Traffic Flow Analysis

Joao.Neves@fe.up.pt

Traffic Flow Analysis

- Flow analysis is the process of characterizing traffic flows for a network: where they are likely to occur and what levels of performance they will require.
- Flow analysis provides:
  - An end-to-end perspective on requirements and shows where requirements combine and interact;
  - Some insight into the degrees of hierarchy and diversity needed in the architecture and design;
  - Information that can be useful in choosing interconnection strategies, such as switching, routing, or hybrid solution.

Objectives

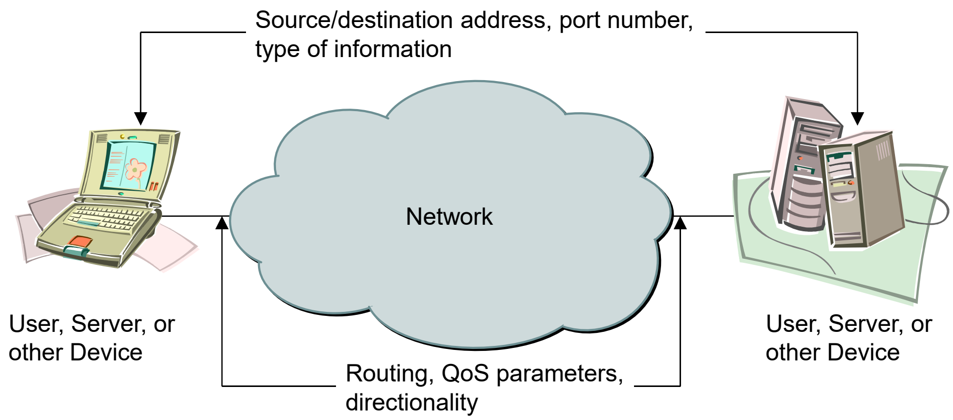
- The intent of flow analysis is not to show all possible flows in a network;
- But identifying and characterizing the flows that will have the greatest impact on network architecture and design (these are usually a small part of the total set of flows for a network).

Flow Characteristics

The concept of flow (aka traffic flow or data flow) for an end-to-end connection, has constant characteristics:

- Source/destination address
- Port number
- Type of information
- Service requirements
- Directionality
- Performance characteristics

Flow Characteristics

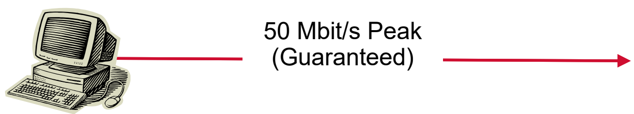


Flow Characteristics

Common Flow Characteristics	
Performance Requirements	Capacity (e.g., Bandwidth)
	Delay (e.g., Latency)
	Reliability (e.g., Availability)
	Quality of Service Levels
Importance/ Priority Levels	Business/Enterprise/Service Provider
	Political
Other	Directionality
	Common Sets of Users, Applications, Devices
	Scheduling (e.g., Time-of-Day)
	Protocols Used
	Addresses/Ports
	Security/Privacy Requirements

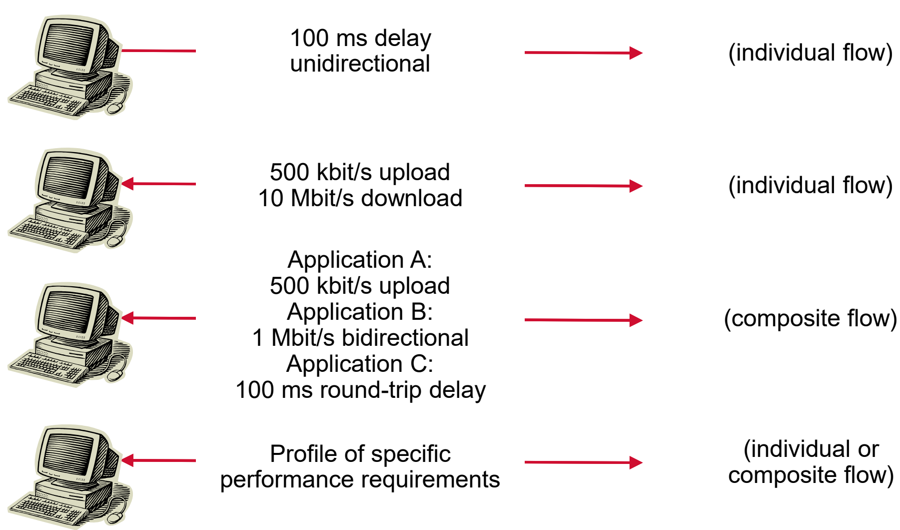
Types of Flows

- Individual: is the flow for a single session of an application (e.g., a single application flow with guaranteed requirements);

