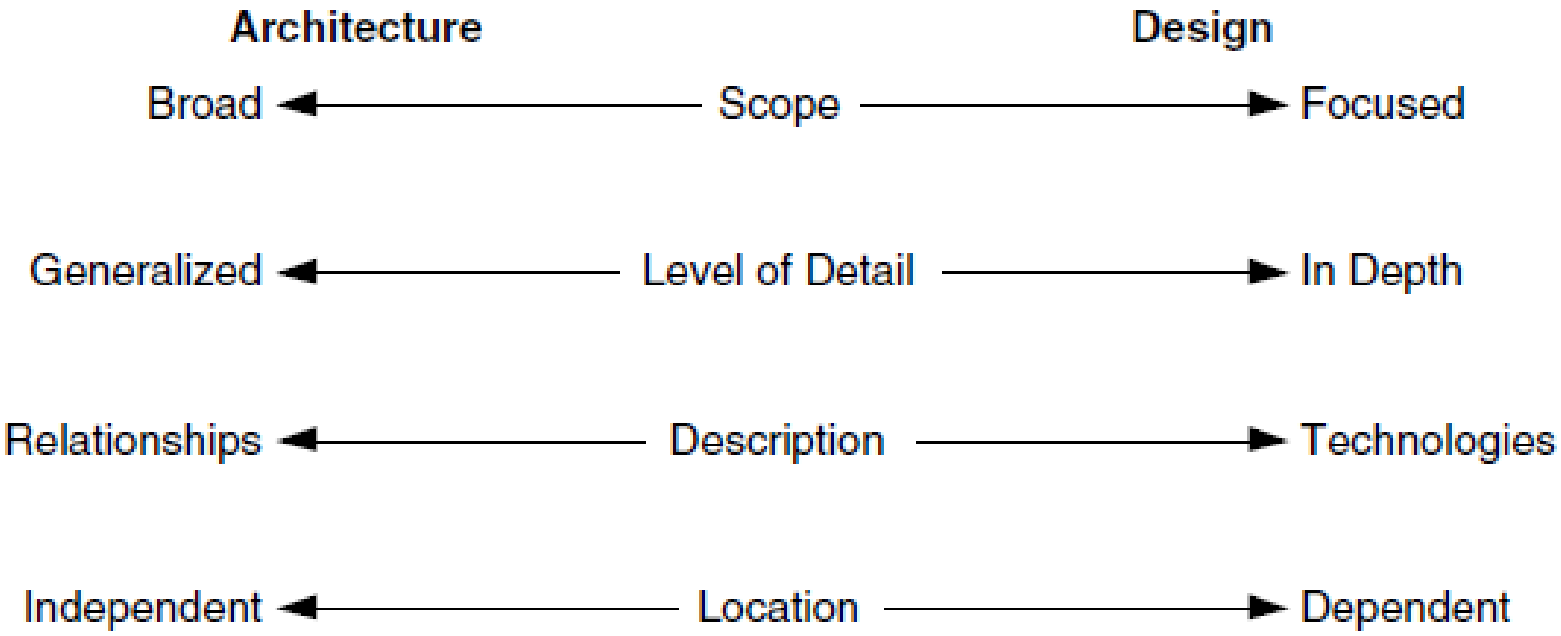
NETWORK

DESIGN & ANALYSIS

05 NETWORK ARCHITECTURE

Contents

5.1 Architecture & Design



5.1 Architecture & Design

- Good network design is a process by which an extremely complex and nonlinear system is conceptualized.

- Network architecture and design development must be done in a systematic and reproducible manner.

5.1 Architecture & Design

- Component **architecture** is a description of how and where each function of a network is applied within that network.

- It consists of a set of **mechanisms** (hardware and software) by which that **function** is applied to the network.

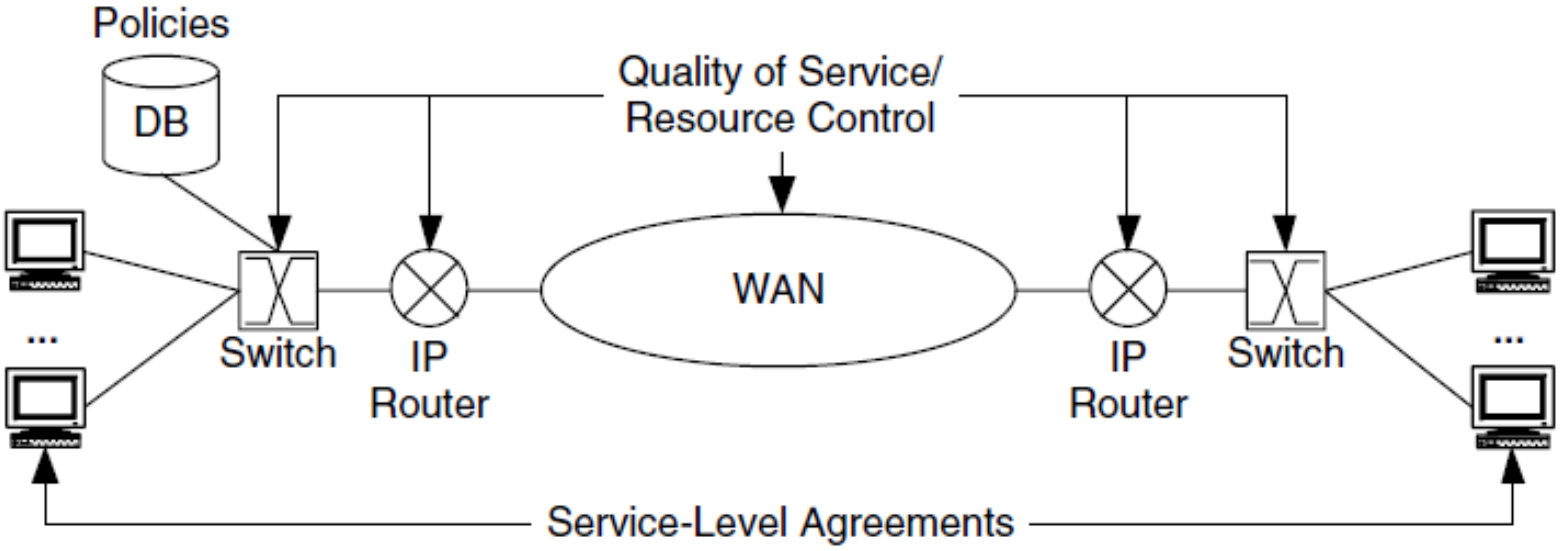
5.1 Architecture & Design

Function	Description of Capability	Example Subset of Mechanisms Used to Achieve Capability
Addressing/Routing	Provides robust and flexible connectivity between devices	• Addressing: Ways to allocate and aggregate address space • Routing: Routers, routing protocols, ways to manipulate routing flows
Network Management	Provides monitoring, configuring, and troubleshooting for the network	• Network management protocols • Network management devices • Ways to configure network management in the network
Performance	Provides network resources to support requirements for capacity, delay, RMA	• Quality of Service • Service-Level Agreements • Policies
Security	Restricts unauthorized access, usage, and visibility within network to reduce the threat and effects of attacks	• Firewalls • Security policies and procedures • Filters and access control lists

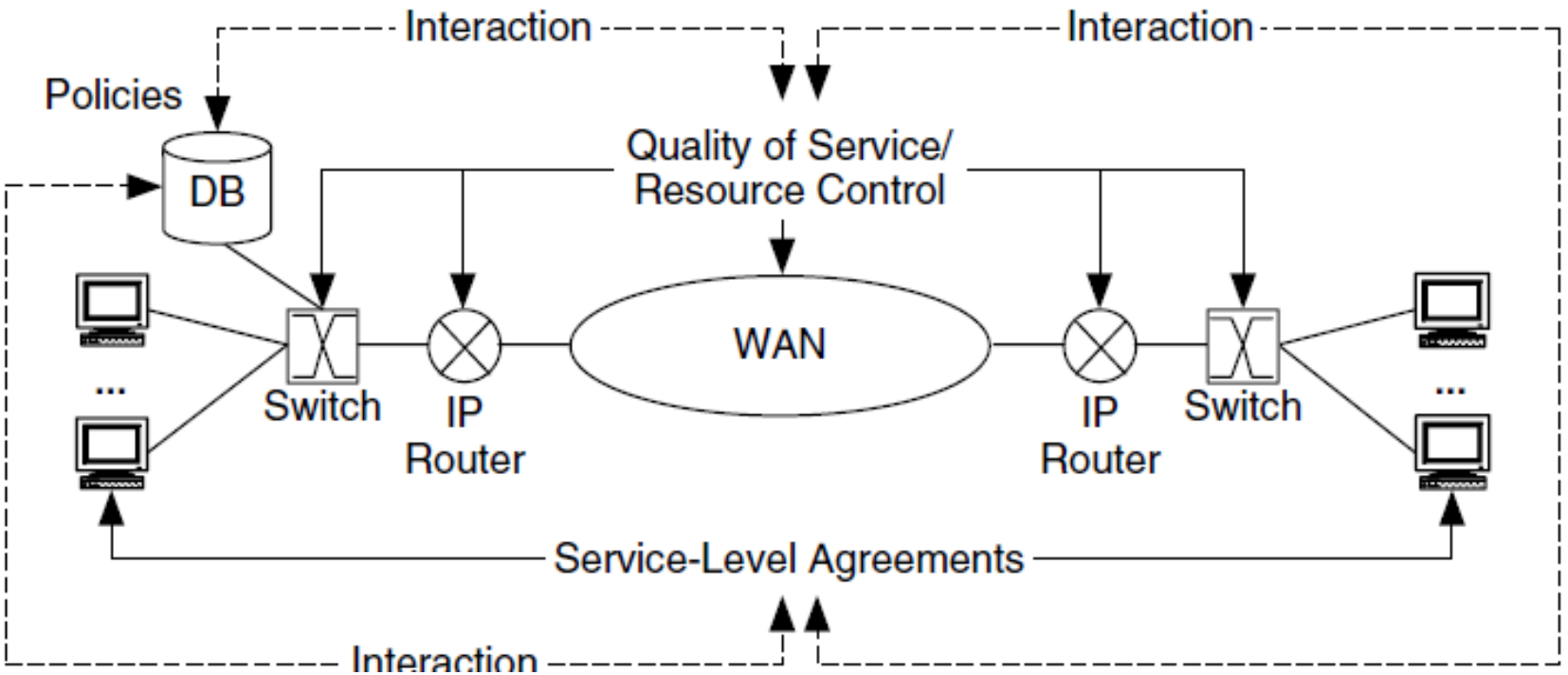
5.1 Architecture & Design

- In order to determine how performance will work for a network, it is needed to determine how each mechanism works, and how they work together to provide performance for the network and system.
- This picture bellow shows how QoS, SLA and policies are applied.

