when a range header causes the server to send only part of the requested resource.

300 Status Codes – Redirection Responses

- 300: Multiple Choices. Sometimes there may be multiple processing resources the server can respond with to fulfill the browser's request. A 300 code means your browser needs to choose between them. This may occur if there are multiple file type extensions available or if the server is experiencing word-sense disambiguation.
- 301: The requested resource has been moved permanently. This code is delivered when a web page or resource has been permanently replaced with a different one. It's used for permanently redirecting a URL from one place to another.
- 302: The requested resource has moved, but was found. This code indicates the resource the browser is requesting was found, but not at the location the browser expected it. It's used for temporarily redirecting a URL from one place to another.
- 303: See Other. This code tells your browser that it found the resource you requested via one of the HTTP Request Methods, such as POST, PUT, or DELETE, but to retrieve it using the other method – GET, you have to issue that request to a different URL than the one you originally used.
- 304: The requested resource has not been modified since the last time you accessed it. This code tells your browser if it has a copy of the page already in the cache, it's okay to use it because the content on it didn't change since it was last cached.
- 307: Temporary Redirect. This code has replaced 302 "Found" as the appropriate action when a resource has been temporarily moved to a different or new URL.
- 308: Permanent Redirect. This code is the successor to the 301 codes.

400 Status Codes – Client Error Responses

- 400: Bad Request. This code means the server can’t return any response due to an error at the client’s end.
- 401: Unauthorized. This code is returned by the server when the resource you’re trying to access is requested without the proper authorization credentials. If you’ve set htpasswd authentication, you’ll see this if you don’t login properly.
- 402: Payment Required. This is a somewhat obscure error and was originally intended for use in a different industry. However, that never happened, so instead the code is used by a few platforms to indicate that a request cannot be fulfilled.
    - The Google Developer API will give this error when you have reached the daily request limit.
    - Shopify will give you this error if you haven’t paid your store fees and the store is temporarily suspended/deactivated.
    - Stripe will show you this error if your payment failed or they are blocking a transaction.
- 403: Access to that resource is forbidden. This code is returned when a user attempts to access something they don’t have permission to view. If you’re trying to access password-protected content without first logging in, you would probably see this error.
- 404: The requested resource was not found. This means the URL / content the browser requested isn’t on the server.
- 405: Method not allowed. This is generated when the web server supports the method received, but the target resource doesn’t.
- 406: Not acceptable response. The resource requested is capable of generating only content that is not acceptable according to the accepted headers sent with the request.
- 407: Proxy Authentication Required. A proxy server is in use and requires your browser to authenticate itself to continue.

- 408: The server timed out waiting for the rest of the request from the browser. This code is generated when the server times out while waiting for the full request from the browser.
- 409: Conflict. A 409 status code means the server couldn’t process the request from the browser because there’s a conflict with the relevant resource. This typically happens when there are multiple edits happening to the page simultaneously.
- 410: The requested resource is gone and won’t be coming pack. This is similar to a 404, but indicates to the browser this was expected, rather than unexpected, and is also very permanent.
- 411: Length Required. This means the requested resource requires the client to specify a certain length, and the client didn’t.
- 412: Precondition failed. Your browser included certain conditions in the request headers and the server didn’t meet those specs.
- 413: Payload too large. Or Request Entity Too Large. Your request is larger than the server is willing/able to process.
- 414: URI Too Long. This means a GET request has been encoded as a query string that is too large for the server to process.
- 415: Unsupported Media Type. This means your request was for a media type the server or resource doesn’t support.
- 416: Range Not Satisfiable. Your request was for a portion of a resource the server isn’t able to return.
- 417: Expectation failed. The server is unable to meet the requirements stated in the requests expect header field.
- 418: I’m a teapot. This is returned by teapots that receive requests to brew coffee. It’s an April Fools Joke.
- 422: Unprocessable Entity. The client request contains semantic errors and the server can’t process it.

- 425: Too Early. This error is sent when the server is unwilling to process a request because it may be replayed.
- 426: Upgrade required. Due to the contents of the requests upgrade header field, the client needs to switch to a different protocol.
- 428: Precondition Required. The server requires conditions to be specified before processing the request.
- 429: Too many requests. This is generated by the server when the user has sent too many requests in a given amount of time. Also known as rate-limiting.
- 431: Request Header Fields Too Large. The server can’t process the request because the header fields are too large. This may indicate a problem with a single header field or all of them.
- 451: Unavailable For Legal Reasons. The operator of the server has received a demand to prohibit access to the resources you have requested. Also a reference to the famous Ray Bradbury novel, Fahrenheit 451.
- 499: Client closed request. This code is returned by NGINX when the client closes the request while Nginx is still processing it.

500 Status Codes – Server Error Responses

- 500: There was an error on the server and the request could not be generated. This is a generic code that simply means, internal server error. Something went wrong on the server and what you’re requesting isn’t available.
- 501: Not implemented. This error indicates that the server does not support the functionality required to fulfill the request.
- 502: Bad gateway. This error code typically means that one server has received an invalid response from another, such as when a proxy server is in use.
- 503: The server is unavailable to handle this request right now. This code happens when a server may be overloaded and is unable to handle additional requests.

- 504: The server, acting as a gateway, timed out while waiting for another server to respond. This is the error returned when there are two servers involved in processing a request, and the first server times out waiting for the second one to respond.

- 505: HTTP Version not supported. The server doesn’t support the version of HTTP the client used to make the request.

- 511: Network Authentication Required. This error code is sent when the network you’re trying to use requires some form of authentication before sending your request to the server. For instance, you may need to agree to the terms and conditions of a public hotspot.

- 521: Web server is down. This is a Cloudflare-specific error message and means your browser was able to successfully connect to Cloudflare’s network, but it wasn’t able to connect to the origin server.

- 525: SSL Handshake failed. This error means that the SSL Handshake between a domain using Cloudflare and the origin web server failed.

C. Give the definition of each term and provide a sample.

1. Ipconfig (Internet Protocol Configuration)

- Internet Protocol Configuration (ipconfig) is a Windows console application that has the ability to gather all data regarding current Transmission Control Protocol/Internet Protocol (TCP/IP) configuration values and then display this data on a screen. Ipconfig also refreshes the Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) settings each time it is invoked. When invoked without additional parameters, ipconfig simply displays the IP address, default gateway and subnet mask for all available adapters.

2. Ping

- Ping is a command-line program designed to allow network admins to track the availability status of different devices in a network. It also helps discover network connectivity and latency issues.

3. Tracert (Traceroute)

- A traceroute provides a map of how data on the internet travels from its source to its destination. When you connect with a website, the data you get must travel across multiple devices and networks along the way, particularly routers.

4. Netstat (Network Statistics)

- (NETwork STATistics) A command line utility that reports the status of TCP/IP and Ethernet connections. Netstat comes with all major operating systems, but the Linux/Unix versions provide the most command options. GUI-based versions for Windows, such as Netstat Live and X-Netstat, are also available. See IPCONFIG and NSLOOKUP.

5. NSLookup (Name Server Lookup)

- (Name Server LOOKUP) A utility program that displays the IP address of a hostname or the hostname of an IP address by querying the domain name system (DNS) server. Originating in the Unix world, there are NSLOOKUP programs for Windows and all operating systems that support IP networks. See IPCONFIG and DNS.