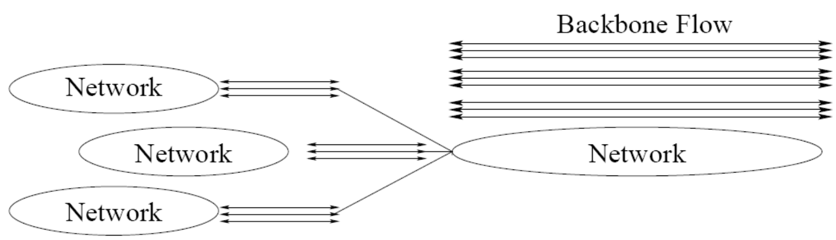


- Composite: is a combination of requirements from multiple applications, or of individual flows, that share a common link, path, or network;
- Backbone: is a combination of several composite flows when the network has a certain level of hierarchy.

Flow Examples



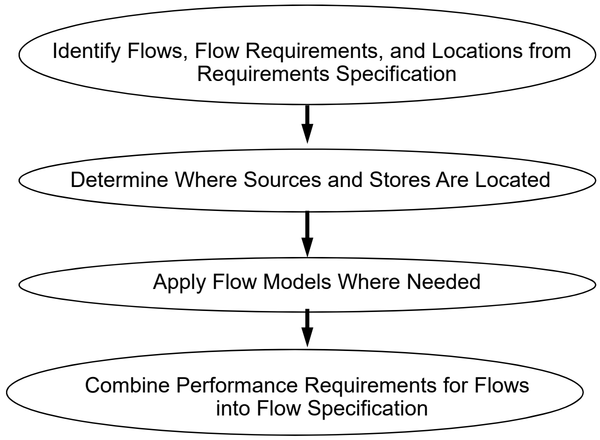
Backbone Flows



Flows and Design

- In the architecture and design of the network the majority of the flows don’t have high performance requirements, are best-effort;
- The few flows that require high, predictable, or guaranteed performance are the ones that drive the architecture and design from a service (capacity, delay, and RMA) perspective;
- All best-effort flows drive the architecture and design from a capacity perspective.

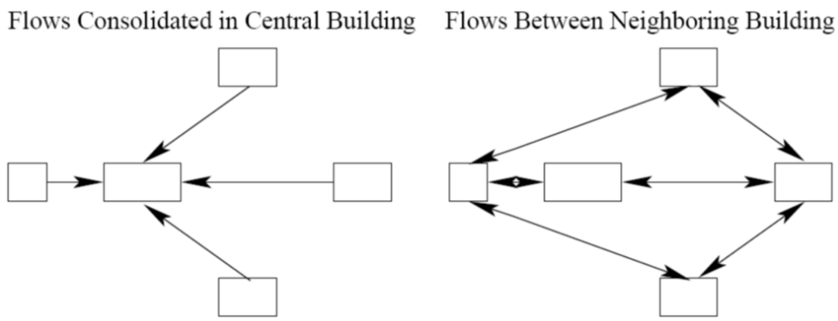
Identifying and Developing Flows



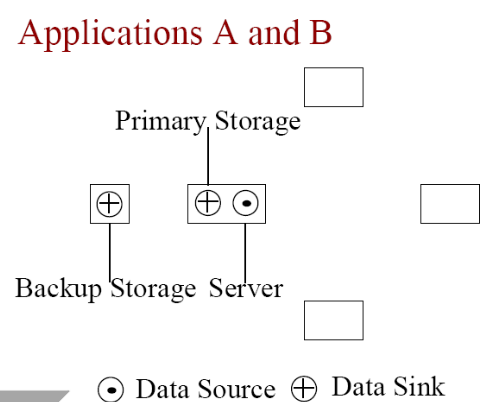
Data Sources and Stores

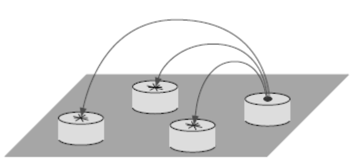
- Map of applications is not enough to identify the data flow, whether the applications are restricted to certain locations or not;
- A method of identifying flows in a network is determining where are the sources and the destinations of data;
- A *data source* generates a traffic flow (e.g. computing servers, cameras);
- A *data sink* or *data store,* terminates a traffic flow (e.g. data storage).