5.1 Architecture & Design



5.1 Architecture & Design

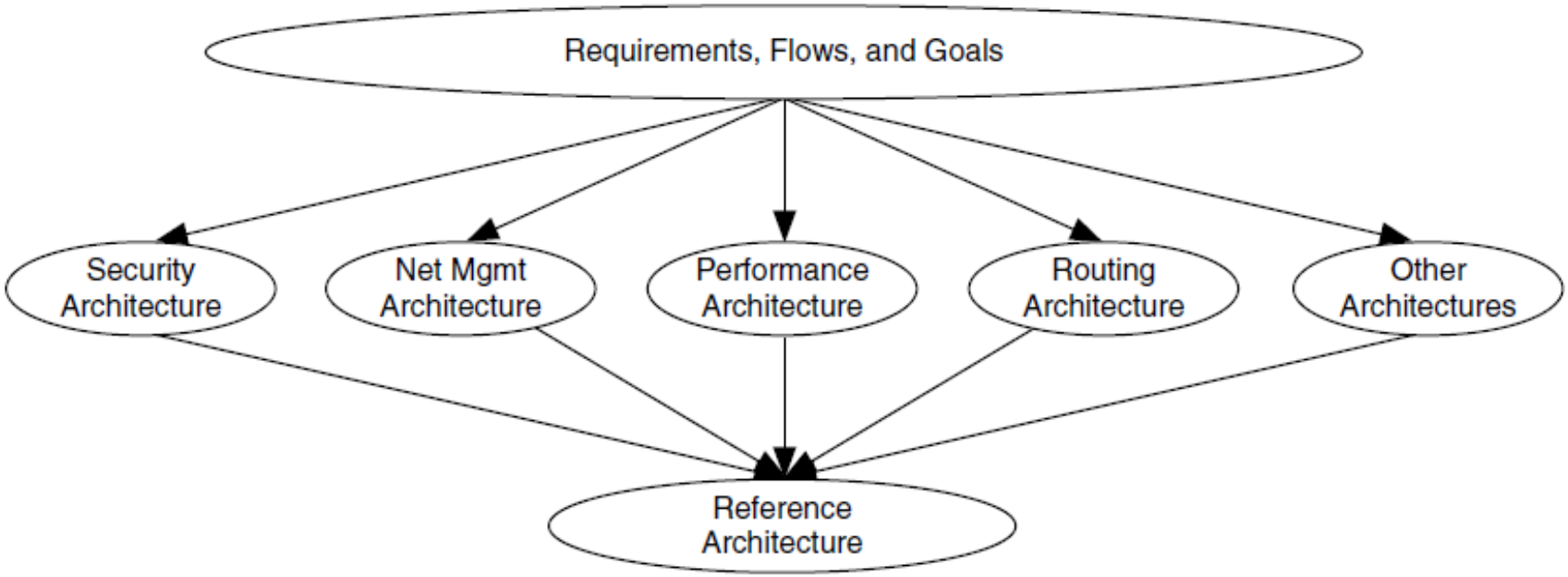


5.1 Architecture & Design

- Developing component architectures requires input, in terms of sets of user, application, and device requirements, estimated traffic flows, and architectural goals defined for each individual network.

- This input forms a common foundation for all network functions.

5.1 Architecture & Design



5.1 Architecture & Design

- To facilitate determining where each mechanism may be applied, the network is divided into regions.
- Commonly used regions include:
  - access (edge),
  - distribution,
  - core (backbone), and
  - external interfaces & DMZs.

5.1 Architecture & Design

- The characteristics of each region help to identify where mechanisms are applied.

- When mechanisms have been chosen and applied the internal relationships between these mechanisms are determined and analyzed.

5.1 Architecture & Design

Dependencies between Performance Mechanisms

	QoS	SLAs	Policies
QoS		QoS dependencies on SLAs—e.g., QoS at network devices may need to enforce SLA values	QoS dependencies on policies—e.g., QoS at network devices may need to enforce policies
SLAs	SLA dependencies on QoS—e.g., can an SLA be enforceable via available QoS mechanisms?		SLA dependencies on policies—e.g., SLAs may need to map to network policies
Policies	Policy dependencies on QoS—e.g., can a policy be enforceable via available QoS mechanisms?	Policy dependencies on SLAs	

5.1 Architecture & Design

5.1.1 Addressing & Routing

- *Addressing* is applying identifiers (addresses) to devices at various protocol layers (e.g., data-link and network),
- While *routing* is learning about the connectivity within and between networks and applying this connectivity information to forward IP packets toward their destinations.

5.1 Architecture & Design

- The addressing/routing describes:
  - how user and management traffic flows are forwarded through the network, and
  - how hierarchy, separation, and grouping of users and devices are supported.
- There are several addressing and routing mechanisms that could be considered.

5.1 Architecture & Design

- From an addressing perspective, mechanisms include:
  - subnetting & supernetting,
  - variable-length subnetting,
  - dynamic addressing,
  - private addressing,
  - virtual LANs (VLANs),
  - IPv6, and
  - network address translation (NAT).

5.1 Architecture & Design

- From a routing (forwarding) perspective, mechanisms include:
  - switching and routing,
  - classless interdomain routing (CIDR),
  - multicasts,
  - mobile IP,
  - route filtering, peering, routing policies, confederations, and
  - IGP, EGP selection and location.

5.1 Architecture & Design

5.1.2 Network Management

- *Network management* is providing functions to control, plan, allocate, deploy, coordinate, and monitor network resources.
- Network management mechanisms include:
  - Monitoring: Obtaining values for end-to-end, per-link, and per-element network management characteristics.
  - Instrumentation: Determining the set of tools and utilities needed to monitor and probe the network for management data.

5.1 Architecture & Design

- Configuration: Setting parameters in a network device for operation and control of that element.
- FCAPS components: The set of fault, configuration, accounting, performance, and security management components.
- In-band and out-of-band management: Whether management data flow along the same path as user traffic or have a separate path

5.1 Architecture & Design

- Centralized and distributed management: Whether the management system is in a single hardware platform or is distributed across the network among multiple platforms.
- Scaling network management traffic: Determining how much network capacity should be reserved for network management.
- Checks and balances: Using multiple mechanisms to verify that variables are represented correctly.

5.1 Architecture & Design

- Managing network management data: Offloading old data, keeping track of storage availability for data, updating data types.
- MIB selection: Determining which management information bases, and how much of each management information base, to use.
- Integration into OSS: How the management system will communicate with higher-level operations support system.

5.1 Architecture & Design

5.1.3 Performance

- *Performance* consists of the set of mechanisms used to configure, operate, manage, provision, and account for resources in the network that allocate performance to users, applications, and devices.
- This includes capacity planning and traffic engineering, as well as a variety of service mechanisms.

5.1 Architecture & Design

- Performance describes how network resources will be allocated to user and management traffic flows.
- This consists of
  - prioritizing, scheduling, and conditioning traffic flows
  - mechanisms to correlate user, application, and device requirements to traffic flows, access control, quality of service, policies, and service-level agreements (SLAs).

5.1 Architecture & Design

- *Quality of service*, or QoS, is determining, setting, and acting upon priority levels for traffic flows.
- *Resource control* refers to mechanisms that will allocate, control, and manage network resources for traffic.

5.1 Architecture & Design

- *Service-level agreements* (SLAs) are informal or formal contracts between a provider and user that define the terms of the provider's responsibility to the user and the type and extent of accountability if those responsibilities are not met.
- *Policies* are sets (again, formal or informal) of high-level statements about how network resources are to be allocated among users.

5.1 Architecture & Design

5.1.4 Security

- *Security* is a requirement to guarantee the confidentiality, integrity, and availability of user, application, device, and network information and physical resources.
- It describes how system resources are to be protected from theft, damage, denial of service (DOS), or unauthorized access.

5.1 Architecture & Design

- This consists of the mechanisms used to apply security, which may include such:
  - hardware and software capabilities as virtual private networks (VPNs),
  - encryption,
  - firewalls,
  - routing filters, and
  - network address translation (NAT).

5.1 Architecture & Design

- In many instances security mechanisms are deployed in regions, often termed *security zones* or *cells*,
- Each region or security zone represents a particular level of sensitivity and access control.

