**Using a Modular Approach to Network Design**

This section expands on the Cisco Service-Oriented Network Architecture (SONA) framework

described in Chapter 2 and explores the six modules of the Cisco Enterprise Architecture, with an emphasis on the network infrastructure design considerations.

The modularity built into the architecture allows flexibility in network design and facilitates

implementation and troubleshooting. Before the details of the architecture itself are introduced, an overview of the evolution of enterprise networks is provided.

**Evolution of Enterprise Networks**

You do not have to go far back in history to find a time when networks were primarily used for file and print services. These networks were isolated LANs that were built throughout the enterprise organization. As organizations interconnected, these isolated LANs and their functions grew from file and print services to include critical applications; the critical nature and complexity of the enterprise networks also grew.

As discussed in the previous section, Cisco introduced the hierarchical model to divide the

enterprise network design (separately for both campus and WAN networks) into the access,

distribution, and core layers. This solution has several weaknesses, especially for large networks,

which are difficult to implement, manage, and, particularly, troubleshoot. Networks became

complex, and it was difficult to evaluate a network solution end-to-end through the network. The

hierarchical model does not scale well to these large networks.

An efficient method of solving and scaling a complex task is to break it into smaller, more

specialized tasks. Networks can easily be broken down smaller because they have natural physical, logical, and functional boundaries. If they are sufficiently large to require additional design or operational separation, these specialized functional modules can then be designed hierarchically with the access, distribution, and core layers.

The Cisco Enterprise Architecture does just that: It reduces the enterprise network into further

physical, logical, and functional boundaries, to scale the hierarchical model. Now, rather than

designing networks using only the hierarchical model, networks can be designed using this Cisco

Enterprise Architecture, with hierarchy (access, distribution, and core) included in the various

modules, as required.

Designing with this Cisco Enterprise Architecture is not much different from what is already used in practice; it formalizes current practice. There have always been separate hierarchies for the campus (with access, distribution, and core) and for the WAN (the remote office was the access layer, the regional office provided the distribution layer, and the headquarters was the core). The hierarchies tied together at the campus backbone. The Cisco Enterprise Architecture extends the concept of hierarchy from the original two modules: Campus and WAN.

**NOTE** The access, distribution, and core layers can appear within each module of the Cisco

Enterprise Architecture

**Cisco SONA Framework**

As illustrated in Figure 3-8, the Cisco SONA provides an enterprise-wide framework that

integrates the entire network—campus, data center, enterprise edge, WAN, branches, and

teleworkers—offering staff secure access to the tools, processes, and services they require.



The modules of the Cisco Enterprise Architecture represent focused views of each of the places in

the network described in the SONA framework. Each module has a distinct network infrastructure

and distinct services; network applications extend between the modules.

**Functional Areas of the Cisco Enterprise Architecture**

At the first layer of modularity in the Cisco Enterprise Architecture, the entire network is divided

into functional *components*—functional areas that contain network modules—while still

maintaining the hierarchical concept of the core-distribution-access layers within the network

modules as needed.

The Cisco Enterprise Architecture comprises the following six major functional areas (also called

*modules*):

■ Enterprise Campus

■ Enterprise Edge

■ Service Provider

■ Enterprise Branch

■ Enterprise Data Center

■ Enterprise Teleworker

Figure 3-9 illustrates the modules within the Cisco Enterprise Architecture.

**NOTE** The access, distribution, and core layers can appear in any functional area or module

of the Cisco Enterprise Architecture.

**KEY POINT**

An enterprise does not implement the modules in the Service Provider functional area;

they are necessary for enabling communication with other networks.

**NOTE** The Cisco SONA Enterprise Edge and the WAN and metropolitan-area network

(MAN) modules are represented as one functional area in the Cisco Enterprise Architecture, the Enterprise Edge.



The Cisco Enterprise Campus Architecture combines a core infrastructure of intelligent switching and routing with tightly integrated productivity-enhancing technologies, including Cisco Unified Communications, mobility, and advanced security. The architecture provides the enterprise with high availability through a resilient multilayer design, redundant hardware and software features, and automatic procedures for reconfiguring network paths when failures occur. IP multicast capabilities provide optimized bandwidth consumption, and QoS features ensure that real-time traffic (such as voice, video, or critical data) is not dropped or delayed. Integrated security protects against and mitigates the impact of worms, viruses, and other attacks on the network, including at the switch port level. For example, the Cisco enterprise-wide architecture extends support for security standards, such as the IEEE 802.1X port-based network access control standard and the Extensible Authentication Protocol. It also provides the flexibility to add Internet Protocol Security (IPsec) and MPLS virtual private networks (VPN), identity and access management, and VLANs to compartmentalize access. These features help improve performance and security while decreasing costs.

