1. **TRANSPORT LAYER PROTOCOLS**

* The transport layer is represented by two protocols: TCP and UDP.
* The IP protocol in the network layer delivers a datagram from a source host to the destination host.
* Nowadays, the operating system supports multiuser and multiprocessing environments, an executing program is called a process. When a host sends a message to other host means that source process is sending a process to a destination process. The transport layer protocols define some connections to individual ports known as protocol ports.
* An IP protocol is a host-to-host protocol used to deliver a packet from source host to the destination host while transport layer protocols are port-to-port protocols that work on the top of the IP protocols to deliver the packet from the originating port to the IP services, and from IP services to the destination port.
* Each port is defined by a positive integer address, and it is of 16 bits.

## **UDP**

* UDP stands for **User Datagram Protocol**.
* UDP is a simple protocol and it provides no sequenced transport functionality.
* UDP is a connectionless protocol.
* This type of protocol is used when reliability and security are less important than speed and size.
* UDP is an end-to-end transport level protocol that adds transport-level addresses, checksum error control, and length information to the data from the upper layer.
* The packet produced by the UDP protocol is known as a user datagram.
* Source port address: It defines the address of the application process that has delivered a message. The source port address is of 16 bits address.
* Destination port address: It defines the address of the application process that will receive the message. The destination port address is of a 16-bit address.
* Total length: It defines the total length of the user datagram in bytes. It is a 16-bit field.
* Checksum: The checksum is a 16-bit field which is used in error detection.

### **DISADVANTAGES OF UDP PROTOCOL**

* UDP provides basic functions needed for the end-to-end delivery of a transmission.
* It does not provide any sequencing or reordering functions and does not specify the damaged packet when reporting an error.
* UDP can discover that an error has occurred, but it does not specify which packet has been lost as it does not contain an ID or sequencing number of a particular data segment.

## **TCP**

* TCP stands for Transmission Control Protocol.
* It provides full transport layer services to applications.
* It is a connection-oriented protocol means the connection established between both the ends of the transmission. For creating the connection, TCP generates a virtual circuit between sender and receiver for the duration of a transmission.

## **FEATURES OF TCP PROTOCOL**

* **Stream data transfer:**
* TCP protocol transfers the data in the form of contiguous stream of bytes. TCP group the bytes in the form of TCP segments and then passed it to the IP layer for transmission to the destination. TCP itself segments the data and forward to the IP.
* **Reliability:**
* TCP assigns a sequence number to each byte transmitted and expects a positive acknowledgement from the receiving TCP. If ACK is not received within a timeout interval, then the data is retransmitted to the destination.  
  The receiving TCP uses the sequence number to reassemble the segments if they arrive out of order or to eliminate the duplicate segments.
* **Flow Control:** When receiving TCP sends an acknowledgement back to the sender indicating the number the bytes it can receive without overflowing its internal buffer. The number of bytes is sent in ACK in the form of the highest sequence number that it can receive without any problem. This mechanism is also referred to as a window mechanism.
* **Multiplexing:** Multiplexing is a process of accepting the data from different applications and forwarding to the different applications on different computers. At the receiving end, the data is forwarded to the correct application. This process is known as DE multiplexing. TCP transmits the packet to the correct application by using the logical channels known as ports.
* **Logical Connections:** The combination of sockets, sequence numbers, and window sizes, is called a logical connection. Each connection is identified by the pair of sockets used by sending and receiving processes.
* **Full Duplex:** TCP provides Full Duplex service, i.e., the data flow in both the directions at the same time. To achieve Full Duplex service, each TCP should have sending and receiving buffers so that the segments can flow in both the directions. TCP is a connection-oriented protocol. Suppose the process A wants to send and receive the data from process B. The following steps occur:
  + Establish a connection between two TCPs.
  + Data is exchanged in both the directions.
  + The Connection is terminated.
* Source port address: It is used to define the address of the application program in a source computer. It is a 16-bit field.
* Destination port address: It is used to define the address of the application program in a destination computer. It is a 16-bit field.
* Sequence number: A stream of data is divided into two or more TCP segments. The 32-bit sequence number field represents the position of the data in an original data stream.
* Acknowledgement number: A 32-field acknowledgement number acknowledge the data from other communicating devices. If ACK field is set to 1, then it specifies the sequence number that the receiver is expecting to receive.
* Header Length (HLEN): It specifies the size of the TCP header in 32-bit words. The minimum size of the header is 5 words, and the maximum size of the header is 15 words. Therefore, the maximum size of the TCP header is 60 bytes, and the minimum size of the TCP header is 20 bytes.
* Reserved: It is a six-bit field which is reserved for future use.
* Control bits: Each bit of a control field functions individually and independently. A control bit defines the use of a segment or serves as a validity check for other fields.
* URG: The URG field indicates that the data in a segment is urgent.
* ACK: When ACK field is set, then it validates the acknowledgement number.
* PSH: The PSH field is used to inform the sender that higher throughput is needed so if possible, data must be pushed with higher throughput.
* RST: The reset bit is used to reset the TCP connection when there is any confusion occurs in the sequence numbers.
* SYN: The SYN field is used to synchronize the sequence numbers in three types of segments: connection request, connection confirmation (with the ACK bit set ), and confirmation acknowledgement.
* FIN: The FIN field is used to inform the receiving TCP module that the sender has finished sending data. It is used in connection termination in three types of segments: termination request, termination confirmation, and acknowledgement of termination