Flows

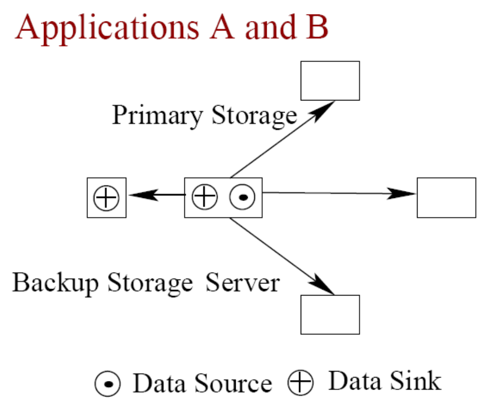


Data Sources and Stores





Flows, Data Sources and Stores



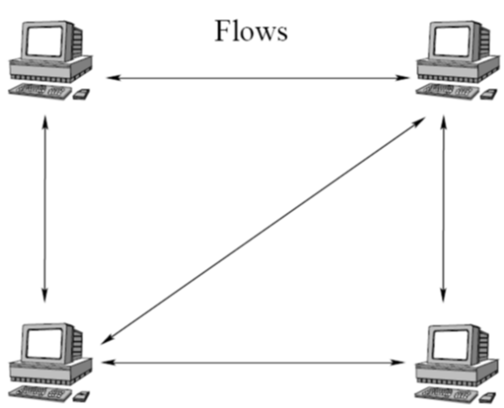
Flow Models

- Flow models are groups of flows that exhibit specific, consistent behavior characteristics;
- Directionality, hierarchy, and diversity are the primary characteristics of flow models
  - Peer-to-peer
  - Client–server
  - Hierarchical client–server (cooperative computing)
  - Distributed computing

Peer-to-Peer

- Users and applications have same type of flow behavior;
- Users and applications are peers, in that they act at the same level in the hierarchy and there is no specific directionality;
- The peer-to-peer flow model is our default when we do not have any other information about the flows in our network;
- Basically, anywhere devices communicate directly with each other is considered peer-to-peer;
- Teleconference is a typical peer-to-peer flow.

Peer-to-Peer



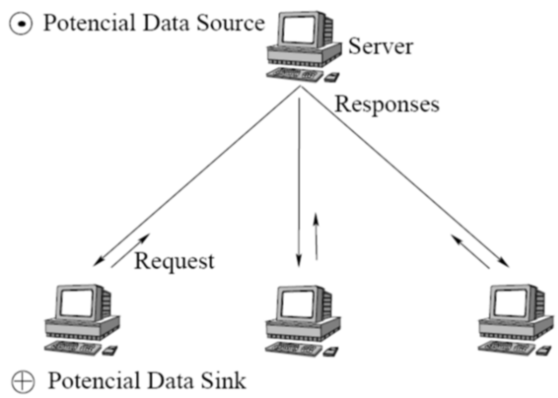
Traffic Flow for Voice over IP

- The flow associated with transmitting the audio voice is separate from the flows associated with call setup and teardown
  - The flow for transmitting the digital voice is essentially peer-to-peer;
  - Call setup and teardown is a client/server flow
    - A phone needs to talk to a server or phone switch that understands phone numbers, IP addresses, capabilities negotiation, and so on.

Client–Server

- The client–server flow model is currently the most generally applicable model;
- This model has both directionality and hierarchy;
- The flows are bidirectional, in the form of requests and responses, but asymmetric and hierarchically focused toward the client;
- Requests tend to be small relative to responses.