5.1 Architecture & Design

- The security mechanisms that were considered are:
  - Security threat analysis: The process to determine which components of the system need to be protected and the types of security risks (threats) they should be protected from
  - Security policies and procedures: Formal statements on rules for system, network, and information access and use, in order to minimize exposure to security threats

5.1 Architecture & Design

- Physical security and awareness: The protection of devices from physical access, damage, and theft (including isolating all or parts of the network from outside access); and getting users educated and involved with the day-to-day aspects of security in their network and helping them to understand the potential risks of violating security policies and procedures

5.1 Architecture & Design

- Protocol and application security: Securing management and network protocols and applications from unauthorized access and misuse.
- Encryption: Making data unreadable if they are intercepted, by applying cipher algorithms together with a secret key.
- Network perimeter security: Protecting the external interfaces between your network and external networks.

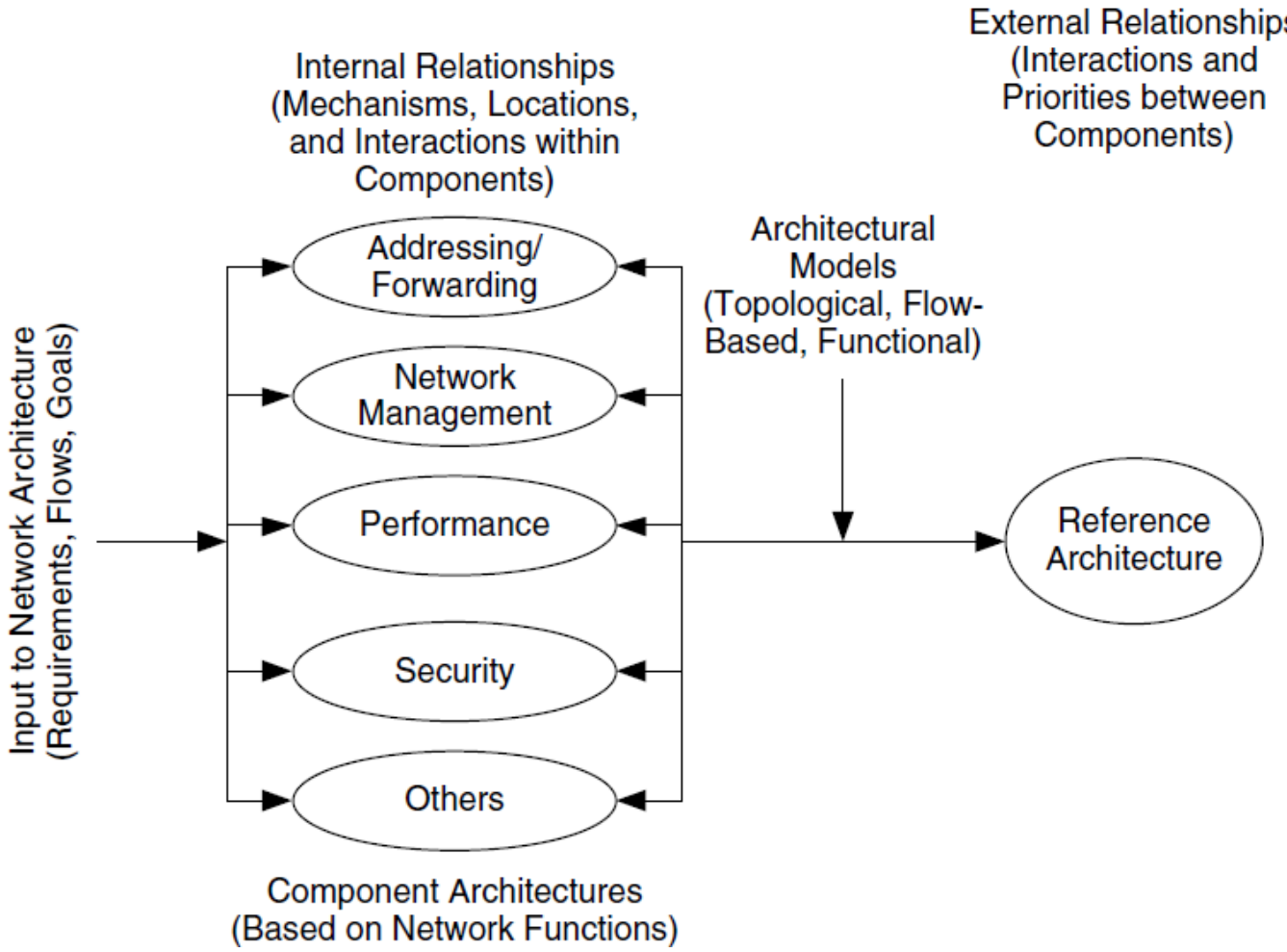
5.1 Architecture & Design

- Remote access security: Securing network access based on traditional dial-in, point-to-point sessions, and virtual private network connections.

5.2 Reference Architecture

- A *reference architecture* is a description of the complete network architecture and contains all of the component architectures (i.e., functions) being considered for that network.

5.2 Reference Architecture



5.2 Reference Architecture

- To some degree, each function depends upon and supports the other functions within a network, as well as the requirements from users, applications, and devices.
- This is reflected in the **external relationships** between their component architectures.

5.3 Architectural Models

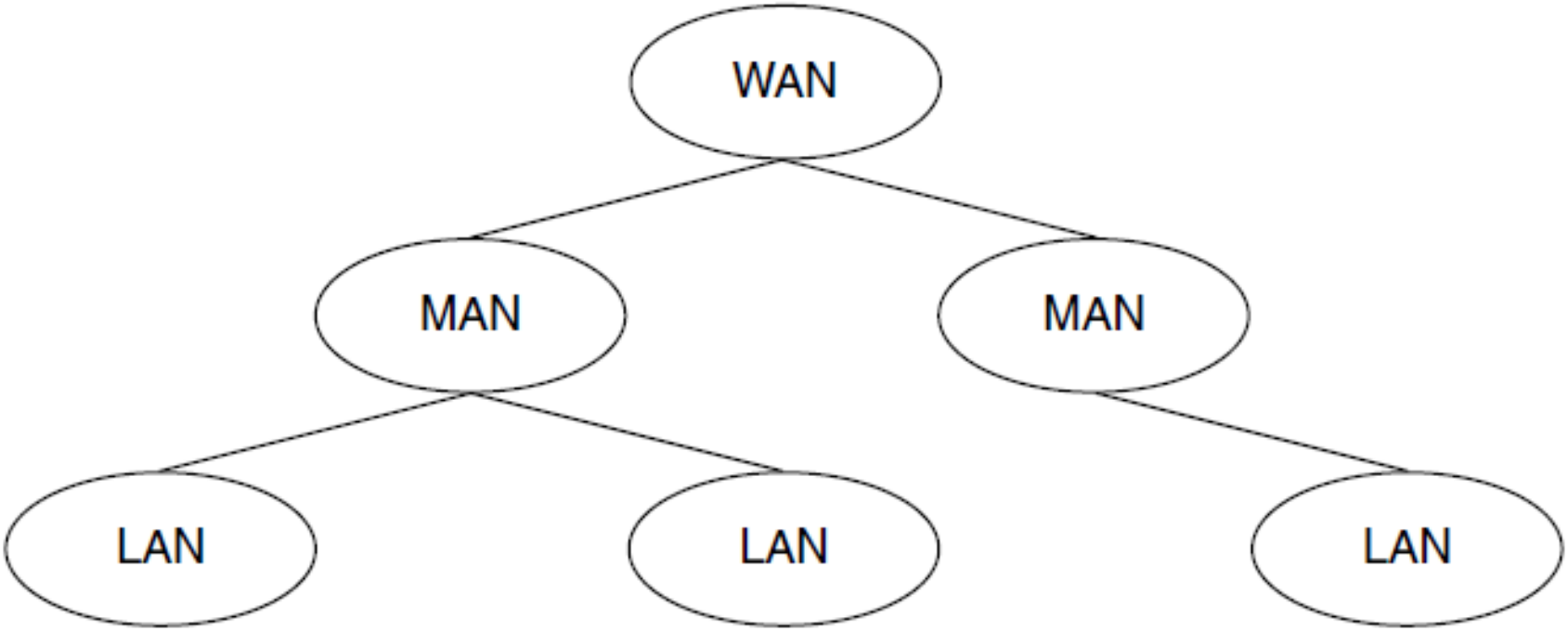
- Three types of architectural models :
  - **topological models**, which are based on a geographical or topological arrangement
  - **flow-based models**, which take particular advantage of traffic flows from the flow specification; and
  - **functional models**, which focus on one or more functions or features planned for in the network.