The Cisco Enterprise Edge Architecture offers connectivity to voice, video, and data services

outside the enterprise. This module enables the enterprise to use Internet and partner resources,

and provide resources for its customers. QoS, service levels, and security are the main issues in

the Enterprise Edge.

The Cisco Enterprise WAN and MAN and Site-to-Site VPN module is part of the Enterprise Edge.

It offers the convergence of voice, video, and data services over a single Cisco Unified

Communications network, which enables the enterprise to span large geographic areas in a cost effective manner. QoS, granular service levels, and comprehensive encryption options help ensure the secure delivery of high-quality corporate voice, video, and data resources to all corporate sites, enabling staff to work productively and efficiently wherever they are located. Security is provided with multiservice VPNs (both IPsec and MPLS) over Layer 2 or Layer 3 WANs, hub-and-spoke, or full-mesh topologies.

The Cisco Enterprise Data Center Architecture is a cohesive, adaptive network architecture that

supports requirements for consolidation, business continuance, and security while enabling

emerging service-oriented architectures, virtualization, and on-demand computing. Staff,

suppliers, and customers can be provided with secure access to applications and resources,

simplifying and streamlining management and significantly reducing overhead. Redundant data

centers provide backup using synchronous and asynchronous data and application replication.

The network and devices offer server and application load balancing to maximize performance. This architecture allows the enterprise to scale without major changes to the infrastructure. This module can be located either at the campus as a server farm or at a remote facility.

The Cisco Enterprise Branch Architecture allows enterprises to extend head-office applications

and services (such as security, Cisco Unified Communications, and advanced application

performance) to thousands of remote locations and users or to a small group of branches. Cisco

integrates security, switching, network analysis, caching, and converged voice and video services

into a series of integrated services routers (ISR) in the branch so that the enterprises can deploy

new services without buying new routers. This architecture provides secure access to voice,

mission-critical data, and video applications—anywhere, anytime. Advanced routing, VPNs,

redundant WAN links, application content caching, and local IP telephony call processing features are available with high levels of resilience for all the branch offices. An optimized network leverages the WAN and LAN to reduce traffic and save bandwidth and operational expenses. The enterprise can easily support branch offices with the capability to centrally configure, monitor, and manage devices located at remote sites, including tools, such as Cisco AutoQoS and the Cisco Router and Security Device Manager graphical user interface QoS wizard, which proactively resolve congestion and bandwidth issues before they affect network performance.

The Cisco Enterprise Teleworker Architecture allows enterprises to securely deliver voice and data services to remote small or home offices (known as small office, home office [SOHO]) over a standard broadband access service, providing a business-resiliency solution for the enterprise and a flexible work environment for employees. Centralized management minimizes the IT support costs, and robust integrated security mitigates the unique security challenges of this environment.

Integrated security and identity-based networking services enable the enterprise to extend campus security policies to the teleworker. Staff can securely log in to the network over an always-on VPN and gain access to authorized applications and services from a single cost-effective platform.

Productivity can be further enhanced by adding an IP phone, thereby providing cost-effective

access to a centralized IP communications system with voice and unified messaging services.

This architecture allows network designers to focus on only a selected module and its functions.

Designers can describe each network application and service on a per-module basis and validate

each as part of the complete enterprise network design. Modules can be added to achieve

scalability if necessary; for example, an organization can add more Enterprise Campus modules if it has more than one campus.

**Guidelines for Creating an Enterprise Network**

When creating an Enterprise network, divide the network into appropriate areas, where the

Enterprise Campus includes all devices and connections within the main Campus location; the

Enterprise Edge covers all communications with remote locations and the Internet from the

perspective of the Enterprise Campus; and the remote modules include the remote branches,

teleworkers, and the remote data center. Define clear boundaries between each of the areas.

Figure 3-10 shows an example of dividing a network into an Enterprise Campus area, an

Enterprise Edge area, and some remote areas.

**NOTE** Each of these modules has specific requirements and performs specific roles in the

network; note that their sizes in Figure 3-9 are not meant to reflect their scale in a real network.

**NOTE** Depending on the network, an enterprise can have multiple campus locations. A

location that might be a remote branch from the perspective of a central campus location might

locally use the Cisco Enterprise Campus Architecture.

