CSC 402 – Internet Technology

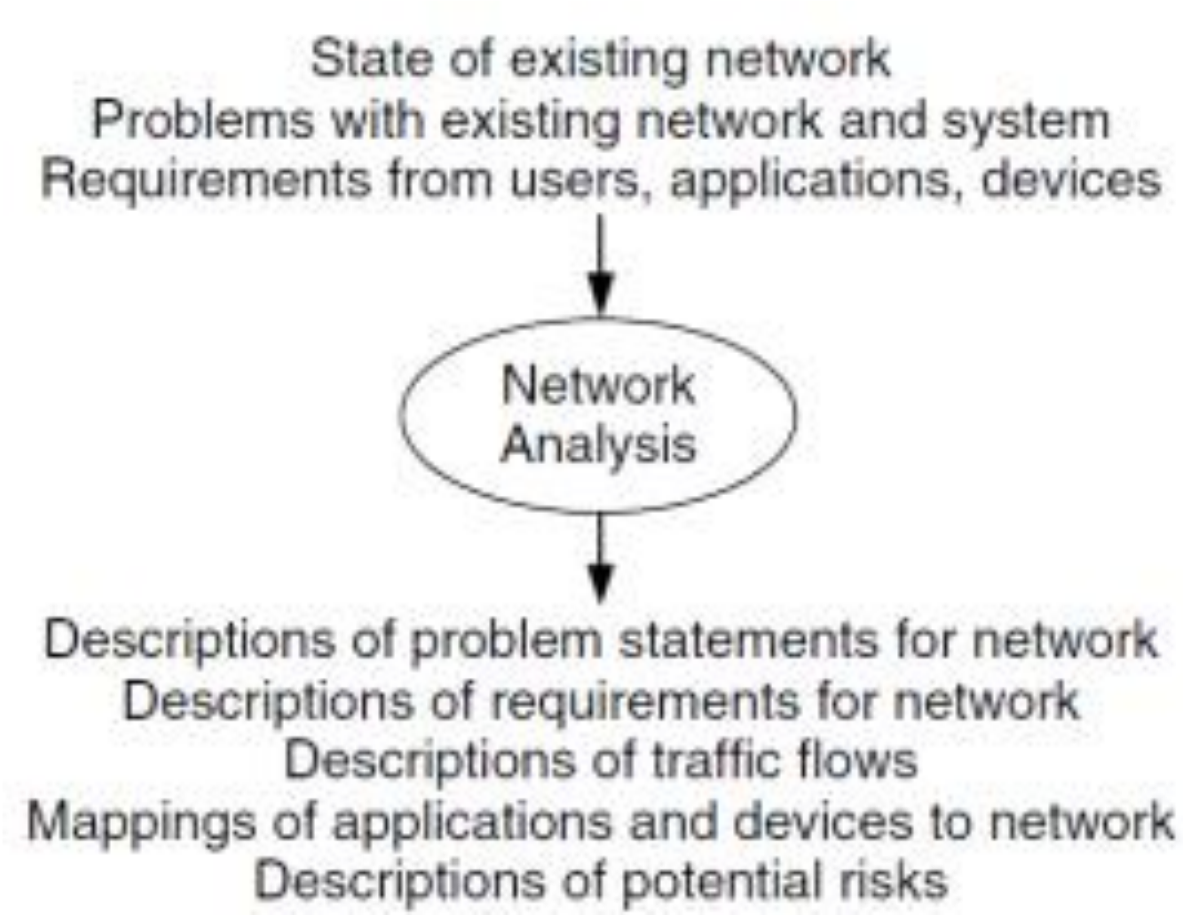
Recap

- Network
- Internet
- Network Architecture
- Choice of Platform

Designing of Internet System Network Architecture

- Traditionally, network analysis, architecture & design focused on
  - Developing & applying a set of rules
    - eg. 80/20 rule, “bridge when you can, route when you must”
  - capacity /bandwidth planning
    - eg. situation -specific and time-specific traffic flow estimation
  - Projections – likely growth & usage pattern
- Today’s evolving network
  - Reliability, maintainability, and availability (RMA)
- Networks as a system providing different services to its users
- Network analysis, architecture & design processes in engineering a new or existing one

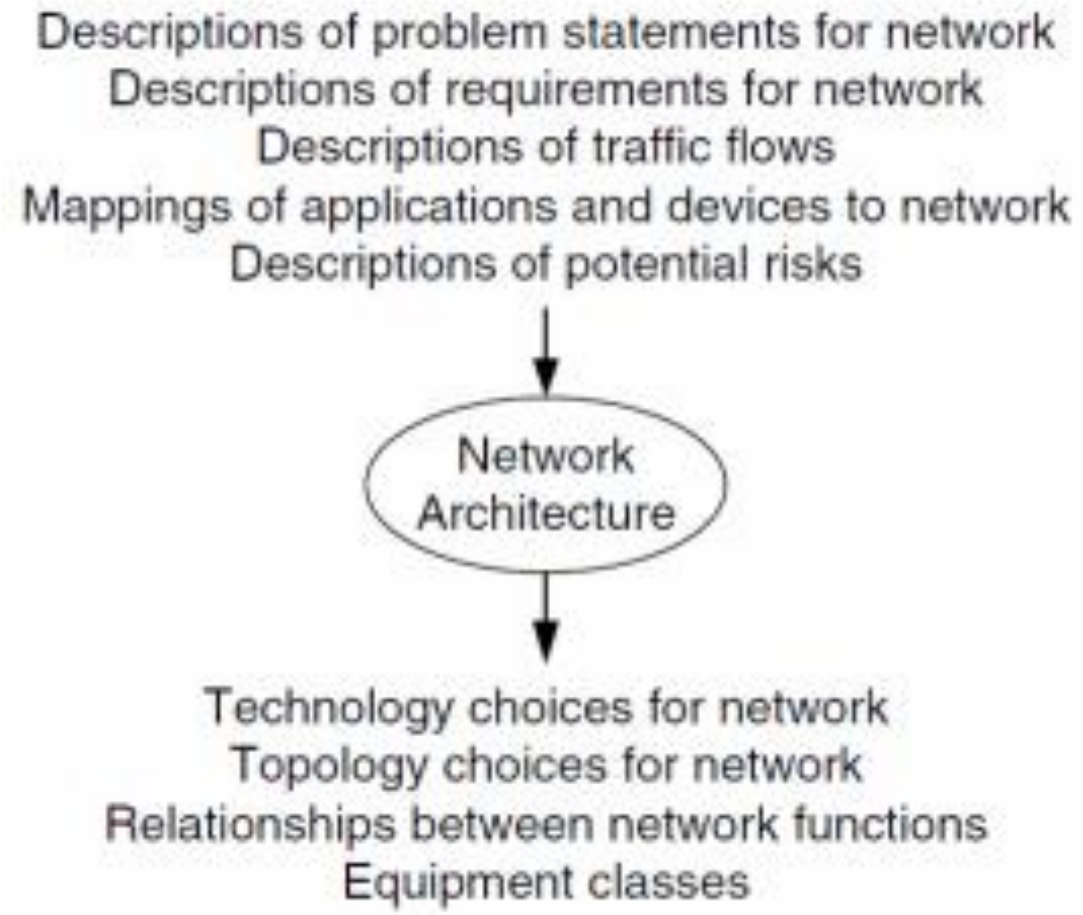
Designing of Internet System Network Architecture



State of existing network
Problems with existing network and system
Requirements from users, applications, devices

Network Analysis

Descriptions of problem statements for network
Descriptions of requirements for network
Descriptions of traffic flows
Mappings of applications and devices to network
Descriptions of potential risks