5.3 Architectural Models

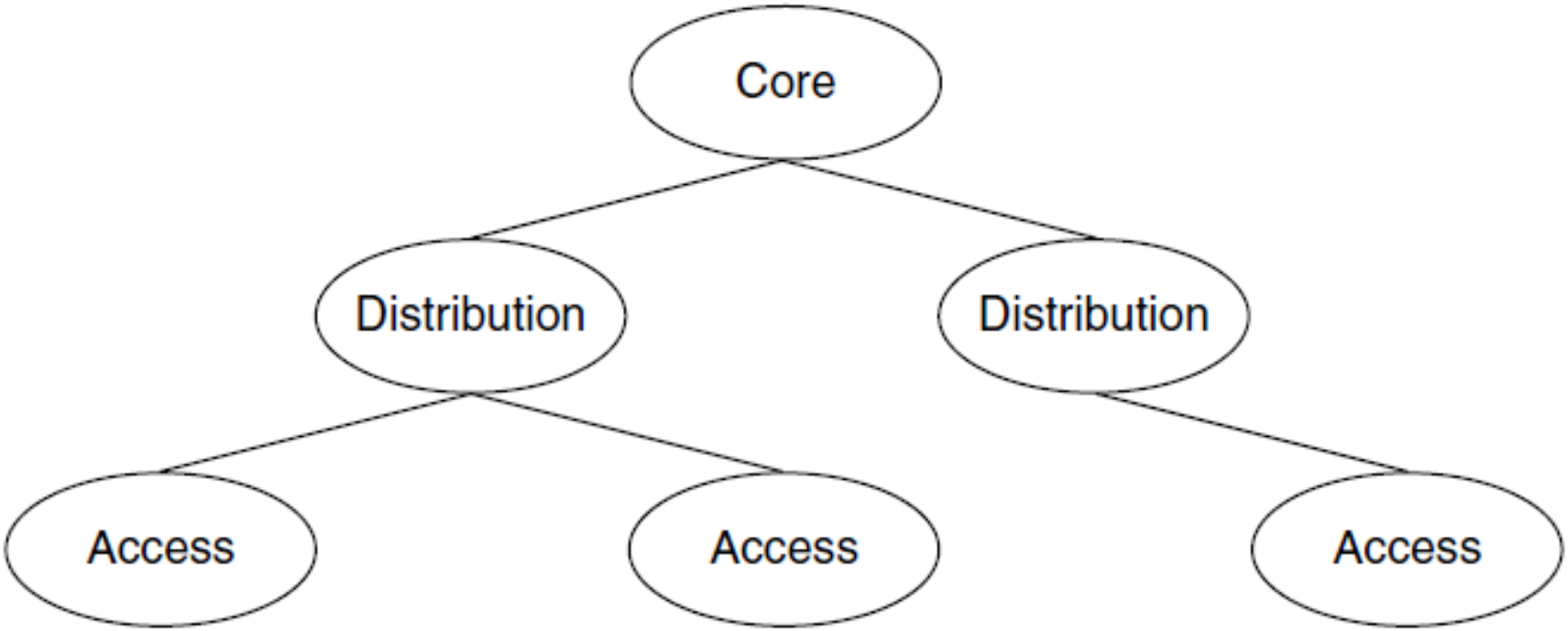
5.3.1 Topological Models

- There are two popular topological models: the
  - LAN/MAN/WAN, and
  - Access/Distribution/Core models.
- Both the LAN/MAN/WAN model and the Access/Distribution/Core model indicate the degree of hierarchy.

5.3 Architectural Models



5.3 Architectural Models



5.3 Architectural Models

5.3.2 Flow-based Model

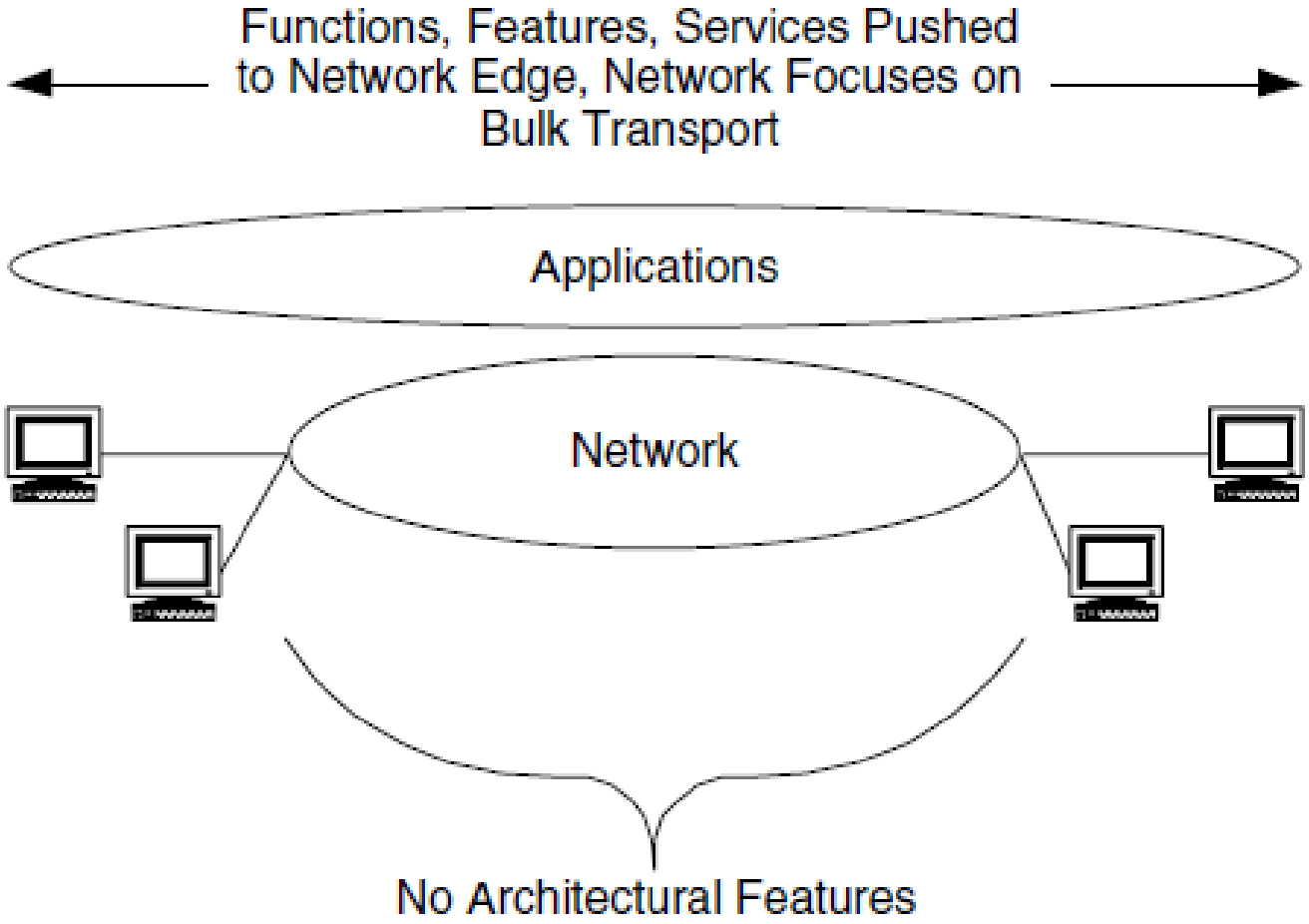
- Flow-based architectural models are based on the flow models.
- Like its counterparts, flow-based model architecture are:
  - Peer to peer,
  - Client-server,
  - Hierarchical client-server, and
  - Distributed computing

5.3 Architectural Models

Peer to Peer Model

- The important characteristics of this model are in the architectural features, flows, function, features, and services.
- There are no obvious locations for architectural features.
- This pushes the functions, features, and services toward the edge of the network, close to users and their devices, and also makes flows end-to-end.

5.3 Architectural Models

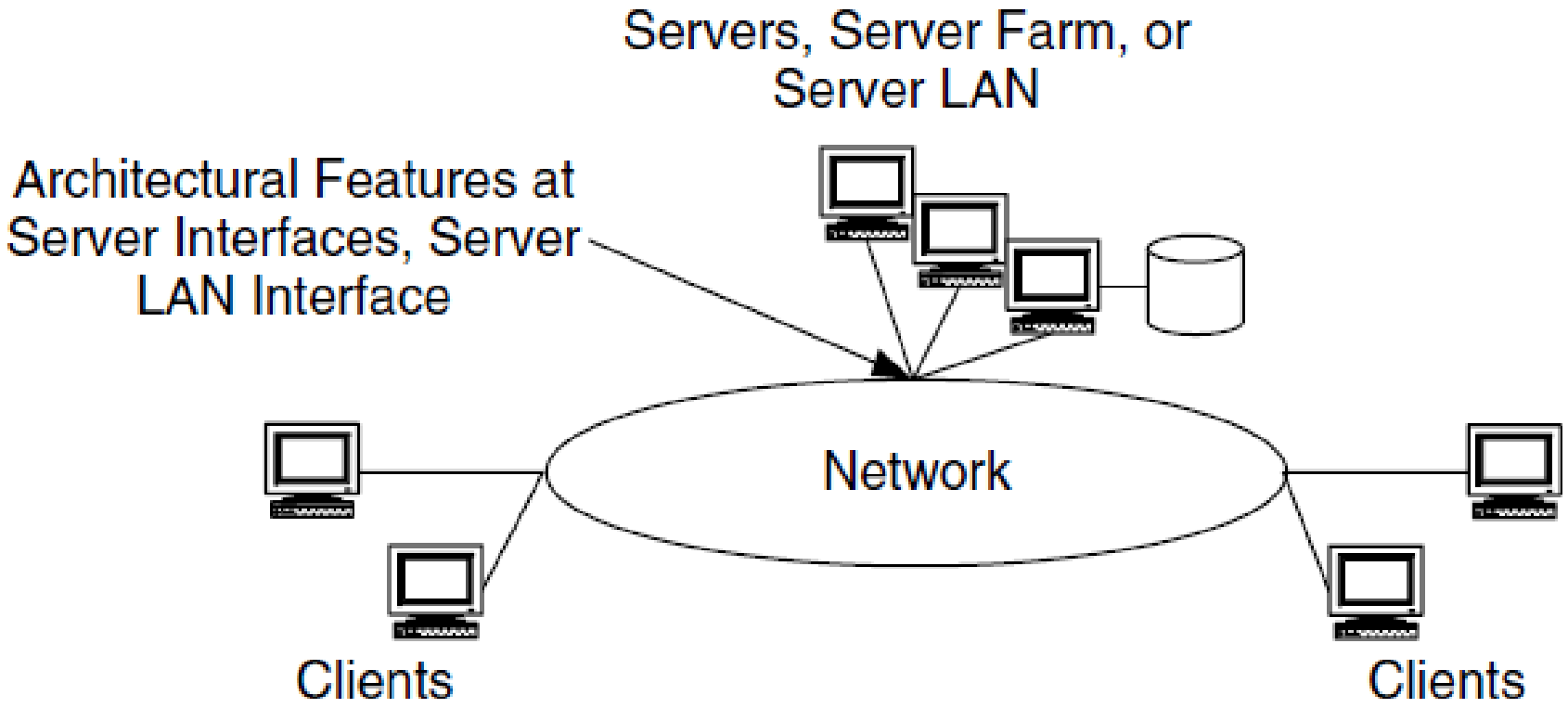


5.3 Architectural Models

Client Server Model

- The *client–server architectural model* also follows its flow model, but in this case there are obvious locations for architectural features—in particular, where flows combine.
- Therefore, functions, features, and services are focused at server locations, the interfaces to client LANs, and client–server flows.

