Ethernet is now the dominant LAN connectivity technology, and Token Ring is rarely seen anymore. Ethernet uses the CSMA/CD specification which stands for "Carrier Sense, Multiple Access / Collision Detect". With Ethernet, data travels through the network inside units called frames, with each frame containing source and destination addresses. If data from multiple computers are transmitted at the same time and a collision happens, the systems wait before transmitting again. In a Token Ring network, all devices are connected to the network, with empty data frames circulating around the ring. A computer is granted the right to transmit data. Then the data and destination are inserted into an empty frame. The destination system grabs the data, the message is removed from the frame, and the now-empty frame is sent back circulating around the ring until another system needs to send a message. Token Ring devices are often quite a bit more expensive than the ethernet equivalent due to the cost of the extra logic the boards need to have as well as having to have MAU's or CAU's etc. Ethernet is available at speeds of 10, 100 and 1000mb/s. There are many tools, utilities and various suppliers of devices for ethernet, whereas the choices for Token Ring are much more limited.

Bridge

In telecommunication networks, a bridge is a product that connects a local area network (LAN) to another local area network that uses the same protocol. Bridge has a single incoming and outgoing port and filters traffic on the LAN by looking at the MAC address. Bridge looks at the destination of the packet before forwarding unlike a hub. It restricts transmission on other LAN segment if destination is not found. A bridge works at the data-link (physical network) level of a network, copying a data frame from one network to the next network along the communications path.

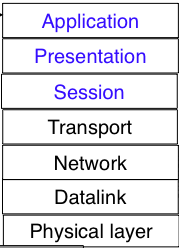
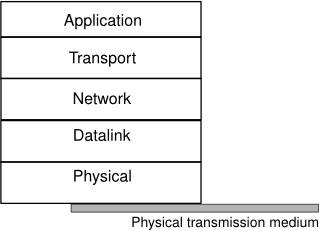
Switch

A switch when compared to bridge has multiple ports. Switches can perform error checking before forwarding data, which are very efficient by not forwarding packets that error-end out or forwarding good packets selectively to correct devices only. Switches can support both layer 2 (based on MAC Address) and layer 3 (Based on IP address) depending on the type of switch. Usually large networks use switches instead of hubs to connect computers within the same subnet.

REPEATER

A network device used to regenerate or replicate a signal. Repeaters are used in transmission systems to regenerate analog or digital signals distorted by transmission loss. Analog repeaters frequently can only amplify the signal while digital repeaters can reconstruct a signal to near its original quality. In a data network, a repeater can relay messages between sub networks that use different protocols or cable types. Hubs can operate as repeaters by relaying messages to all connected computers. A repeater cannot do the intelligent routing performed by bridges and routers.

SMTP, POP3 and IMAP are TCP/IP protocols used for mail delivery. SMTP stands for Simple Mail Transfer Protocol. SMTP is used when email is delivered from an email client, such as Outlook Express, to an email server or when email is delivered from one email server to another. SMTP uses port 25. POP3 stands for Post Office Protocol. POP3 allows an email client to download an email from an email server. The POP3 protocol is simple and does not offer many features except for download. Its design assumes that the email client downloads all available email from the server, deletes them from the server and then disconnects. POP3 normally uses port 110. IMAP stands for Internet Message Access Protocol. IMAP shares many similar features with POP3. It, too, is a protocol that an email client can use to download email from an email server. However, IMAP includes many more features than POP3. The IMAP protocol is designed to let users keep their email on the server. IMAP requires more disk space on the server and more CPU resources than POP3, as all emails are stored on the server. IMAP normally uses port 143.



Compared to the five layers reference model explained above, the OSI reference model defined is divided in seven layers. The four lower layers are similar to the four lower layers described above.

The main similarities between the two models include the following:

Both of the models share a similar architecture. This can be illustrated by the fact that both of them are constructed with layers.

They share a common application layer. Both of the models share a common "application layer". However in practice this layer includes different services depending upon each model.