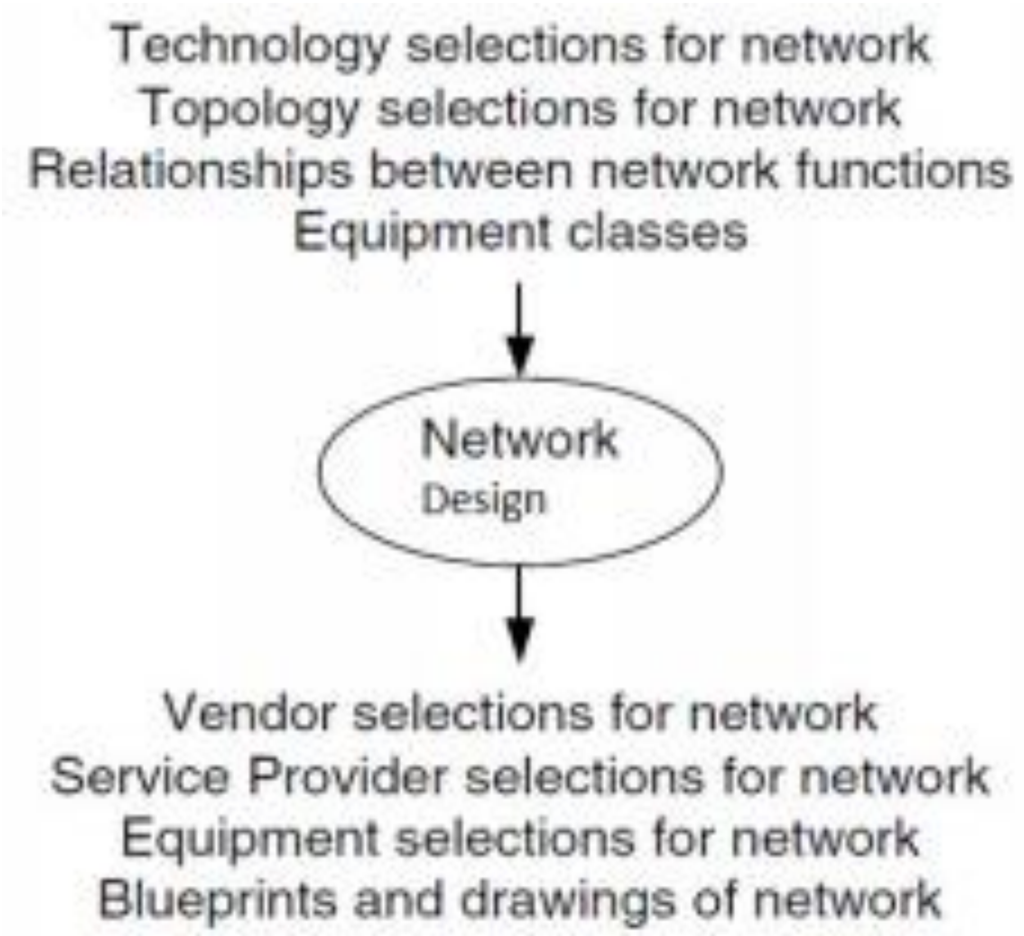


Descriptions of problem statements for network
Descriptions of requirements for network
Descriptions of traffic flows
Mappings of applications and devices to network
Descriptions of potential risks

Network Architecture

Technology choices for network
Topology choices for network
Relationships between network functions
Equipment classes

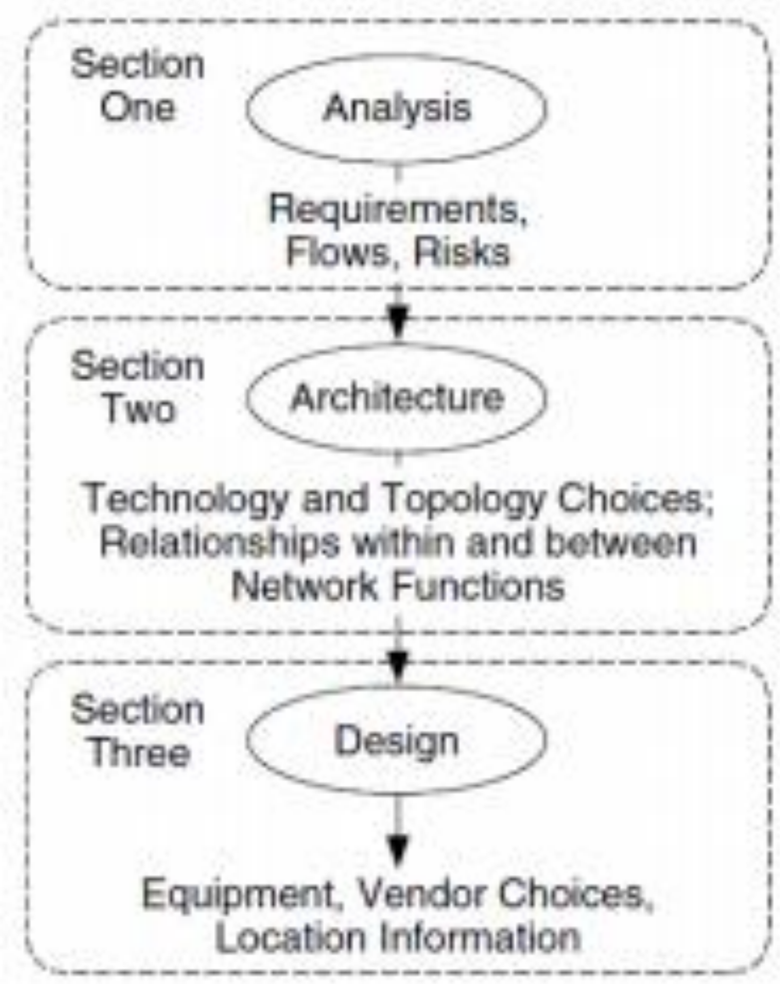
Designing of Internet System Network Architecture



Technology selections for network
Topology selections for network
Relationships between network functions
Equipment classes

Network
Design

Vendor selections for network
Service Provider selections for network
Equipment selections for network
Blueprints and drawings of network