5.3 Architectural Models

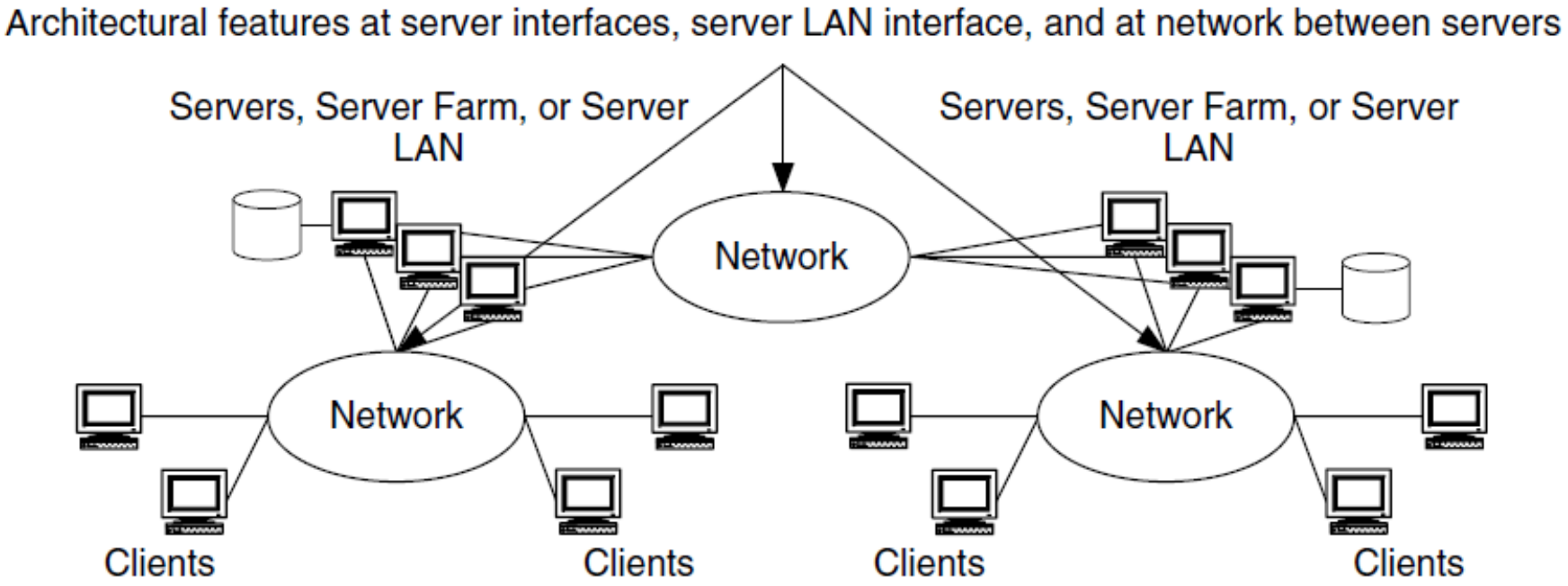


5.3 Architectural Models

Hierarchical Client-Server Model

- The characteristics of the client–server model also apply to the *hierarchical client–server architectural model*.
- In addition to the functions, features, and services being focused at server locations and client–server flows, they are also focused at the server–server flows.

5.3 Architectural Models

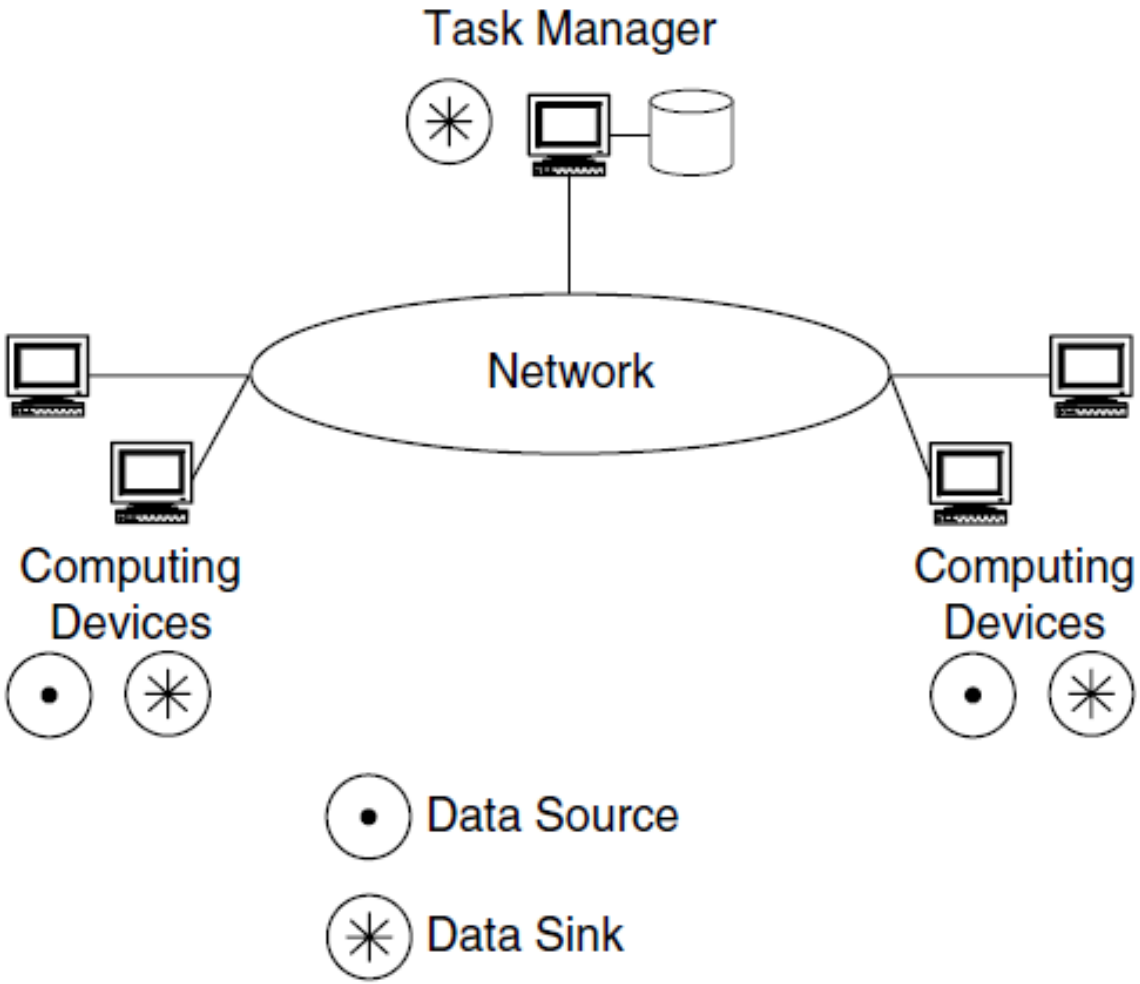


5.3 Architectural Models

Distributed Computing Model

- In the *distributed-computing architectural model* the data sources and sinks are obvious locations for architectural features.

5.3 Architectural Models



5.3 Architectural Models

- Flow-based models, like the topological models, are intuitive and can be easy to apply.

- Since they are associated with flows, they should map well to any flow maps as part of the requirements analysis process.

5.3 Architectural Models

5.3.3 Functional Model

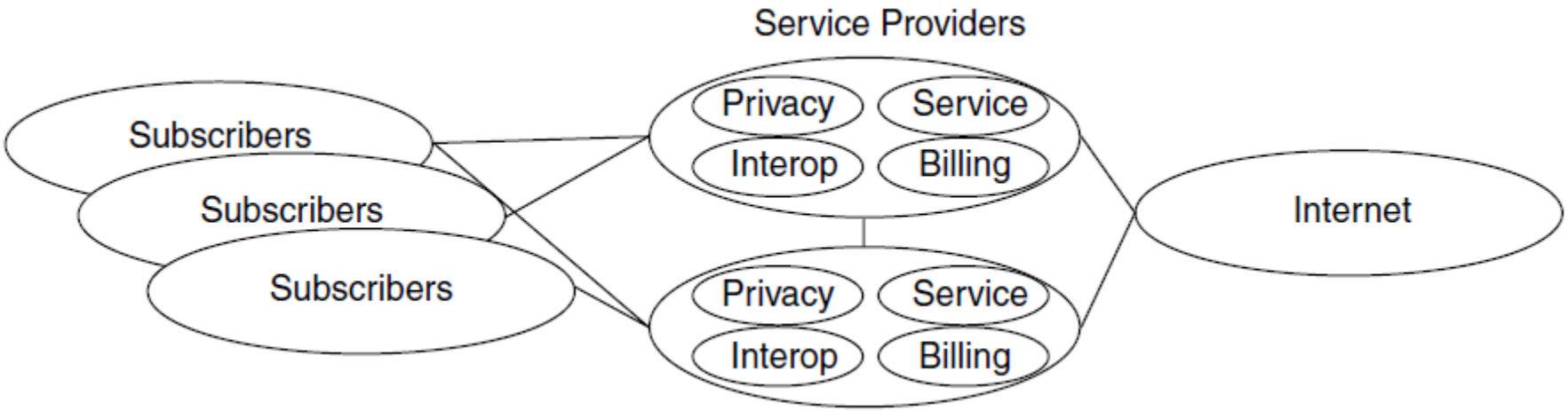
- Functional architectural models focus on supporting particular functions in the network.
- There are:
  - service-provider,
  - intranet/extranet,
  - single-/multi-tiered performance, and
  - end-to-end models.