Both models have comparable transport and network layers. This can be illustrated by the fact that whatever functions are performed between the presentation and network layer of the OSI model similar functions are performed at the Transport layer of the TCP/IP model.

Both models assume that packets are switched. Basically this means that individual packets may take differing paths in order to reach the same destination.

DIFFERENCES

TCP/IP Protocols are considered to be standards around which the internet has developed. The OSI model however is a "generic, protocol-independent standard."

TCP/IP combines the presentation and session layer issues into its application layer.

TCP/IP combines the OSI data link and physical layers into the network access layer.

TCP/IP appears to be a more simpler model and this is mainly due to the fact that it has fewer layers.

TCP/IP is considered to be a more credible model. This is mainly due to the fact because TCP/IP protocols are the standards around which the internet was developed therefore it mainly gains creditability due to this reason. Whereas in contrast networks are not usually built around the OSI model as it is merely used as a guidance tool.

A datagram is a basic transfer unit associated with a packet-switched network. The delivery, arrival time, and order of arrival need not be guaranteed by the network.

RFC 1594 defines the term Datagram as follows:

A self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network.”

Applications that communicate via datagrams send and receive completely independent packets of information. These clients and servers do not have and do not need a dedicated point-to-point channel. The delivery of datagrams to their destinations is not guaranteed. Nor is the order of their arrival.

The following are advantages of using UDP over TCP:

1) UDP does not need the overhead required to detect reliability.

2) It does not need to maintain the unexpected deception of a data flow.

3) UDP requires less processing at the transmitting and receiving of hosts

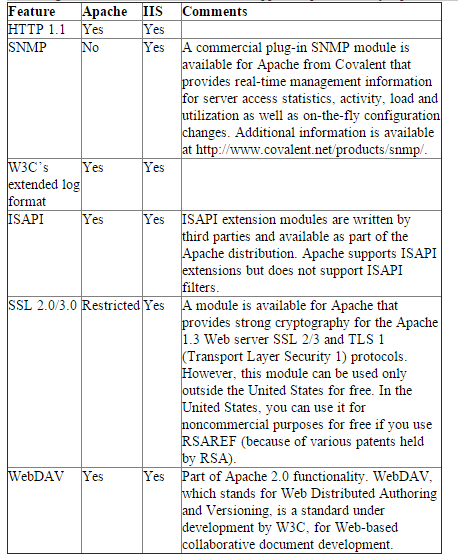
4) It is simple to use for a network.

5) The operating system does not need to maintain UDP connections information.

UDP is more appropriate to use it on large distributed systems where each host has to communicate with many destinations at the same time.

Standards Support

Standards support is very important in many government contracts and procurements. The following table summarizes the standards support implemented by Apache and IIS.



Web Server Prerequisites

A major difference between Apache and IIS is their prerequisites. While Apache is available for many Unix versions, Linux, Windows and OS/2, IIS can run only in the Windows environment.

Administration Considerations

Both Apache and IIS provide many built-in administration functions. These functions include:

Web server administration using scripts for commonly performed functions

Support for multiple hardware virtual servers using separate IP addresses

The ability to manage multiple Web servers as one server

Support for multiple software virtual servers using host headers

Unlike Apache, IIS provides GUI support for server administration. Besides administrative GUI support, IIS also provides the ability to administer one or more IIS Web servers from a Web browser. IIS also provides some common administration functions available with other Microsoft products, such as a setup wizard and unattended/remote setup and maintenance. IIS even provides integration with Windows operating system functions such as directory services, backup and restore of IIS configuration information and the Windows performance monitor (to view IIS performance data).

Log Considerations

Both Apache and IIS can write to multiple logs using standard and extended log formats (from the W3C) and can even support custom logging. Both products permit logging to text files. Both products also let you automatically close an aging log file and open a new file based on elapsed time. Here again, IIS provides better integration with Windows OS facilities. For example, IIS can write file security and application events to the Windows event log, which can then be viewed using standard Windows tools, such as Event Viewer. IIS also provides logging to any ODBC database. In fact, multiple IIS servers can log to a single ODBC database. Logging to an ODBC database in Apache is possible, but only through an add-on. Likewise, modules are available outside the official Apache distribution that provide log file analysis, data distribution and so on.