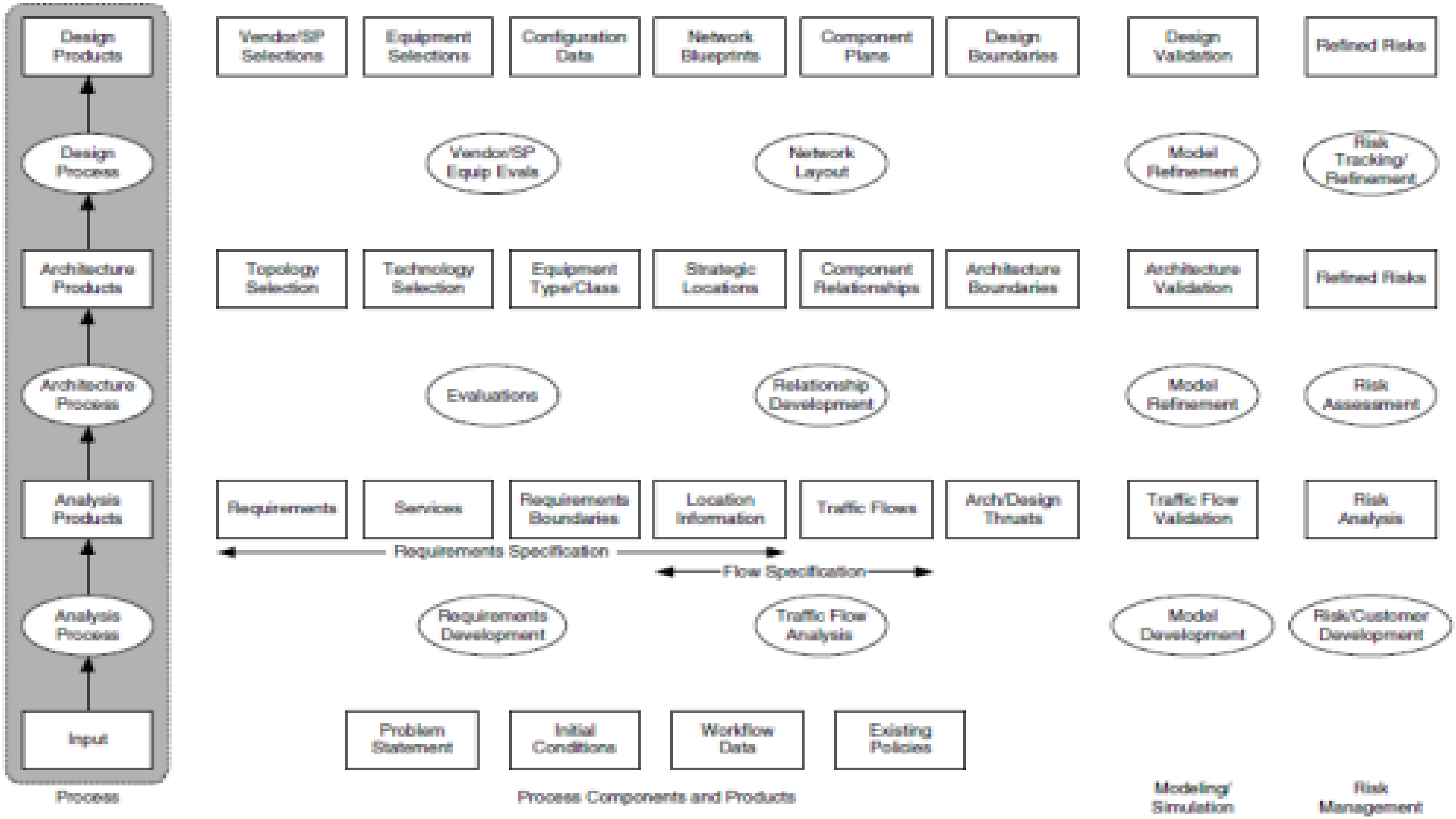


Section One
Analysis
Requirements, Flows, Risks

Section Two
Architecture
Technology and Topology Choices; Relationships within and between Network Functions

Section Three
Design
Equipment, Vendor Choices, Location Information

Designing of Internet System Network Architecture



Design Issues

- Server Design Issues:
  - Functionality
    - Handle multiple clients concurrently
    - Maintaining client-specific state at a server (usually)
      - Require fault-tolerance
  - Access control
    - Authenticate clients
    - Evaluate whether client is allowed access
    - Secure data
  - Robustness
    - Performance
    - Reliability
- If interested: Colleen Roe & Sergio Gonik, “Server-Side Design Principles for Scalable Internet Systems”.

Server

- We’ll discuss (Different types of Servers):
  - Web
  - Proxy
  - RADIUS
  - MAIL

Web Servers

HTTP

- HTTP is the way a Web server communicates with browsers.
- HTTP lets visitors view a site and send information back to the Web server un-encrypted.

HTTPS

- HTTPS runs HTTP on top of SSL/TLS (Secure Sockets Layer or Transport Layer Security).
- Communications through an HTTPS server are encrypted by a secure certificate known as an SSL that prevents third-parties from eavesdropping on communications to and from the server.
- Trade off:
  - HTTPS usage is increasing despite potential deployment costs.
  - HTTPS has a perceptible impact on clients in terms of latency.
  - Its data overhead seems to be limited.
  - It could lead to significantly increased battery consumption for large objects.

Web Servers

- Refer: Client-Server model.
- HTTP or HTTPS form the basis of web technology.
- Browsers speak HTTP and Web Servers speak HTTP.
    - Browsers (or Web Clients): send HTTP/HTTPS request and get HTTP/HTTPS responses.
    - Web Server: get HTTP/HTTPS requests and send HTTP/HTTPS responses.
- HTTP is layered on TCP/IP so a web server runs this infinite loop:
    - Accept TCP connection from browser.
    - Read HTTP request from TCP connection.
    - Process HTTP request.
    - Write HTTP response to TCP connection.
    - Shutdown TCP connection (except if Connection: keep-alive).
    - Check HTTP request.
- HTTP is connection oriented and a stateless protocol.

Web Servers

- The server can generate the response message in a variety of ways:
  - The server simply retrieves the file associated with the URL and returns the contents to the client.
  - The server may invoke a script that communicates with other servers or a back-end database to construct the response message.
- Web site and Web server are different:
  - Web site consists of a collection of Web pages associated with a particular hostname.
  - Web server is a program to satisfy client requests for Web resources.
- One web server can host multiple websites.

Web Servers

- Role of Web Servers:
  - Web servers serve various resources.
    - As file (document) servers.
    - As application front ends.
  - Other servers also provide services on the Internet, each speaking its own protocol:
    - SMTP, POP, IMAP, NNTP, FTP, etc.
  - Web server = HTTP server.
  - HTTP servers serve HTTP clients (browsers and other user agents) with the help of HTTP intermediaries (proxies).

Web Servers

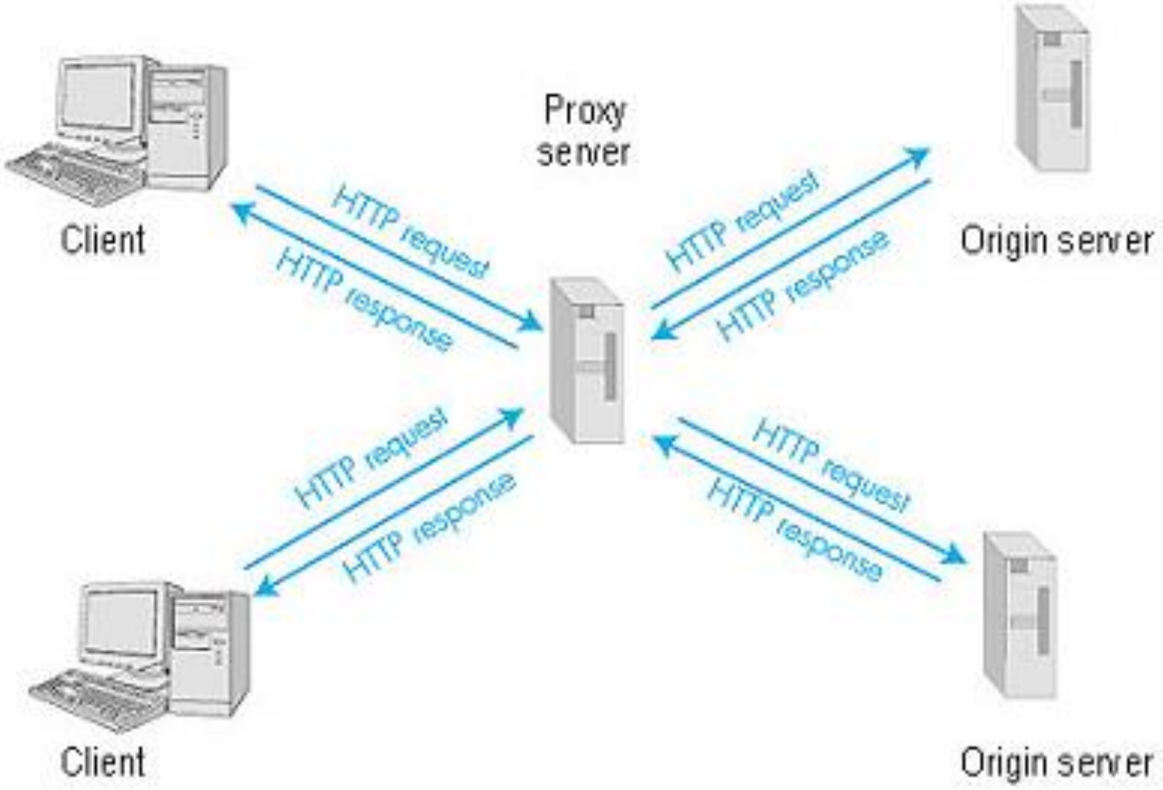
- Architecture:
    - Event – driven server architecture.
    - Process – driven server architecture.
    - Hybrid server architecture.
- Event – Driven Server Architecture
    - Has a single process that alternates between servicing different requests.
    - Allows the server to serialize operations that modify the same data.
    - Not used in most high-end Web servers.

Web Servers

- Process-driven server
  - Allocates each request to a separate process.
  - One master process listens for new connection.
  - The master process creates, or forks, a separate process for each new connection.
  - Terminates the process after parsing the client request and transmitting the response.
  - To prevent memory leak.
  - Introduces overhead for switching from one process to another.
- In Hybrid server architectures
  - The strengths of the event-driven and process-driven models are combined.
  - Each process would become an event-driven server that alternates between a small collection of requests.
  - A single process has multiple independent threads.
  - Main process instructs a separate helper process to perform time-consuming operations.
- If interested: Check out the Application Server Vs. Web Server.