5.3 Architectural Models

Service-Provider Model

- This model is based on service-provider functions, focusing on privacy and security, service delivery to customers (users), and billing.
- In this model, interactions between providers (the networks) and with users are compartmentalized.

5.3 Architectural Models

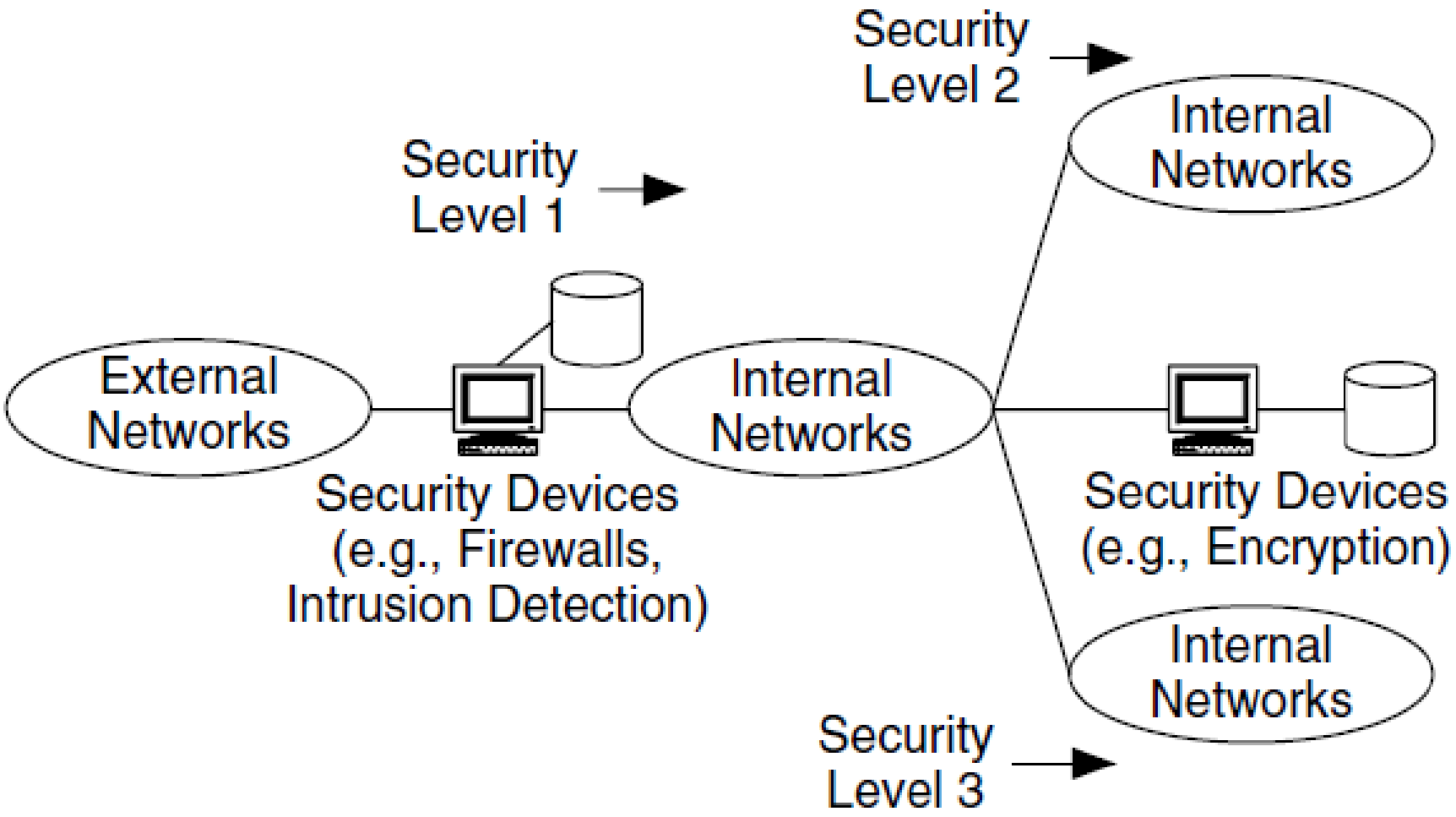


5.3 Architectural Models

Intranet/Extranet Model

- The *intranet/extranet architectural model* focuses on security and privacy, including the separation of users, devices, and applications based on secure access.
- Note that in this model there can be several levels of hierarchy (security/privacy).

5.3 Architectural Models



5.3 Architectural Models

Single-/Multi-tiered Performance Model

- The *single-/multi-tiered performance architectural model* focuses on identifying networks or parts of a network as having a single tier of performance, multiple tiers of performance, or having components of both.
- This model is based on results from the requirements and flow analyses, where single- and multi-tiered performance is determined.

5.3 Architectural Models

End-to-End Model

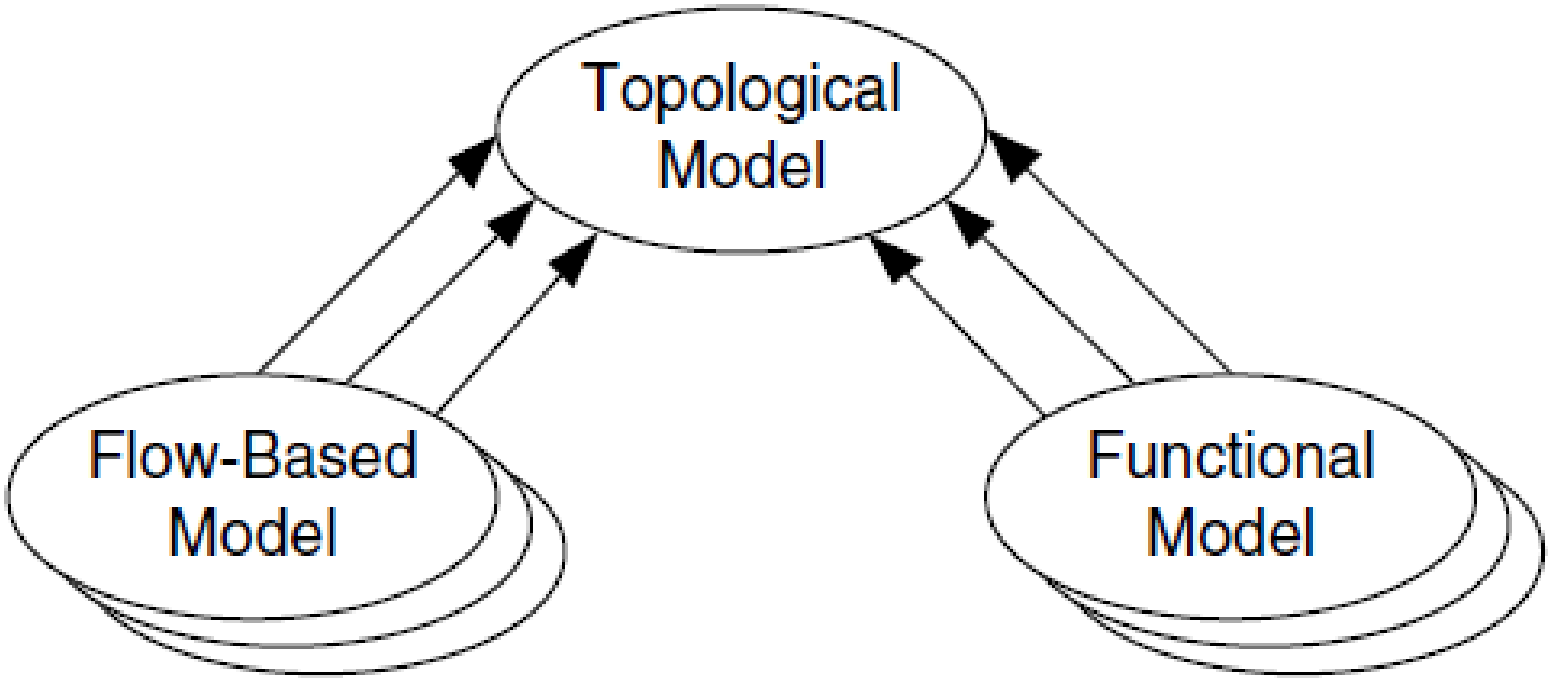
- The *end-to-end architectural model* focuses on all components in the end-to-end path of a traffic flow.
- This model is most closely aligned to the flow-based perspective of networking.

•Functional models are the most difficult to apply to a network, in that you must understand where each function will be located.

5.4 Using The Models

- Typically, a few of the models from the previous sections are combined to provide a comprehensive architectural view of the network.
- This is usually achieved by starting with one of the topological models and then adding flow-based and functional models as required.