|  |  |  |
| --- | --- | --- |
| **Basis for Comparison** | **TCP** | **UDP** |
| Definition | TCP establishes a virtual circuit before transmitting the data. | UDP transmits the data directly to the destination computer without verifying whether the receiver is ready to receive or not. |
| Connection Type | It is a Connection-Oriented protocol | It is a Connectionless protocol |
| Speed | slow | high |
| Reliability | It is a reliable protocol. | It is an unreliable protocol. |
| Header size | 20 bytes | 8 bytes |
| acknowledgement | It waits for the acknowledgement of data and has the ability to resend the lost packets. | It neither takes the acknowledgement, nor does it retransmit the damaged frame. |

* Confirmation.
  + Window Size: The window is a 16-bit field that defines the size of the window.
  + Checksum: The checksum is a 16-bit field used in error detection.
  + Urgent pointer: If URG flag is set to 1, then this 16-bit field is an offset from the sequence number indicating that it is a last urgent data byte.
  + Options and padding: It defines the optional fields that convey the additional information to the receiver.

## **WHAT IS A PORT?**

Port is a part of [the transport layer](https://www.baeldung.com/cs/osi-model) and helps in network communication. **A port is a logical identifier assigned to a process in order to identify that process uniquely in a network system.** When two network devices communicate, they do so by sending packets to each other. Each packet received by a receiver device contains a port number that uniquely identifies the process where the packet needs to be sent.

Not all the network protocol uses a port for communication. For example, [ICMP](https://www.baeldung.com/cs/popular-network-protocols) doesn’t use a port. On the other hand, protocols like [TCP, UDP, HTTP](https://www.baeldung.com/cs/popular-network-protocols) utilize a port for communication.

Let’s look at an example. A client computer is requesting the server for a virtual connection with the port number. [Telnet](https://en.wikipedia.org/wiki/Telnet) is a well-known protocol for establishing a remote connection over a [TCP/IP](https://www.baeldung.com/cs/popular-network-protocols) and it uses port. Hence, the server acknowledges the request from the client and start a telnet connection:

## **WHAT IS A SOCKET?**

Two processes that are running on a computer or running on two different systems can communicate via a socket. A **socket works as an inter-process communicator and seen as the endpoint of the process communication.** For communication, the socket uses a [file descriptor](https://en.wikipedia.org/wiki/File_descriptor) and is mainly employed in [client-server](https://en.wikipedia.org/wiki/Client%E2%80%93server_model) applications.

A socket consists of the [IP address](https://en.wikipedia.org/wiki/IP_address) of a system and the port number of a program within the system. The IP address corresponds to the system and the port number corresponds to the program where the data needs to be sent:

**Sockets can be classified into three categories: stream, datagram, and raw socket.** Stream sockets use connection-oriented network point to send and receive data. This type of sockets generally utilizes [TCP](https://www.baeldung.com/cs/popular-network-protocols) to permit processes to communicate with each other.

Datagram sockets use connectionless network protocols like [UDP](https://www.baeldung.com/cs/popular-network-protocols) to allow process communication. Raw sockets are datagram oriented and allow the processes to use ICMP for communication purpose.