Proxy Servers

- Proxy: Authority provided to do something on behalf of someone.
  - Analogy: In a class, Alice wants to pass a note to Bob. Alice -> Friend -> Bob. Alice pass a note to a friend, who passes it to Bob. Bob replies in the note and passed it to friend, who passes it back to Alice.
  - Friend is the proxy here.
- It can be a dedicated hardware or a software running in a server.
- A proxy server:
  - A network entity that satisfies HTTP requests on the behalf of a client.
  - Has its own disk storage.
  - Stores copies of recently requested objects.



Proxy Servers

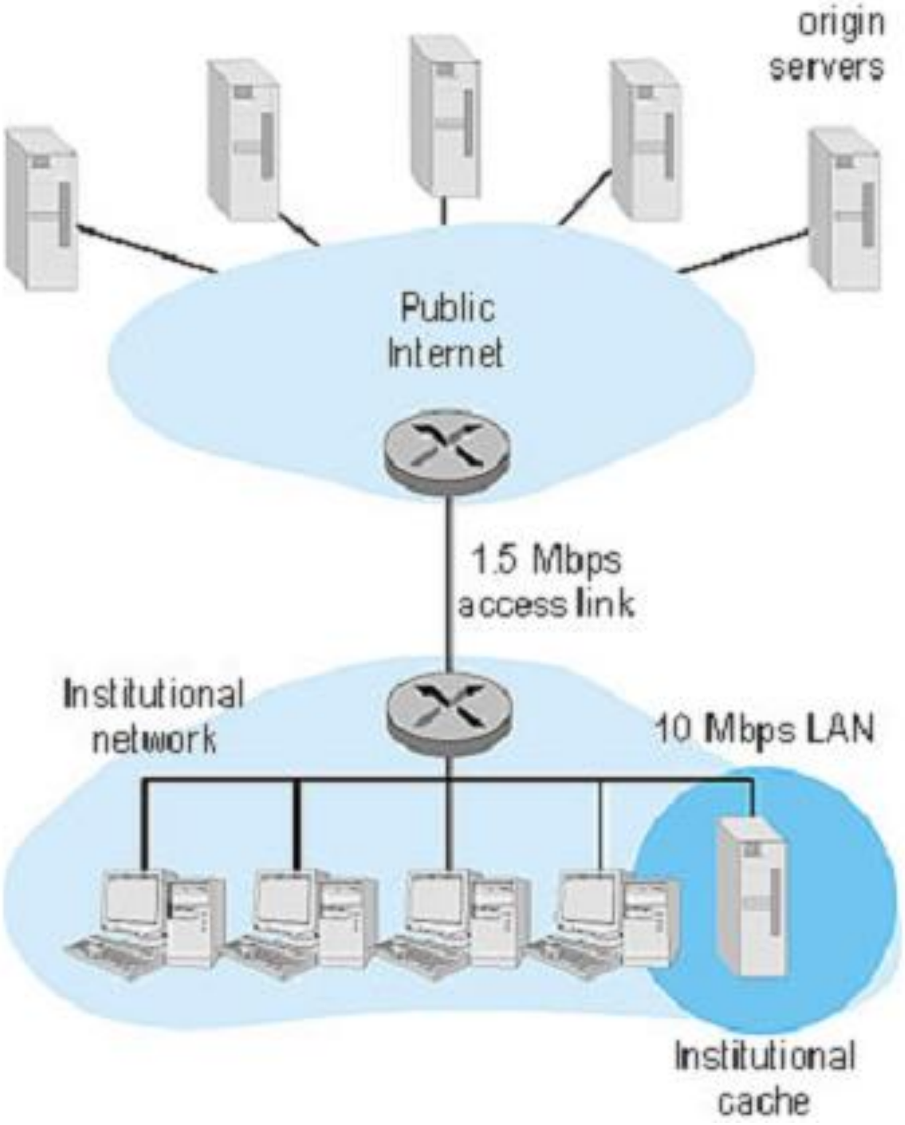
- Users configure their browsers so that all of the HTTP requests are first directed to the Web cache.
    - Each browser request is first directed to the Proxy Server (or Web cache).
- Cache is both a server and a client at the same time.
    - When it receives requests from and sends responses to a browser, it is a server.
    - When it sends requests to and receives responses from an origin server it is a client.

Why use Proxy Servers?

- They can substantially reduce the response time for a client request.
  - e.g., if the bottleneck bandwidth between the client and the origin server is much smaller.
  - If there is a high-speed connection between the client and the cache and if the cache has the requested object, then cache is able to rapidly deliver the object to the client.
- They can substantially reduces traffic on an access link to the Internet.
  - User does not have to upgrade bandwidth as quickly, thereby reducing costs.
  - Web caches can substantially reduce Web traffic in the Internet as a whole, improving performance for all applications.
    - In 1998, over 75% of the Internet traffic was WWW, so a significant reduction in Web traffic can translate into a significant improvement in Internet performance.
    - Nowadays the situation changed due to increase in the p2p traffic.
- Internet dense with proxy servers (at institutional, regional, and national levels) provides an infrastructure for rapid content distribution, even for providers who run their sites on low-speed servers behind low-speed access links.
  - If such a "resource-poor" content provider has popular content, this popular content will quickly be copied into the Internet caches, and high user demand is satisfied.

Proxy Servers

- Main objectives (incl. web caching):
  - Obscure client IP.
    - Convert IP address from a LAN to Public IP address to access a website.
    - Makes a user “anonymous”.
  - Block malicious traffic.
  - Block web sites in a LAN.
    - Facebook, Twitter, Youtube, etc.
  - Log activity.
    - Web site visited.
    - Amount of time spent on a webpage.
  - Improve performance.

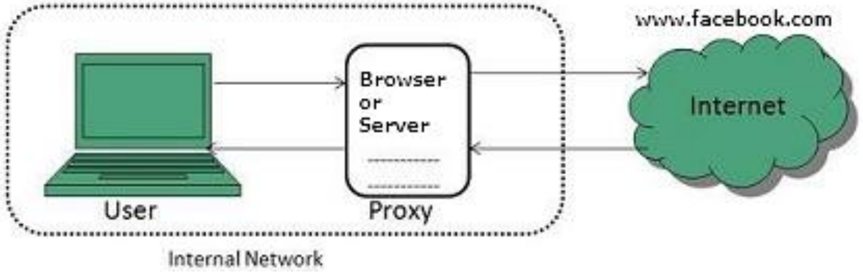


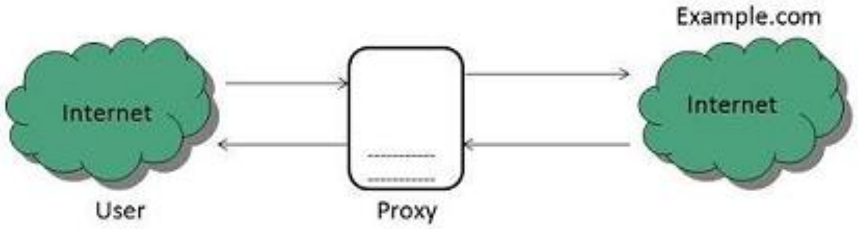
Proxy Server – Cooperative Caching

- Multiple Web caches, located at different places in the Internet, can cooperate and improve overall performance.
- Example: An institutional cache can be configured to send its HTTP requests to a cache in a backbone ISP at the national level.
  - When the institutional cache does not have the requested object in its storage, it forwards the HTTP request to the national cache.
  - The national cache then retrieves the object from its own storage or, if the object is not in storage, from the origin server.
  - The national cache then sends the object (within an HTTP response message) to the institutional cache, which in turn forwards the object to the requesting browser.
  - Whenever an object passes through a cache (institutional or national), the cache keeps a copy in its local storage.
  - The advantage of passing through a higher-level cache, such as a national cache, is that it has a larger user population and therefore higher hit rates.