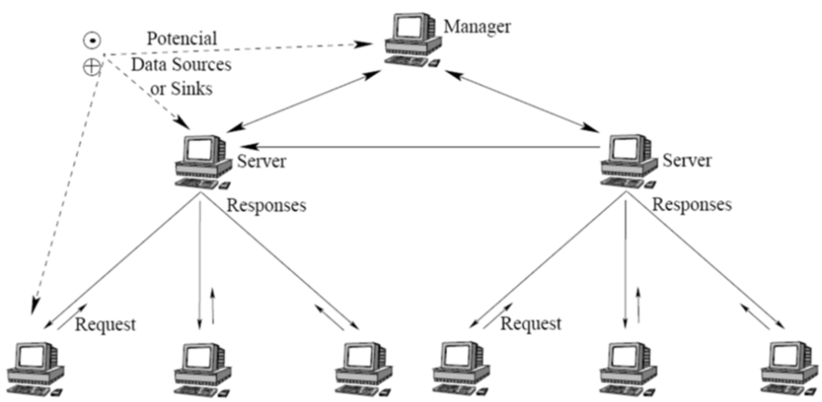
Client–Server



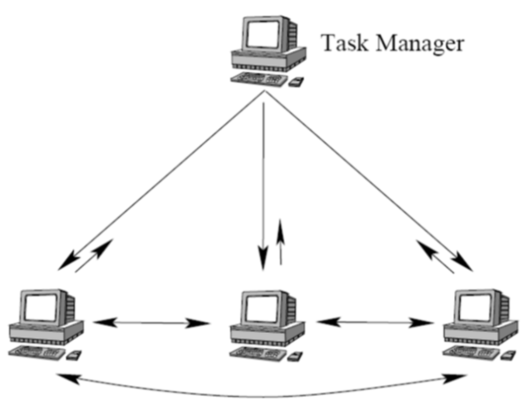
Hierarchical Client–Server

- As the flows within a client–server model become more hierarchical, in terms of adding layers, or tiers, then their behavior can be represented as a hierarchical client–server flow model;
- With the additional layers of hierarchy in this model, the servers can be either data sources or sinks (or both);
- These flows (server-to-server and server-to-manager) may be considered critical, in addition to the server-to-client flows;
- A hierarchical client–server flow model is indicated when multiple applications work together and share information to accomplish a task.

Hierarchical Client–Server



Distributed-Computing



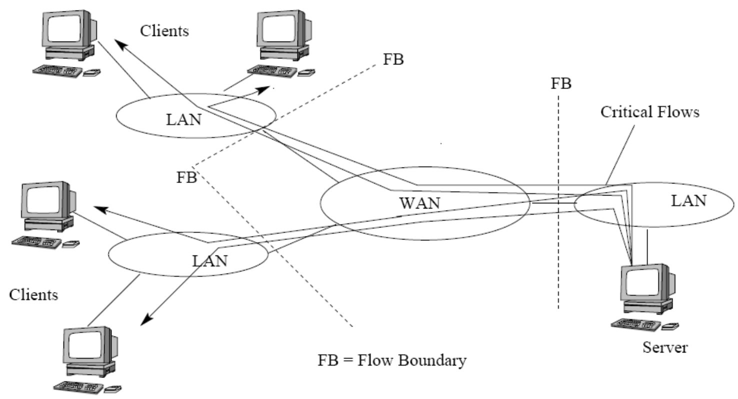
Geographical Boundaries of Flows

- Local Area Networks and Wide Area Networks (LAN/WAN)
- Local Area Networks and Metropolitan Area Networks (LAN/MAN)
- Metropolitan Area Networks and Wide Area Networks (MAN/WAN)
- Multiple Campus
- Multiple buildings in Campus
- Multiple floors in a building

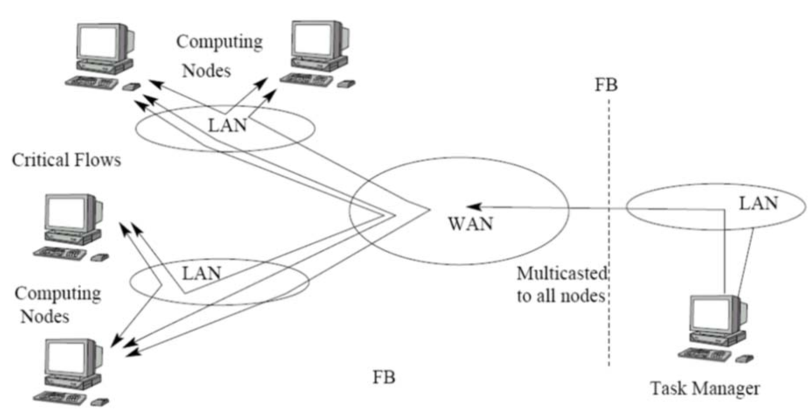
Logical Boundaries of Flows

- Logical boundaries of flows are where the responsibility or authority of information changes ownership, e.g.:
  - Backbones intra areas;
  - Flows concentration points;
  - WAN access with more than one ISP;
  - Specialized areas, with special requirements.