Learn about popular enterprise routing protocols, including EIGRP and BGP, and how they differ.

ll dynamic routing protocols serve a single purpose: to direct data traffic down the optimal path toward a destination when given the choice between multiple paths. The “dynamic” part refers to the protocol's ability to recalculate and re-route traffic when more optimal paths become available or when links along the most optimal path fail. That said, not all dynamic routing protocols are alike. Let's examine four of the most popular routing protocols used within enterprises today to see how they differ and where they are best used within network infrastructures.

1. **RIPv2**

[Routing Information Protocol version 2 (RIPv2)](http://www.techrepublic.com/article/cisco-administration-101-know-the-basics-about-ripv2/), was a common LAN routing protocol in the '90s, but is rapidly fading away in production networks. RIPv2 suffered from scalability issues due to a relatively low maximum hop count of 15 routing devices. Compared to more modern dynamic routing protocols, RIPv2's methods for selecting optimal routes and the substantial convergence time it takes to recalculate paths renders it nearly obsolete. Today, the only reason you might run across a network running RIPv2 is either that the network is very old and in serious need of an upgrade or the network is running cheaper, consumer-grade routing hardware that can only support RIP.

**10-EIGRP**

Like RIPv2, [Enhanced Interior Gateway Routing Protocol (EIGRP)](http://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html) is a [hybrid distance vector protocol](http://www.professormesser.com/network-plus/n10-006/link-state-distance-vector-and-hybrid-routing-protocols-2/). But in terms of scalability and convergence times, EIGRP blows RIPv2 out of the water. EIGRP is a popular choice for routing within campus networks both big and small. Many network engineers believe that EIGRP is the best choice for a routing protocol on private networks because it offers the best balance between speed, scalability and ease of management.

**11-OSPF**

The main alternative to EIGRP for most campus LAN routing deployments is the [Open Shortest Path First (OSPF)](http://searchenterprisewan.techtarget.com/definition/OSPF) dynamic routing protocol. Unlike EIGRP, OSPF was always an open standard protocol and is an available option on virtually any modern enterprise network hardware made in the past two decades. While some say that OSPF is a bit more complicated to set up and manage compared to EIGRP, it's relatively easy to run once you get the hang of things such as [autonomous system routing domains](https://technet.microsoft.com/en-us/library/cc957842.aspx). Odds are that unless a network is very small, old or primarily Cisco, the dynamic routing protocol in use on the LAN will be OSPF.

**12-BGP**

The dynamic routing protocol that is the most different from all the others is the [Border Gateway Protocol (BGP)](http://www.networkcomputing.com/networking/bgp-fundamentals/1064527314). RIP, EIGRP and OSPF are all interior gateway protocols (IGP) while BGP is an exterior gateway protocol (EGP). Basically, interior protocols are meant to dynamically route data across a network that you fully control and maintain. Exterior routing protocols are used to exchange routes between distinctly separate networks that you have no administrative control over. BGP is the routing protocol used on the internet; therefore, the most common enterprise use is to run BGP on your internet edge when connecting to your ISP.

Now, why use a dynamic routing protocol such as BGP for routing to the Internet as opposed to simply creating a static default route? The reason would be if you have multiple internet connections to multiple providers and want to provide automatic failover and load balancing capabilities. That means you have multiple paths or choices on which ISP is the best path in and out for specific destinations on the internet. BGP can be used to either dynamically fail over from one ISP link to another when the primary connection fails. BGP also can be configured to teach either full or partial routing tables to make better routing decisions based on the optimal outbound internet path to the destination router.

As you can see, routing protocols have their own pros and cons and situations where they work best. Because of this, many organizations run multiple routing protocols on the same network and use [route redistribution](http://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/8606-redist.html) techniques to get them to play nice with one another.

# 13- TCP CONGESTION CONTROL

# Important Application Layer Protocols: DNS, FTP, SMTP, and MIME Protocols

**An In-Depth Look at the DNS, FTP, SMTP, and MIME Application Layer Protocols of TCP/IP Protocol Suite:**

In this [**In-Depth Networking Training Series**](https://www.softwaretestinghelp.com/computer-networking-basics/), we explored the [**Differences between IPv4 and IPv6 Addressing**](https://www.softwaretestinghelp.com/ipv4-and-ipv6/) in our previous tutorial. The application layer is the uppermost layer of the TCP/IP protocol suite.