Proxy Servers - Types

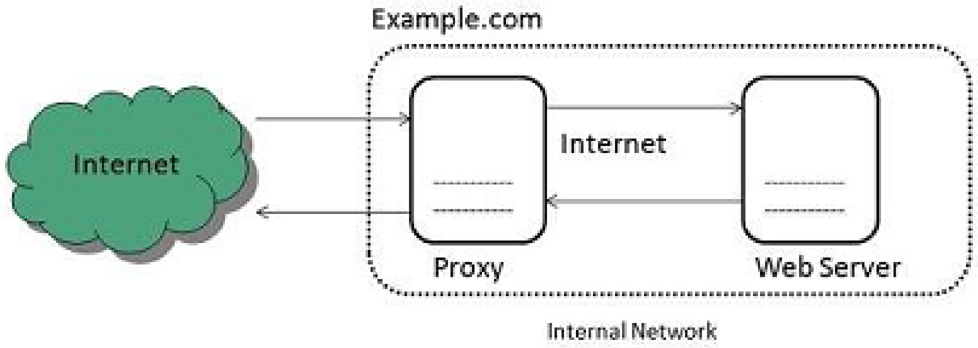
- Forward Proxy
  - Client requests its internal network server to forward to the internet.
  - Remember the proxy from your browser.
- Open Proxies
  - Helps the clients to conceal their IP address while browsing the web.
  - Widely used by spammers to send spam because the proxy hides the spammer's IP address from recipients.
  - Spammers routinely scan the Internet for vulnerable proxy servers.
  - Also used by different agencies to lure spammers (called honeyproxy).
  - All devices are configured to use closed proxy. If open proxy is used then browser sends all its web content requests to proxy rather than the URL being resolved to an IP address and web request being sent to the server.
  - Open proxy does the DNS name resolution, connects to destination web site, and returns the content to browser.
  - If end user attempts to access a blocked site through open proxy, the name of the site is encoded in the request, and the content filter works as if the browser wasn’t configured to use an open proxy.





Proxy Servers - Types

- Reverse Proxy
  - **Encryption / SSL acceleration** – SSL encryption with SSL acceleration hardware for secure website.
  - **Load Balancing** – distribute load to several web servers, each web server serving its own application area ,translation of externally known URLs to internal locations.
  - **Cache static content** – offload web servers by caching static content & benefits dynamically generated pages. (Remember Web Caching).
  - **Compression** – can optimize & compress web content to speed up load time.
  - **Security** – additional layer of defense and can protect against some OS & Web Server attacks but web application or service.
  - **Extranet Publishing** – providing extranet access to some functions while keeping servers behind firewall.

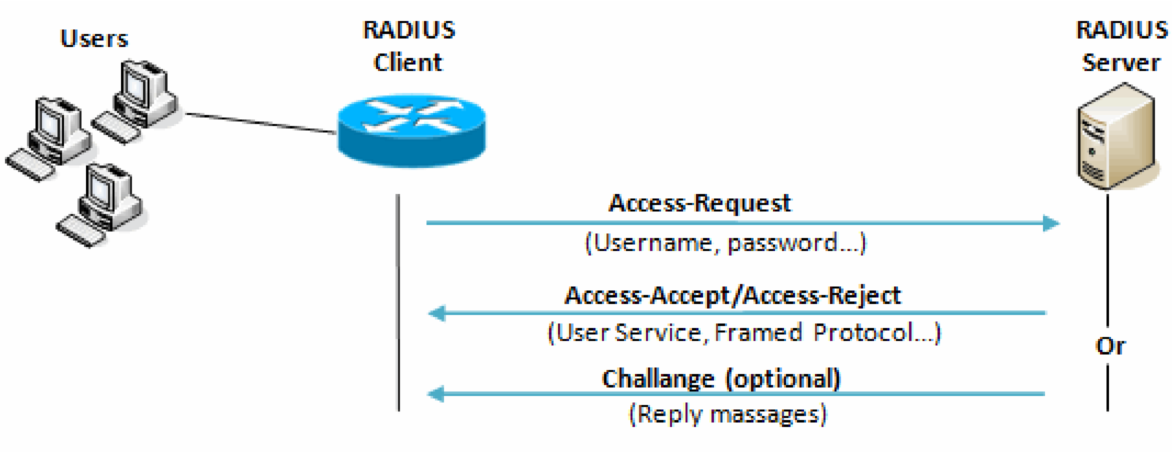


RADIUS

- Remote Authentication Dial In User Service (RADIUS).
- A central authentication and authorization service for all access requests that are sent by RADIUS clients.
- A central accounting recording service for all accounting requests.
- Uses UDP - ports 1812 for Authentication & 1813 for Accounting.
- AAA transaction.
  - Authentication & Authorization - RFC 2865.
  - Accounting - RFC 2866.
- RADIUS is a network protocol - a system that defines rules and conventions for communication between network devices - for remote user authentication and accounting.
  - Commonly used by Internet Service Providers (ISPs), cellular network providers, and corporate and educational networks, the RADIUS protocol serves three primary functions:
    - Authenticates users or devices before allowing them access to a network
    - Authorizes those users or devices for specific network services
    - Accounts for and tracks the usage of those services
- Check http://networkradius.com/doc/FreeRADIUS%20Technical%20Guide.pdf for further reference

RADIUS

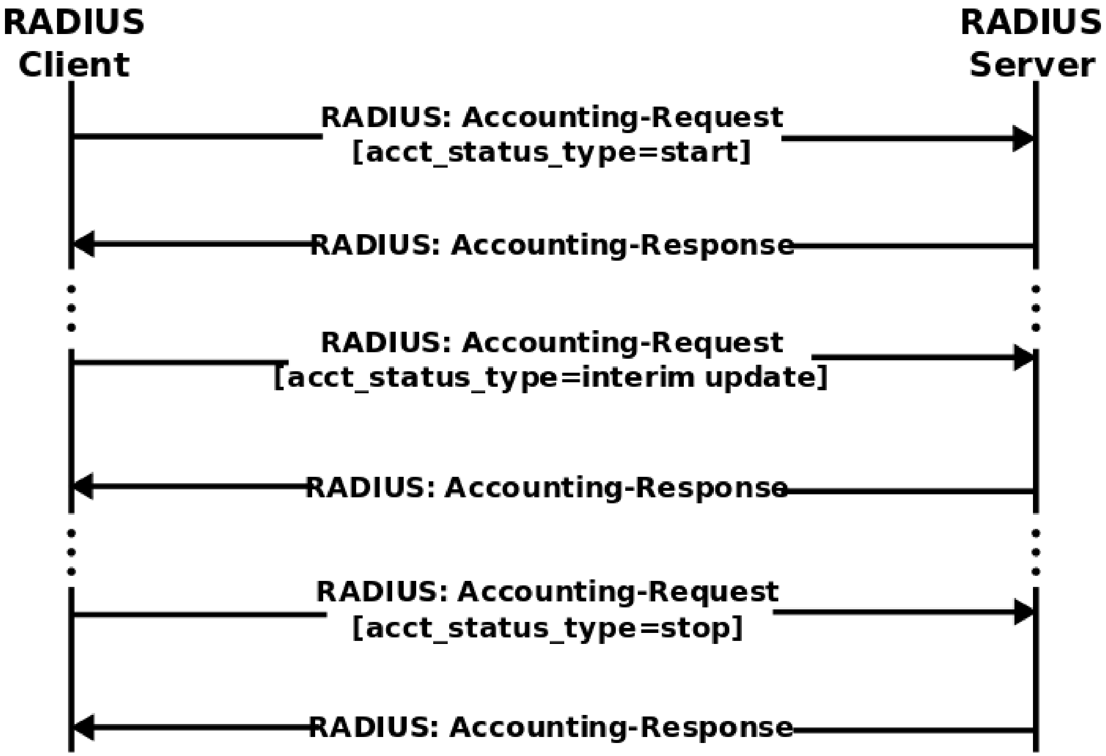
- AAA transaction: **Authentication & Authorization**.
- User sends a request to a Remote Access Server (RAS) to gain access.
  - Credentials sent via link-layer protocol (eg. PPP in dialup or DSL) or posted in HTTPS.
- RAS sends a RADIUS Access Request to RADIUS server, requesting authorization.
  - RADIUS server uses authentication schemes like PAP, CHAP.
  - RADIUS server refers to local log file or external sources - SQL, Kerberos, Lightweight Directory Access Protocol (LDAP), or Active Directory servers - to verify the user's credentials.
- The RADIUS server then returns one of three responses to the RAS:
  - Access Reject.
  - Access Challenge.
  - Access Accept.