Security Considerations

Both Apache and IIS support basic security features out of the box. These include:

Restrict access by domain name

Restrict access by user

Restrict access by group

Restrict access by directory and/or file

Restrict access by IP address

Basic HTTP user authorization with clear-text passwords

However, IIS provides the ability to integrate Web server security with Windows security features.

Content Management Considerations

Both Apache and IIS provide functions for content management, such as:

Content expiration

Multiple platform support for content store and make commands

Built-in image map handling

Custom HTTP headers

HTTP redirects

Document footers

Custom error messages

Additionally, IIS provides Windows-style tools, such as HTML page and site wizards as well as HTML templates. With its tight Windows integration, IIS can also provide enhanced file system security.

Phone modems are typically 56 kbps, DSL modems are faster ranging from 100s of kbps to a 1-2 mbps, Cable ranges from 100s of kbps to 10s of mbps. T1 is at 1.5mbps, T2 is at 6 mbps and T3 can go up to 50 mbps. T1, T2, and T3 are "two-point”, dedicated, high capacity, and digital service network of leased lines used in telecommunications. All lines are reserved circuits that operate over either copper or fiber optic cables. Typical ISDN speeds are about 100kbps. Wireless LAN bit rates can range from 1-100 mbps. Fiber optic cables can have speeds of 111gbps or more. Satellite transmissions are slower than all others and bit rates can range from 1mbps. My home internet connection speed is 15. 5mps.

MIME was designed to extend the format of email to support non-ASCII characters, attachments other than text format, and message bodies which contain multiple parts. MIME describes the message content type and the type of encoding used with the help of headers. All manually composed and automated emails are transmitted through SMTP in MIME format. The association of Internet email with SMTP and MIME standards is such that the emails are sometimes referred to as SMTP/MIME email. The MIME standard defines the content types which are of prime importance in communication protocols like HTTP for the World Wide Web. The data are transmitted in the form of email messages through HTTP even though the data are not an email.

The features offered by MIME to email services are as follows:

Support for multiple attachments in a single message

Support for non-ASCII characters

Support for layouts, fonts and colors which are categorized as rich text.

Support for attachments which may contain executables, audio, images and video files, etc.

Support for unlimited message length.

A simple HTTP transaction is one where the client makes a single request for HTTP content.

DNS Lookup: The client tries to resolve the domain name for the request.

Client sends DNS Query to local ISP DNS server.

DNS server responds with the IP address for hostname.com

Connect: Client establishes TCP connection with the IP address of hostname.com

Client sends SYN packet.

Web server sends SYN-ACK packet.

Client answers with ACK packet, concluding the three-way TCP connection establishment.

Send: Client sends the HTTP request to the web server.

Wait: Client waits for the server to respond to the request.

Web server processes the request, finds the resource, and sends the response to the Client. Client receives the first byte of the first packet from the web server, which contains the HTTP Response headers and content.

Load: Client loads the content of the response.

Web server sends second TCP segment with the PSH flag set.

Client sends ACK. (Client sends ACK every two segments it receives. from the host)

Web server sends third TCP segment with HTTP\_Continue.

Close: Client sends a FIN packet to close the TCP connection.

A POST request is different from a GET request in the following ways:

There's a block of data sent with the request, in the message body. There are usually extra headers to describe this message body, like Content-Type: and Content-Length:.

The request URI is not a resource to retrieve; it's usually a program to handle the data you're sending.

The HTTP response is normally program output, not a static file.

CGI is a means by which Web servers interface to other application programs, thus extending the services provided by the Web server. By way of CGI scripts, users gain program access to Web servers and can extend the capability of HTML. It should be noted that the term ‘Web server’ does not necessarily mean a physical piece of harware; it is a piece of software that can reside locally or on another remote machine. CGI was one of the first practical techniques for creating dynamic content and it has made possible all sorts of new functionality in Web pages. CGI has become a de facto standard used on most modern Web servers today.