In this tutorial, we will explore the various protocols that work on this layer in detail.

Being a software tester, it is important to understand the different features of each of the application layer protocols as the testers work on this layer and need it for their day to day work.

Each of the protocol has its own role and importance. A few of the majorly deployed protocols which we will discuss here include DNS, FTP, HTTP, MIME, SMTP, LDP, and DHCP.

## **DNS (DOMAIN NAME SERVER)**

If any user from the personal computer, laptop or tablet uses the Internet and tries to login into some website then the user is using DNS for sure. Thus it is very important to understand the working on a domain name server.

PC’s, laptop or tablets don’t understand the language of a web address, which means the domain name like Google.com to make them understand for which site we are looking for. Thus DNS came into the role and provides the host with the mapped IP address in respect to the domain name of the website.

**Suggested read =>>**[What is Uniform Resource Identifiers](https://www.softwaretestinghelp.com/what-is-uri/)

As shown in the above figure, when we request for a web page from our PC on the Internet like PC1 is requesting for www.softwaretestinghelp.com, then resolving the domain name query and providing the respective IP address in return is the part of work of the DNS server.

DNS server stores the database of all the relevant IP addresses mapped with their respective domain names.

***Further reading =>>***[*How to flush the DNS Cache*](https://www.softwaretestinghelp.com/flush-dns-cache/)

The DNS query for requesting the IP address in respect to the domain name goes to the DNS server 1 from PC1. The server checks within itself, if it has the IP address regarding the query, and it returns a DNS response with the resolution.

Otherwise, it forwards it to another DNS server 2 requesting for information. This time it gets the resolution from the DNS 2 and it gets mapped with the IP address i.e. 10.150.120.2 corresponding to the Domain name in response and sends it back to PC1.

The PC1 now have the destination IP address and it can communicate further with the known IP address as per the routing.

Now the question arises, as of how the PC will come to know which DNS should be used to get the IP address.

The answer to this is when we connect our system to the ISP, the network devices like a router or switch which assigns the routing information and other configurations as well send which or how many DNS server the PC should connect with to get the address translation.

## **14- FTP (FILE TRANSFER PROTOCOL)**

It is one of the widely used application layer protocol of the TCP/IP protocol suite. FTP is basically used to exchange data between two host devices over the Internet or Intranet securely.

It is referred to as one of the safest modes of file sharing among systems, and thus it is deployed by large industries, universities, and offices.

It works in the client-server model and thus the user needs an FTP client program to run FTP on its system. The common types of FTP client program include Filezilla and Dreamweaver etc.

The data transfer takes place only in one direction at a time. The FTP protocol carry out many duties apart from file transfer like creation and deletion of data files, listing, renaming, etc.

### **15- THE FTP MODEL**

In this model, one host behaves as the client and another host as a server. The one who requests for file-sharing or data is the client host and one which in response completes the request is the server host.

Firstly the FTP connection is established between the client and server computer and data exchange take place after that. Two channels come into the picture of FTP connection i.e. control channel and data channel.

The control channel establishes the connection between the client and server and remains open for the overall session. The control channel port number is 21 in TCP/IP. While the data channel opens when the client request for a file sharing and get closed after the completion of the request by the server.

Two processes naming data transfer process (DTP) and protocol interpreter (PI) are used in managing the communication between the client and the server. The DTP establishes and manages the connection for the data channel, while PI manages the DTP by applying commands given by the control channel.

The server host end PI is accountable for analyzing the commands received from the client host end via the control channel, connection establishment, and in running the DTP. The client PI is accountable for forwarding the FTP commands, receiving the response from the server and establishment of the connection with the FTP server.

After the establishment of a connection between the FTP client and the FTP server, the client builds up the connection and sends the FTP commands to the server. The server analyzes them and in response completes the request.

Now the server end PI sends the port detail on which the files will be forwarded to the client DTP. The client DTP then waits for the data to arrive at the decided port from the server.

### **16- THE FTP RESPONSE**

To make out a secure and reliable file transfer between the client and server, it is important that the server and client should remain in synchronization with each other.