RADIUS Authentication and Authorization Flow

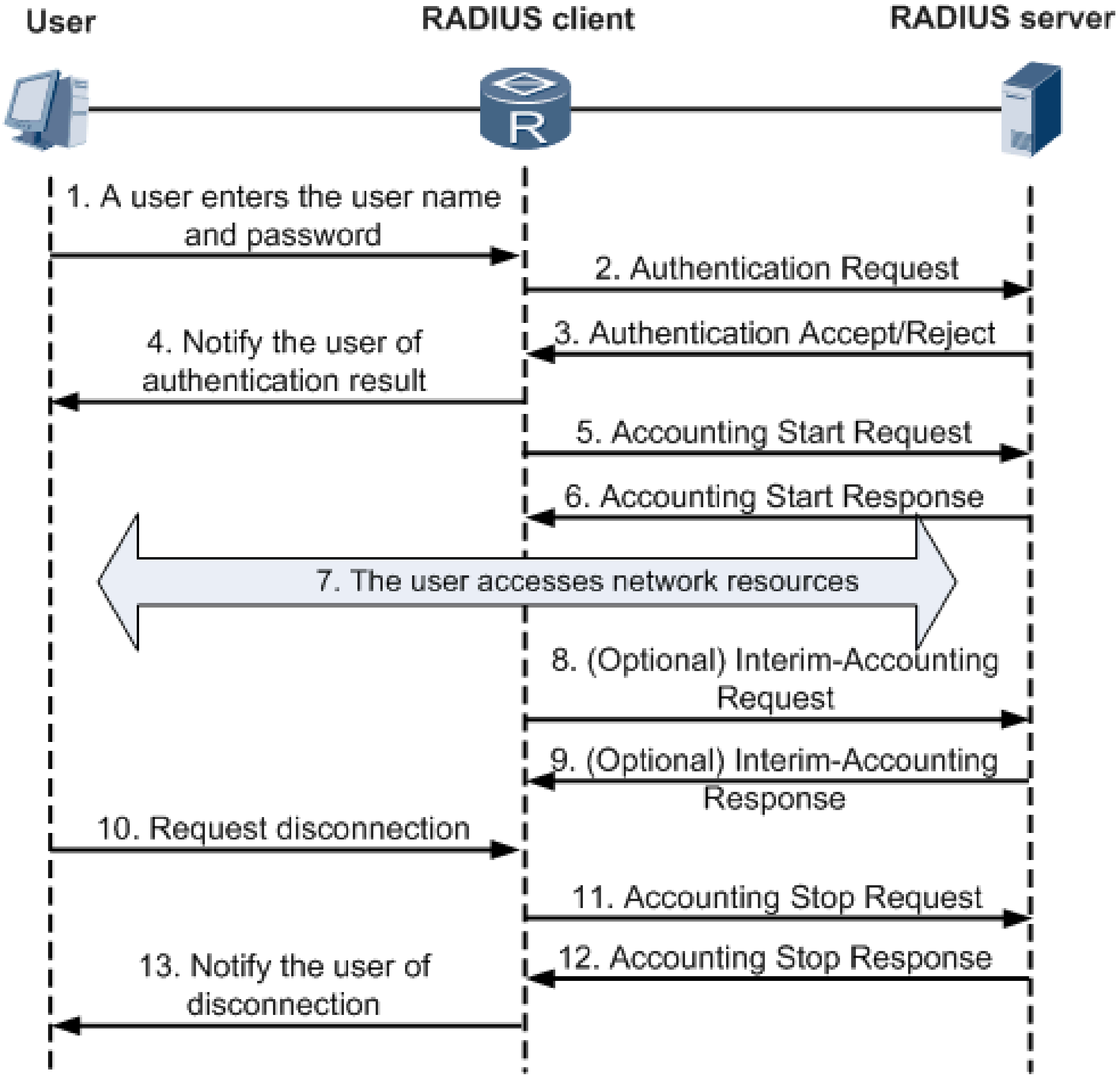
RADIUS

- AAA transaction: **Accounting**
- After network access is granted to user by Network Access Server (NAS), Accounting Start is sent by the NAS to the RADIUS server to signal the start of the user's network access.
  - “Start” records - user's identification, network address, a unique session identifier.
- NAS may send Interim Update records to the RADIUS server to update it on the status of an active session.
  - “Interim” records - current session duration , information on current data usage
- NAS issues a final Accounting Stop record to the RADIUS server.
  - “Stop” records - final usage time, packets transferred, data transferred, reason for disconnect & other information related to the user's network access



RADIUS Client
RADIUS Server
RADIUS: Accounting-Request [acct_status_type=start]
RADIUS: Accounting-Response
RADIUS: Accounting-Request [acct_status_type=interim update]
RADIUS: Accounting-Response
RADIUS: Accounting-Request [acct_status_type=stop]
RADIUS: Accounting-Response

RADIUS

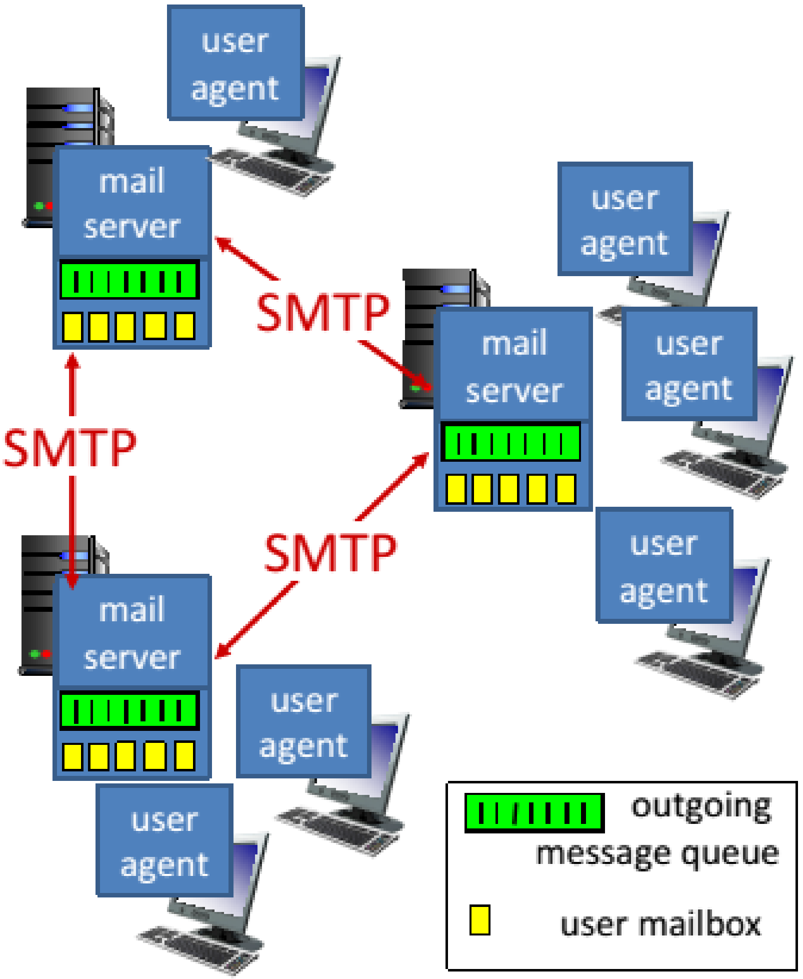

User
RADIUS client
RADIUS server
1. A user enters the user name and password
2. Authentication Request
3. Authentication Accept/Reject
4. Notify the user of authentication result
5. Accounting Start Request
6. Accounting Start Response
7. The user accesses network resources
8. (Optional) Interim-Accounting Request
9. (Optional) Interim-Accounting Response
10. Request disconnection
11. Accounting Stop Request
12. Accounting Stop Response
13. Notify the user of disconnection

Mail Server

Acronym	Meaning	Definition
MUA	Mail User Agent	The program that allows the user to read and send email.
MSA	Mail Submission Agent	The program that receives emails from MUA and cooperates with MTA for delivery of the emails.
MTA	Mail Transfer Agent	The program in charge of receiving and delivering mails to users.
SMTP	Simple Mail Transfer Protocol	SMTP is a communication protocol for mail servers to transmit emails over the internet.
SASL	Simple Authentication & Security Protocol	SASL is the mechanism is framework for providing authentication and data security services in connection- oriented protocols.
LMTP	Local Mail Transfer Protocol	LMTP is designed as an alternative to normal SMTP for situations where the receiver has no mail queue. (like mail storage server)
LDA	Local Delivery Agent	another name for MDA when the email is delivered locally.
MDA	Mail Delivery Agent	The program responsible for the delivery of emails to a recipients.
IMAP	Internet Mail Access Protocol	A protocol allowing a client to access and manipulate email on the mail server.
POP3	Post Office Protocol 3	POP3 is a protocol for receiving and holding email on remote mail server over network.