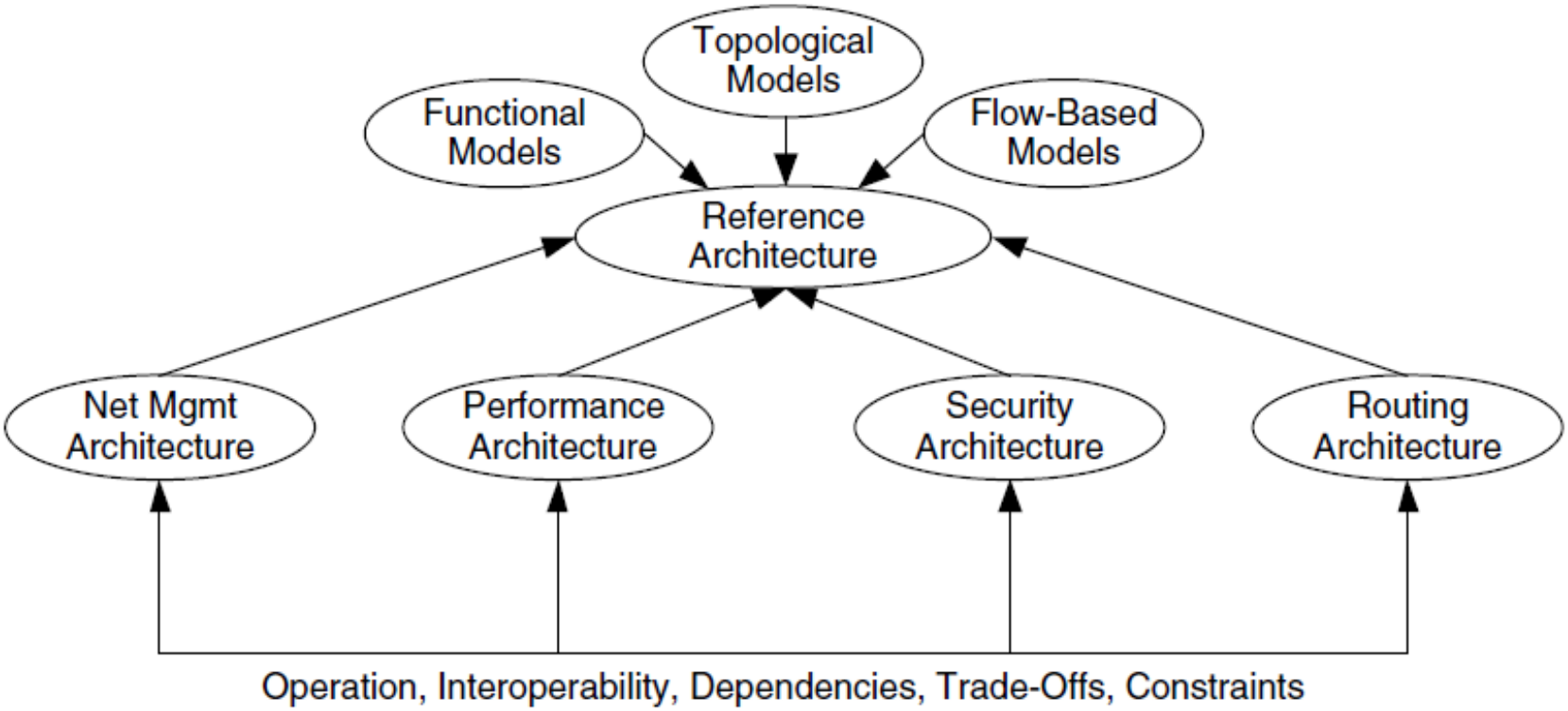
5.4 Using The Models



5.4 Using The Models

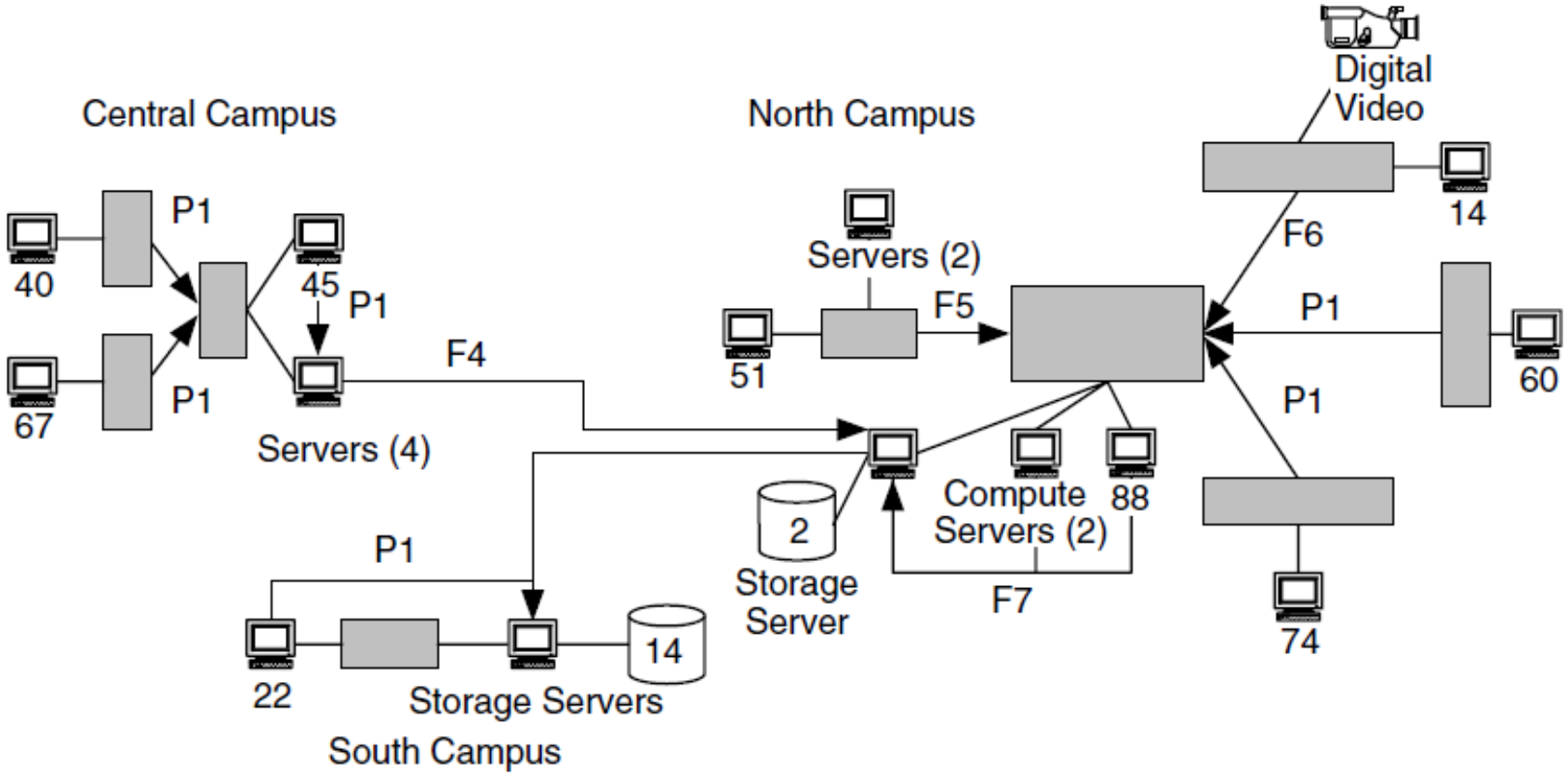
- The result of combining models and developing the relationships between architectural components is the reference architecture.