Client–Server Flow Boundary



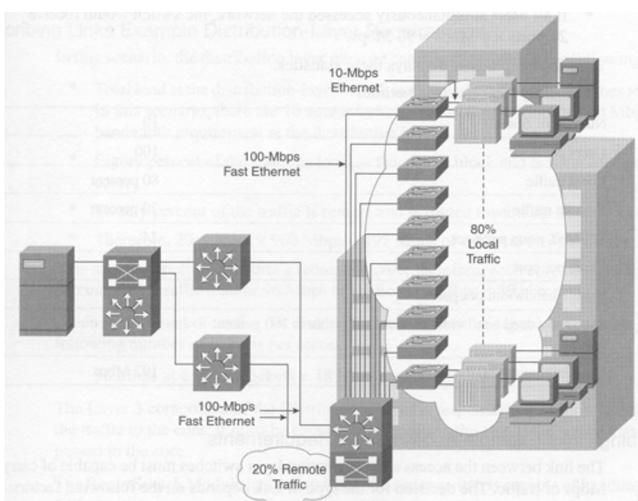
Distributed-Computing Flow Boundary



Flows Distribution

- The traditional distribution of flows is based on the 80/20 rule where 80 % of the traffic is limited on the local network and 20 % is exchanged with the outside;
- The 80/20 rule admits as assumptions that users are logical and physically close to the resources they use;
- With virtual networks and virtual private networks the users have access to resources now located outside de local network, and therefore the 80/20 rule is no longer valid.

Flows Distribution



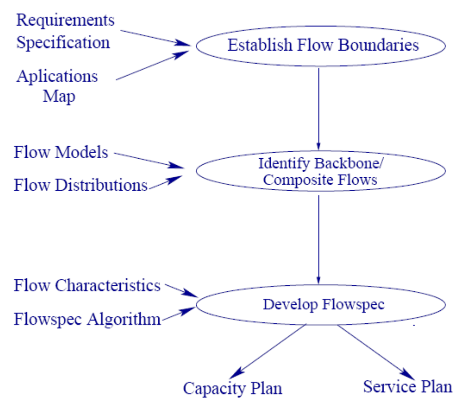
Flows Specification

- *One-part* flow specification, used for capacity planning, describes flows that have only best-effort requirements;
- T*wo-part* flow specification describes flows that have predictable requirements and may include flows that have best-effort requirements;
- *Multi-part* flow specification describes flows that have guaranteed requirements and may include flows that have predictable and/or best-effort requirements.

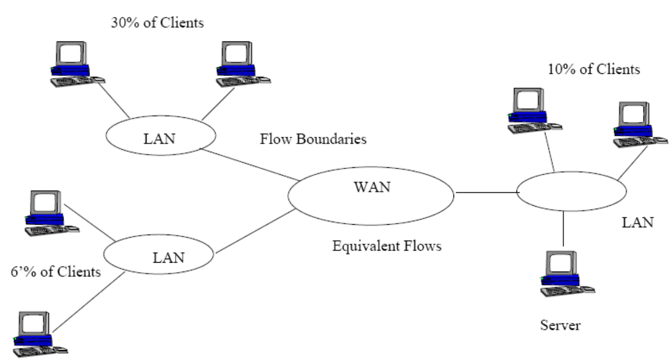
Algorithm Flows Specification

- For best-effort type flows it is not possible to specify reliability, or delay requirements, only capacity will be considered in the calculations;
- For specified flows all specified characteristics are used in calculations;
- When the delay or guaranteed reliability are part of the requirements these will be used individually in the calculations;
- Capabilities generated from flows do not reflect any performance modifier.