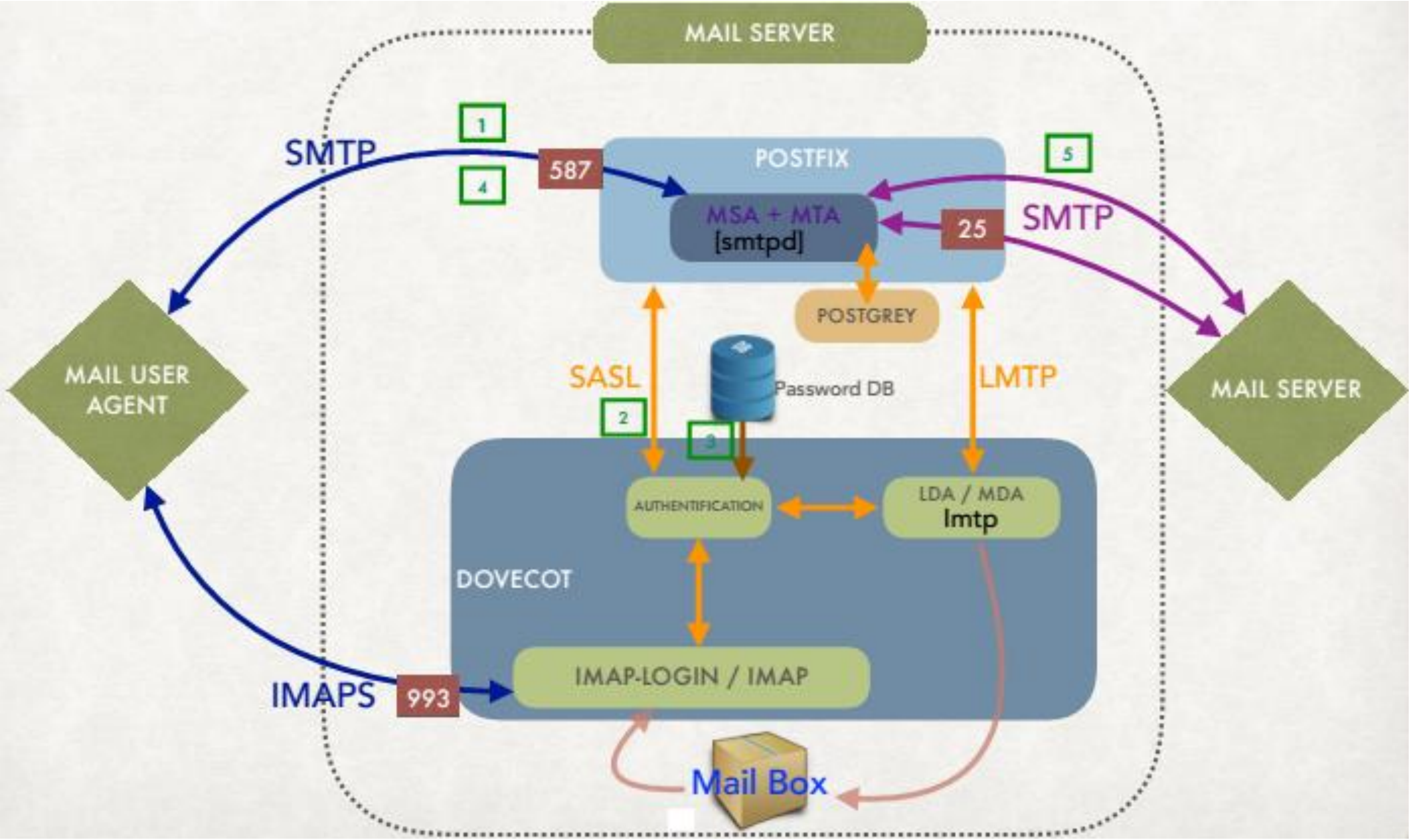
Mail Server

- Recall: SMTP, POP or POP3, and IMAP from Application layer.
- Three major components:
  - Mail user agent (MUA)
  - Mail transfer agent (MTA)
  - Simple mail transfer protocol: SMTP
- Mail User Agent
  - “mail reader”.
  - Composing, editing, reading mail messages.
  - E.g. Outlook, Thunderbird, iPhone mail client.
  - outgoing, incoming messages stored on server.
- Mail Transfer Agent:
  - Mailbox contains incoming messages for user.
  - Message queue of outgoing (to be sent) mail messages.
- SMTP protocol between mail servers to send email messages (one-way).
  - client: sending mail server
  - “server”: receiving mail server



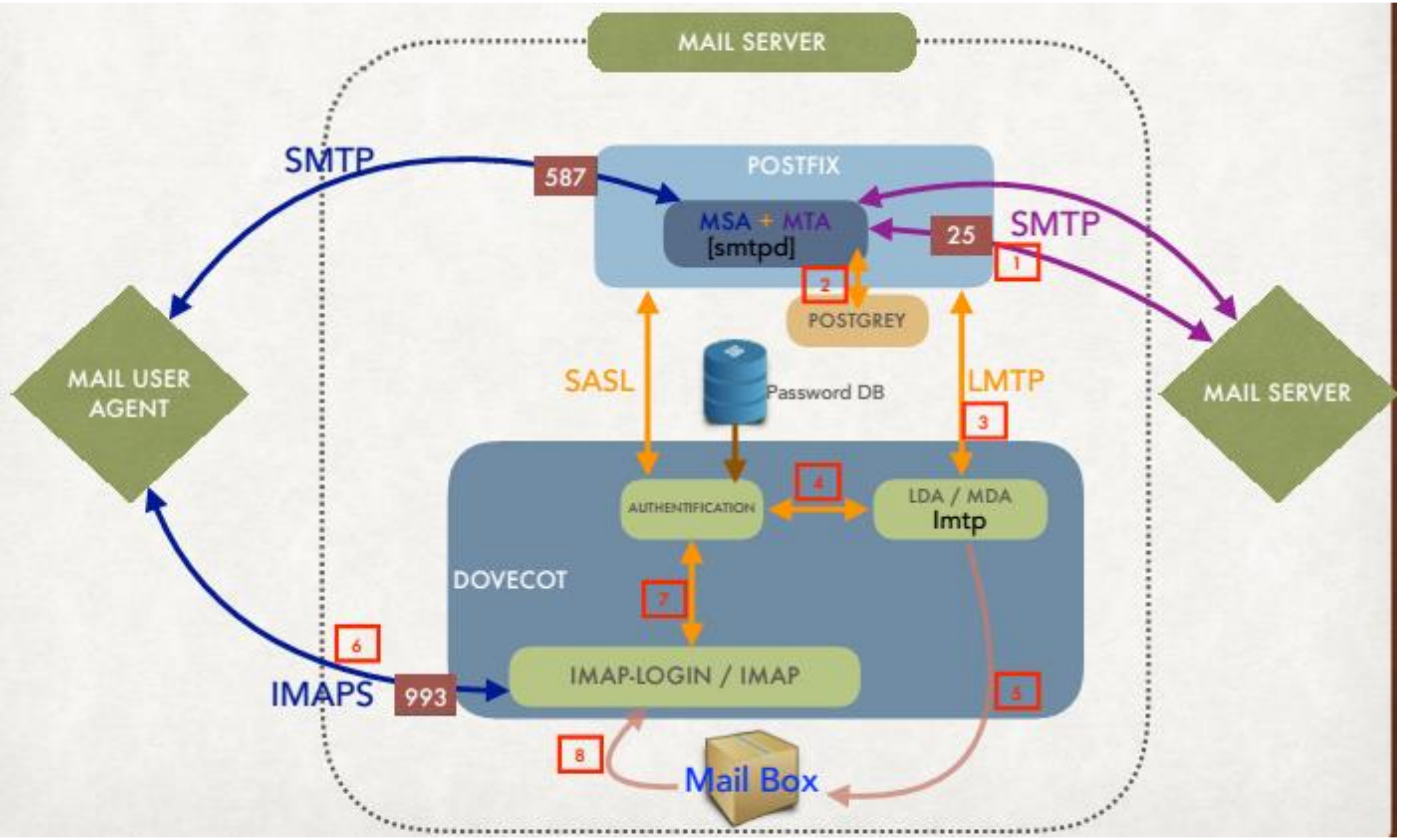
Mail Server

- Sending:



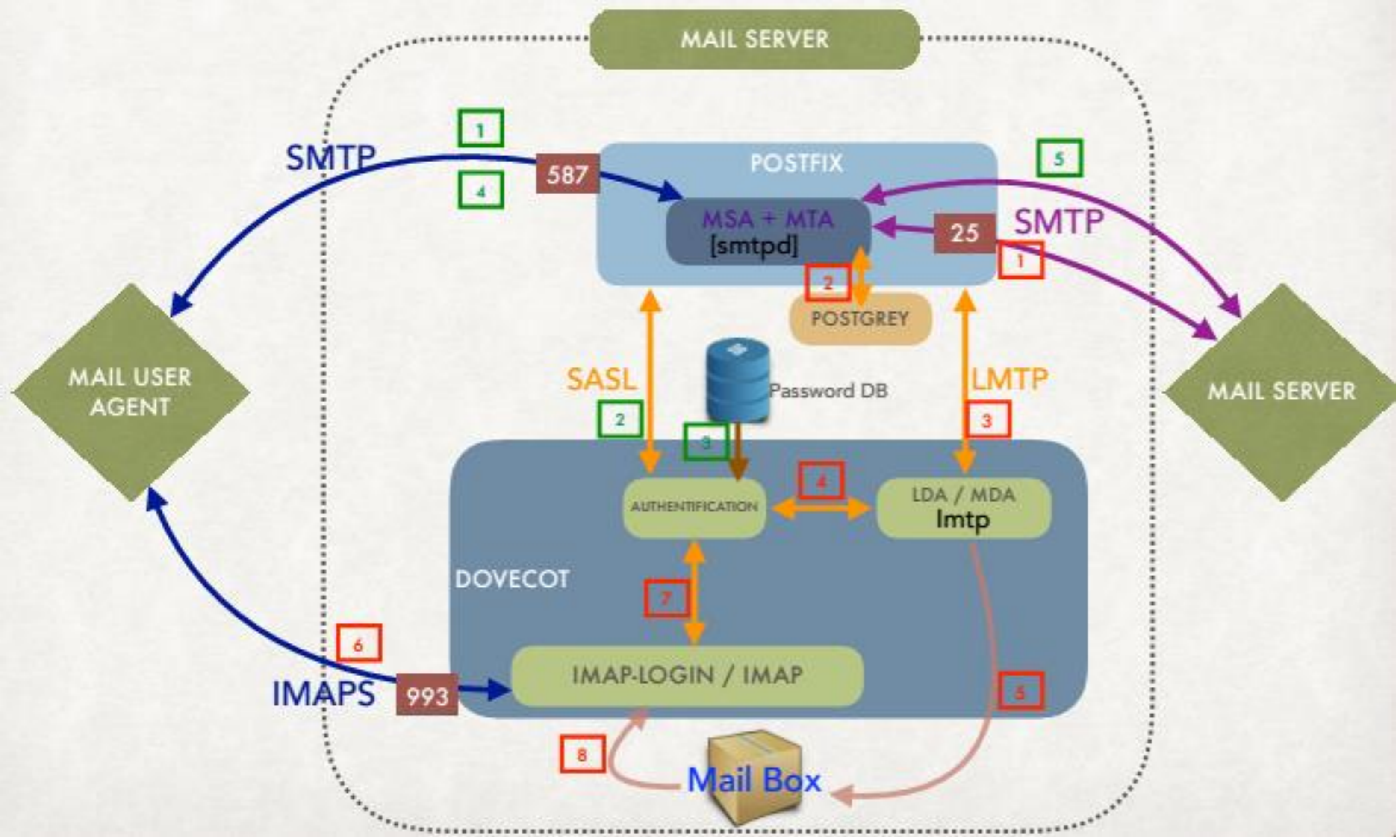
Mail Server

- Receiving:



Mail Server

- Sending/Receiving:



Mail Server

- Always on, because they always need to be ready to accept mail.
- Usually owned by ISP
- You use the email server for DWIT to send official emails.
- Outbound Mail
    - SMTP for outbound email
        - Port 25 or 2525
- Inbound Mail
    - POP3 for inbound email
        - Port 110
    - IMAP for inbound email
        - Port 143

Cookies

- Small, often encrypted text files, sent by website’s server & residing in browser directories.
- When same website is revisited, the website retrieves the data stored in the cookie & notify the website of the user's previous activity.
- Cookies remember the state of the website or user activity in previous browsing – clicking particular buttons, logging in, or a record of pages visited, user online behavior.
- **Tracking cookies** & **Third-party cookies** compile individuals' browsing history & habits - a major privacy concern.
- Authentication cookies
  - Used by web servers to know if the user is logged in or not & which account the user is logged in under.
  - Security of an authentication cookie generally depends on the security of the issuing website and the user's web browser.

Cookies

- Used for:
  - Session mgmt.
    - To implement “shopping cart” with unique session identifier
    - To maintain data related to the user during navigation
  - Personalization
    - To show relevant content in the future eg. username used for login
    - User preferences eg. skin & themes
  - Tracking
    - To track internet users' web browsing habits
- Drawbacks
  - Privacy concerns
  - Inaccurate identification
    - Browsers in same computer maintain own cookies
    - Multiple users using the same computer, user name & browser
  - Inconsistent state on client and server
    - E.g. if the user presses a button to add an item in a shopping cart and then clicks on the "Back" button, the item remains in the shopping cart

Load Balancing – Proxy Arrays

- Load Balancing
  - **Problem**: Single physical Origin or Proxy Server may not be able to handle its load.
  - **Solution**: Install multiple servers and distribute the requests.
- How do we distribute requests among the servers?
  - DNS Round Robin
    - DNS is configured so multiple IP Addresses correspond to a single host name.
    - multiple type “A” records in DNS Database.
      - A harpo 10.0.0.15
      - A harpo 10.0.0.16
      - A harpo 10.0.0.17
    - Modify the DNS server to round-robin through the IP addresses for each new request.
    - This way, different clients are pointed to different servers.

Load Balancing – Proxy Arrays

- Problems with DNS Round Robin
  - Not optimal for proxy servers
  - cache content is duplicated
  - multi-tier proxy arrangement won’t work if cookies are used
  - load is not truly balanced
  - Assignment is at DNS lookup level, not HTTP request level
- How do we distribute requests among the servers?
  - Weighted round robin with response-time as weight.
    - An enhancement of the round robin method.
    - Response times for each server are constantly measured to determine which server will take the next connection/session.
  - Fewest connections with limits.
    - Determines which server gets the next connection by keeping a record of how many connections each server is currently providing.
    - The server with fewer connections gets the next request.

Load Balancing – Proxy Arrays

- Internet Cache Protocol (ICP).
  - Used for querying proxy servers for cached documents.
  - Typically used by proxy servers to check other proxy server’s cache.
  - Could be used by clients however.
  - RFC 2186, 2187.
  - ICP request has desired URL in it.
- Problems with ICP.
  - ICP queries generate extra network traffic.
  - Does not scale well.
    - more proxy servers = more querying.
  - Caches become redundant.
- Non-redundant Proxy Load Balancing.
  - Proxy selection based on a hash function.
  - Hash value is calculated from the URL.
  - Use resulting hash value to choose proxy.
  - Use Host name in hash function to ensure request routed to same proxy server.

Load Balancing – Proxy Arrays

- Other techniques:
  - Cache Array Routing Protocol (CARP): Reading assignment for students.

Server Setup & Configuration Guidelines

- Basic guidelines:
  - Choose the platform i.e. Windows Vs. UNIX/Linux.
  - Always read the “Installation Guidelines” doc.
  - Always read the “Readme.<some_extension>” file.