5.4 Using The Models

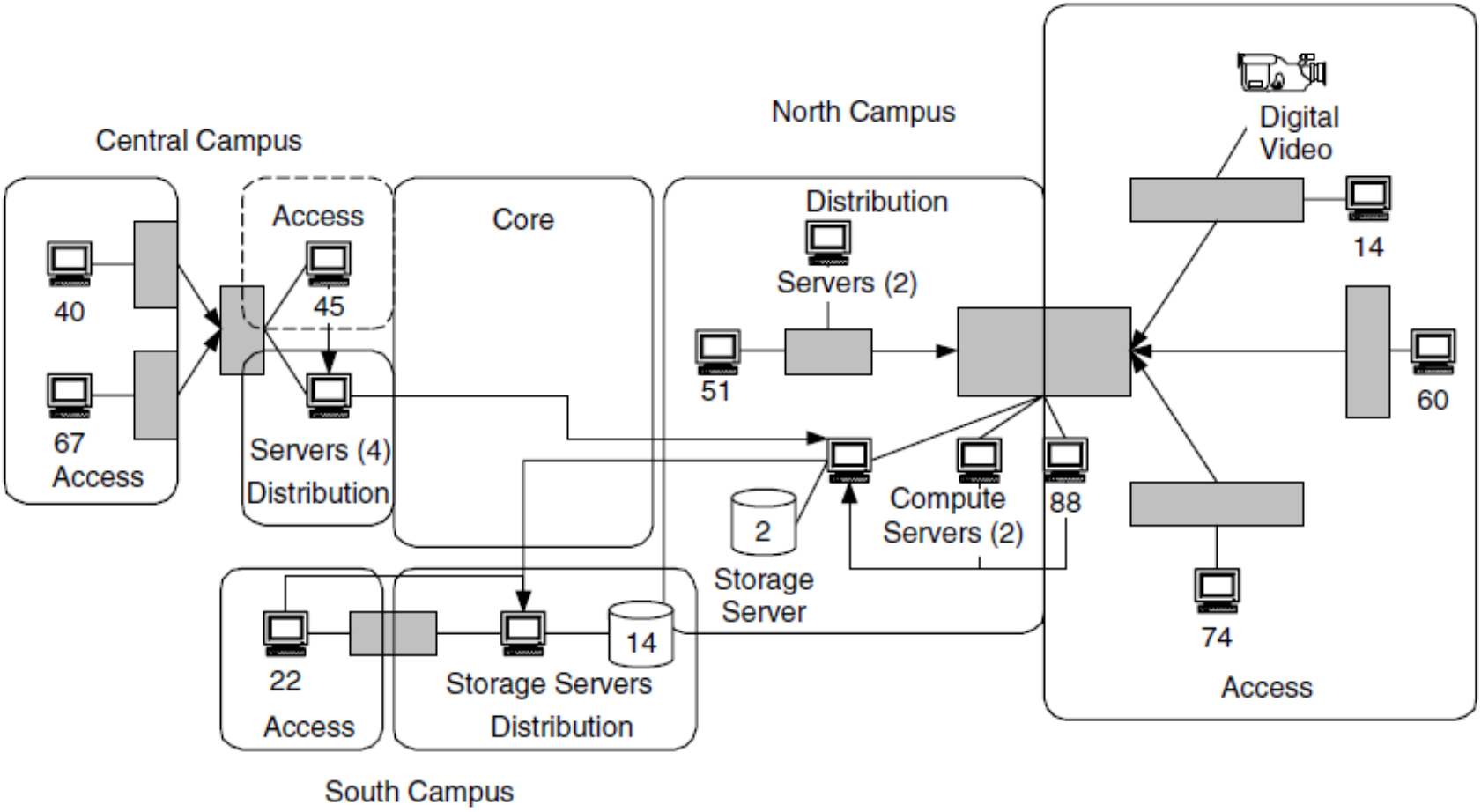


5.4 Using The Models

Example Applying Architecture Model



5.4 Using The Models



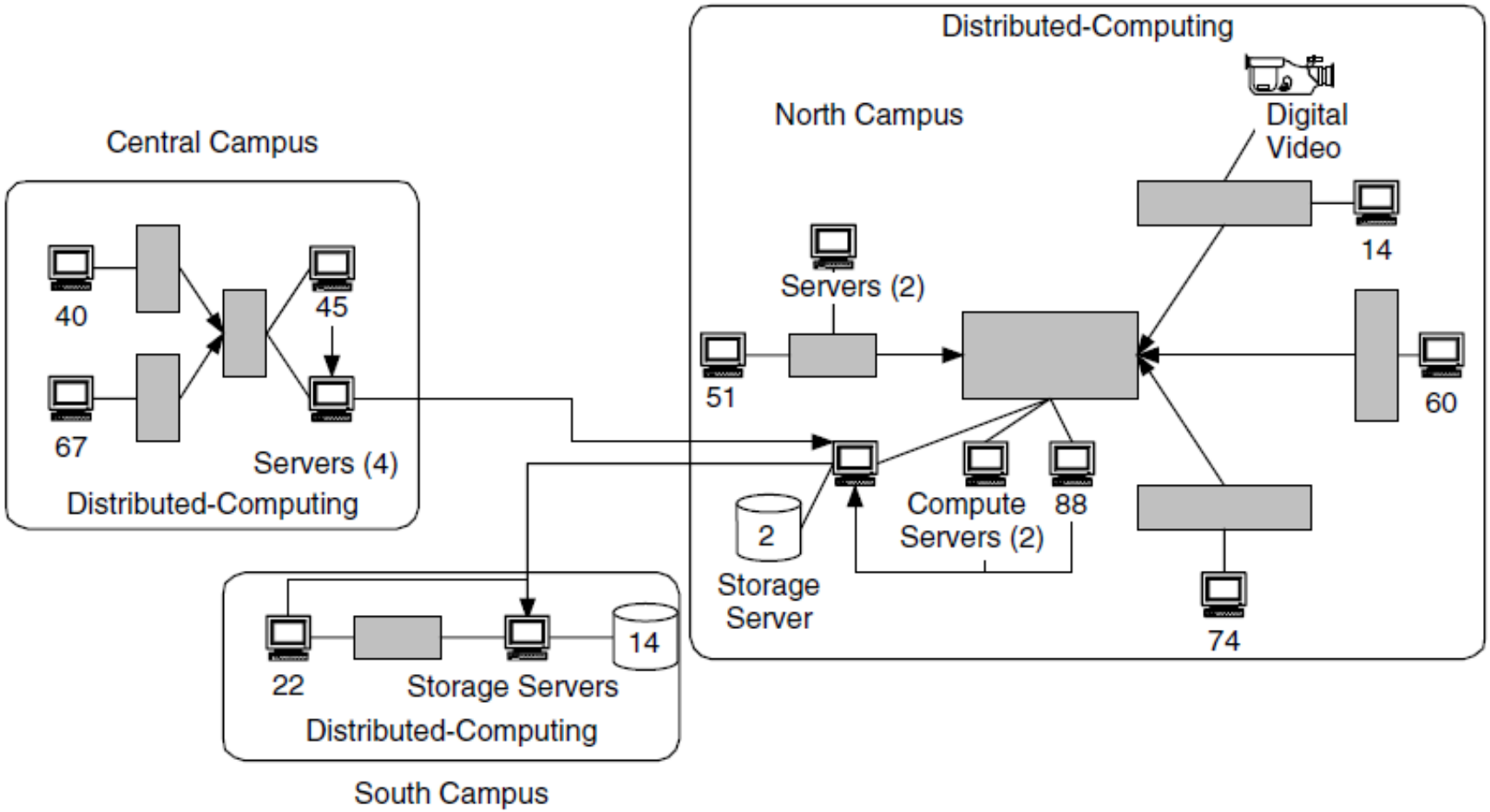
5.4 Using The Models

- For this flow map, *the access areas* are where user devices are located, as the primary sources of data.
- *Distribution areas* are where servers are located in each campus, as sinks and also source of data.
- *The core area* are between building, where bulk data transport is needed, there are no obvious sources or sinks.

5.4 Using The Models

- *A distributed-computing architectural model* between servers and their clients could also be applied.
- There are three areas where the distributed-computing model can apply in this example, one at each campus.
- Note that in each area the flows within it are from user devices to servers.

5.4 Using The Models

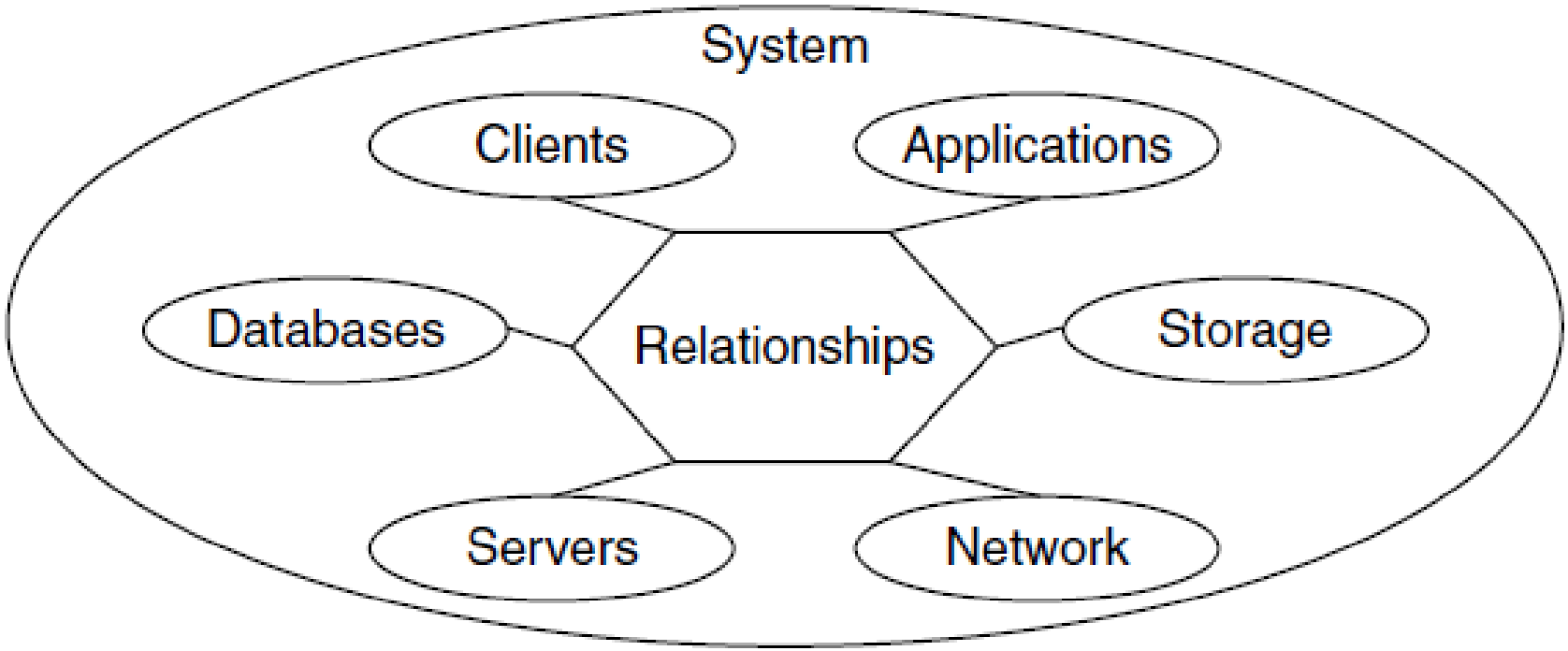


5.5 System Architecture

- The systems architecture considers the total or comprehensive picture, including the network, servers/clients, storage, servers, applications, and databases.

- Potentially, each component in the system could have its own architecture.

5.5 System Architecture



5.5 System Architecture

- In contrast, the network architecture considers the relationships within and between each of the network architectural components.
- It is could be one of the components of system architecture.

5.5 System Architecture