Thus for each command executed by the client, a user is acknowledged by the response and the action is performed by the server host in order. The response consists of a 3 digit code plus a text (a character string is separated from digit by a space) denoting the processing of the commands.

### **17- TYPES OF CONNECTION**

The FTP server is connected to the FTP client on the control port 21. After this, the client will decide which type of connection it will make with the FTP server, i.e. whether an active or passive connection.

**(i) Active Connection:**If an active connection is established, then the data connection from the server end is opened on port 20 or to a greater range towards the client’s end. Then all the data flow will take place on this connection.

**(ii) Passive Connection**: If the passive connection is established, the client requests for passive connection from the server and assigns any port greater than 10,000. The server bounds itself to this port and gets back to the client with it.

The client then opens a new data connection for a particular session on this newly bounded port. In a passive connection, every time a new port is assigned when a new data connection request is raised from the client’s end. The latest trend in the networking system operates mostly in passive mode.

**Example:**Let’s take the example of a software organization, where hundreds of performance and daily activity reports are generated by the employees and those need to be shared with their vertical head, CEO or seniors at the remote end.

One way of sharing the daily reports and tracker is to send an e-mail to all of them. However, it takes a lot of time and if the size of the attachment is big in an e-mail, then it will take much time for downloading and the mailbox will get full frequently due to oversized mails.

The other way to do this is that the creators of data will put the reports and trackers on the FTP server and share the path with each concern. In this case, the end-user will behave as the client host and can access the files of their era from the server by just logging onto the server.

The server can be made secure by putting a password. Only the concerns will have the username and password to access it. The port used here is 21. As per rights granted to the clients, they can also create a copy, modify and delete the files on the server and from the server.

## **18- SMTP (SIMPLE MAIL TRANSFER PROTOCOL)**

It is used by the e-mail server for sending and receiving messages, but the client host-based application only uses it for sending messages to the mail server. For receiving purposes, they use POP3 or IMAP.

It is a TCP/IP application layer protocol and the TCP port used by the mail servers is 25 while the mail clients use the port 587 or 465 for communication.

The outlook mail system of Microsoft system, Gmail and Yahoo mail, deploy SMTP for sending and retrieving emails from the exterior world whereas for interior mail exchange between their respective systems they use their own protocols.

The client using the e-mail services known as mail user agent (MUA) deposit mail to the mail server, Mail submission agent (MSA) using SMTP on port 587. The MSA forwards the mail to its Mail transfer agent (MTA) which in turn does the processing on the PC or laptop host device.

**#1)** Sometimes for sending the mail to the recipient host, it can move through many intermediate computer host devices, therefore, each device uses SMTP to forward messages on the next host device until it reaches the destination.

**#2)**The MTA deploys the DNS to find out the mail exchanger record (MX), which provide the details about the domain of the receiver. (Means the part of the mail address after @ **For Example** Gmail or Yahoo mail etc).

On the basis of information gathered from the MX record about the destination host, the MTA finds out the exchange server and connects to it as a SMTP client for message delivery.

**#3)** The transportation of message can move through a single hop or series of intermediate hops to reach the final destination. Once the final destination is reached, the MTA handovers the message to MDA (message delivery agent) for final delivery. The MDA stores messages in the appropriate mailbox format.

**#4)** After the delivery of the mail to the local mail server, the mail is stored, so that it can be retrieved by authenticated end users, i.e. MUA’s. The e-mail clients use IMAP or POP protocol to access the emails and for receiving the mail in the desired format Microsoft Outlook, Lotus Notes etc., which are designed for the SMTP format are used.

**#5)** The SMTP only concerns about the transportation of the e-mail and not the content of it. It is a connection-oriented protocol and the protocol messages are text-based.

A particular SMTP session includes commands initiated by a SMTP client and the respective response from the SMTP server. At the sending end, the initiating agent performs the actions while at the receiving end the listening agents and the recipient perform the tasks.

The role of SMTP in outlook is shown with the help of the below screenshots and which of the configurations of SMTP is done for sending e-mails is described as well.

## **18- MIME (MULTIPURPOSE INTERNET MAIL EXTENSIONS)**

It is basically an extension of the initial e-mail protocol known as SMTP and allows the users to use the protocol for sharing various kinds of data files on the Internet such as Audio, video, images and various program files along with ASCII text as deployed in the original one.