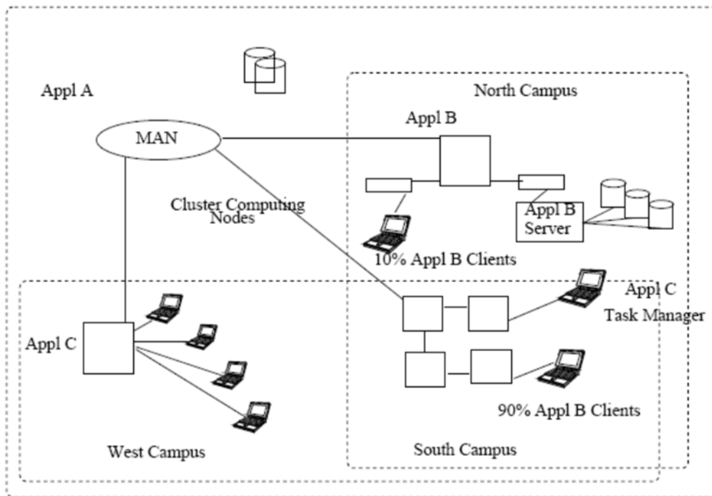
Flow Analysis



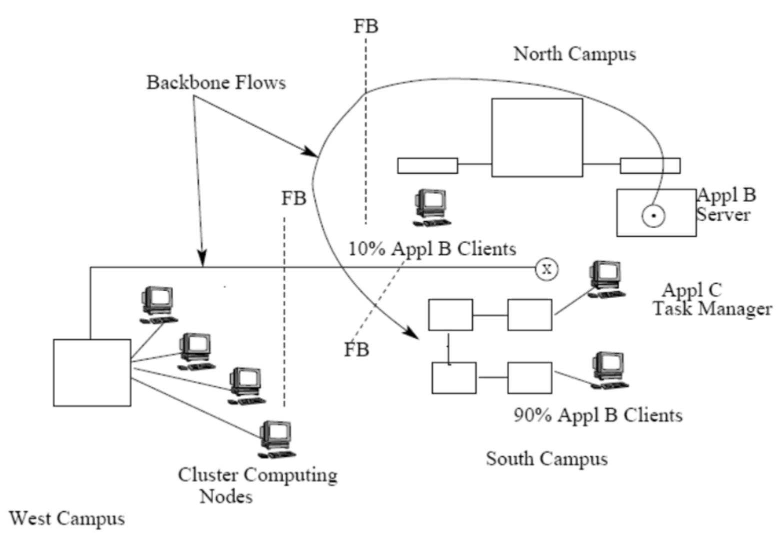
Client–Server Flows Distribution



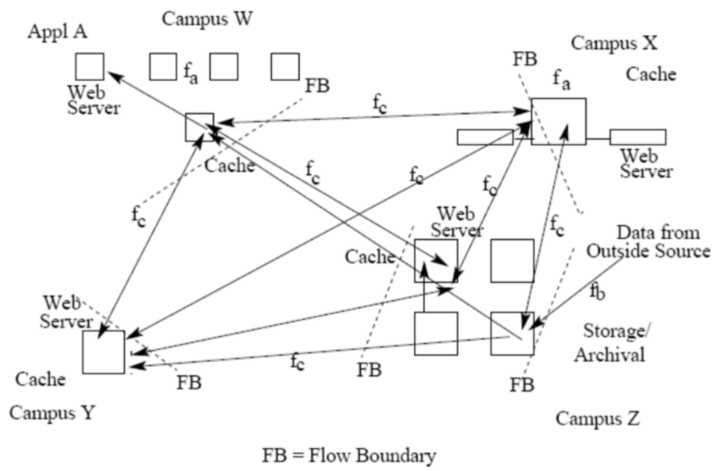
MAN environment example



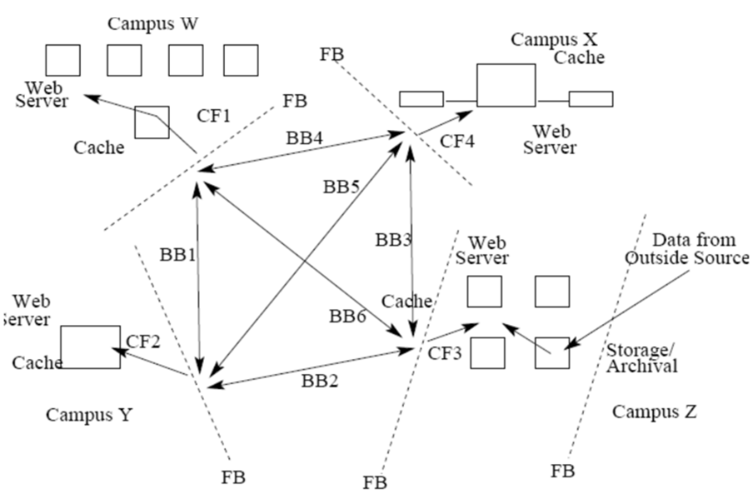
Flows in the MAN example



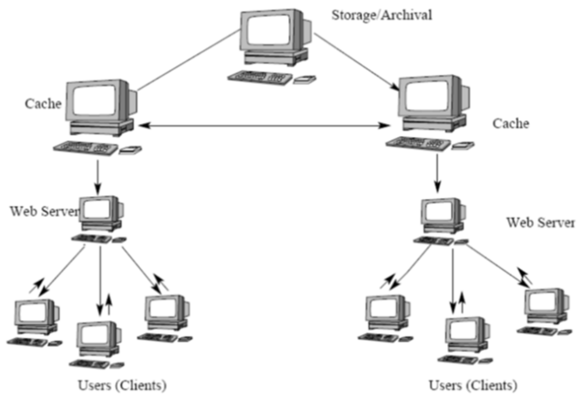
Applications Flows



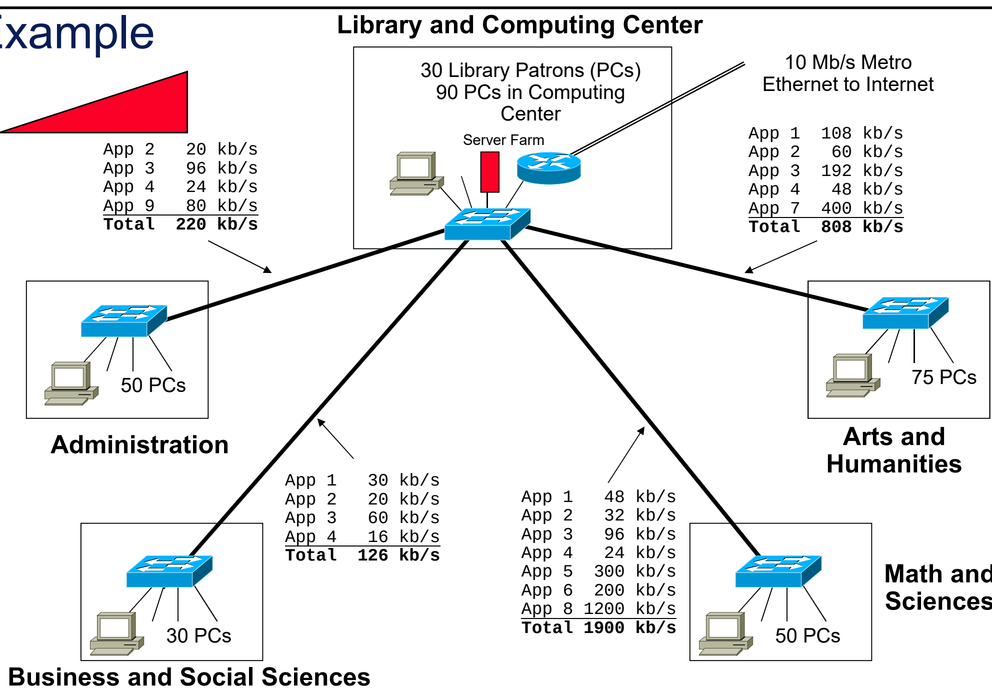
Backbone Flows



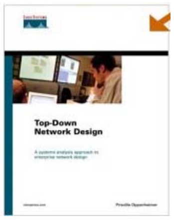
Flows Model



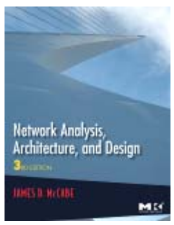
Example



Bibliography



• **Oppenheimer, Priscilla**
Top-Down Network Design
3rd Ed., Cisco Press
ISBN-13: 978-1-58720-283-4
ISBN-10: 1-58720-283-2



• **McCabe, James D.**
Network Analysis, Architecture and Design
3rd Ed., The Morgan Kaufmann Series in Networking
ISBN 978-0-12-370480-1
eBook ISBN: 978-0-08054-875-3