### **FEATURES OF MIME**

* In a single message, several attachments can be sent easily.
* There is no limitation of the length of the message.
* Apart from ASCII codes, other data files can also be shared through it.
* Different kinds of layouts, font style, colors, and size can be used in the message.
* MIME uses the special header format to illustrate the type of format that the mail body is using. Hence, it will make it simple for the email-client to understand it in the correct format.
* Even though MIME is designed to support the SMTP, the content type which is defined in the MIME has the significance in the Communication protocols apart from the e-mail.

The web servers add the MIME header at the starting point of the circulation of web data. The web clients, thus use this content-type header for finalizing the suitable viewer application for their service as indicated by the header.

### **MIME HEADERS**

### 

**(i) MIME-VERSION**

The existence of this header specifies that the message is MIME formatted. The latest version used is 1.0, hence it is shown as **MIME-Version: 1.0.**

**(ii) CONTENT-TYPE**

It specifies the message data’s type and subtype. The default header value will appear as **Content-Type: text/plain.**The above type and sub-type mean that the message contains simple text.

**For Example**, The detailing for image, audio, and video will be like image/gif, audio/mp3, and video/mp4.

**(iii) CONTENT-TRANSFER-ENCODING**

It specifies the type of encoding deployed in the message body. The various encoding techniques used are 7-bit, 8-bit, binary, base-64 for binary files with attachments and quoted-printable.

**(iv) CONTENT-DISPOSITION**

It specifies the presentation style and the filename associated with the message.

The presentation style can be of two types, first is inline in which whenever the mail is displayed, the presentation style will automatically come up, and second is the attachment type in which it is not displayed until we perform a certain action to open it.

The MIME is used in the HTTP protocol to distinguish between the types of web documents used. During the communication session between the web server and a browser, firstly the web server sends the MIME content type.

**For Example,** **Content-disposition: attachment** to browser thus the browser comes to know how it should display the content.

**18-Voice over INTERNET PROTOCOL**

### **VoIP**

Voice over [Internet protocol](https://www.sciencedirect.com/topics/computer-science/internet-protocol) (VoIP) carries voice via data networks, a fundamental change from analog POTS, or [plain old telephone service](https://www.sciencedirect.com/topics/computer-science/plain-old-telephone-service), which remains in use after over 100 years. VoIP brings the advantages of packet-switched networks, such as lower cost and resiliency, to the telephone.

Common VoIP protocols include real-time transport protocol (RTP), designed to carry streaming audio and video. VoIP protocols such as RTP rely upon session and signaling protocols including [*session initiation protocol*](https://www.sciencedirect.com/topics/computer-science/session-initiation-protocol) (SIP, a signaling protocol) and H.323. SRTP (secure real-time transport protocol) is able to provide secure VoIP, including confidentiality, integrity, and secure [authentication](https://www.sciencedirect.com/topics/computer-science/authentication). SRTP uses AES for confidentiality and SHA-1 for integrity.

### **THE BENEFITS OF VoIP**

VoIP allows users to make phone calls over the Internet, or any other [IP](https://www.sciencedirect.com/topics/computer-science/internet-protocol) network, using the packet-switched network as a transmission medium rather than the traditional circuit transmissions of the PSTN. If a quality Internet connection is available, phone service can be delivered through this Internet connection instead of from the local phone company. This assumes that the Internet connection is from someone else other than the local telephone company such as a CATV company or a wireless provider.6 As the technology has become more reliable in recent years, enterprise organizations and residential customers have been moving to VoIP for a number of reasons:

Consolidation of voice and data on one network reduces costs and results in a lower network [total cost of ownership](https://www.sciencedirect.com/topics/computer-science/total-cost-of-ownership) (TCO).

Operating expense savings include lower long-distance charges, reduced support costs, and savings via workforce virtualization.

Newer and increased functionality, specifically automatic routing of calls to the VoIP phone set no matter where it may be.

Using an ATA users can talk and surf the web at the same time on a single connection.7

Companies also use the migration to VoIP as an opportunity to replace aging telephony equipment with feature-rich technology such as teleconferencing and collaboration/multimedia applications.

VoIP supports increased mobility, since remote workers have the same access to voice features as corporate office employees.