CHAPTER 1

Small Enterprise Design Profile (SEDP) Overview

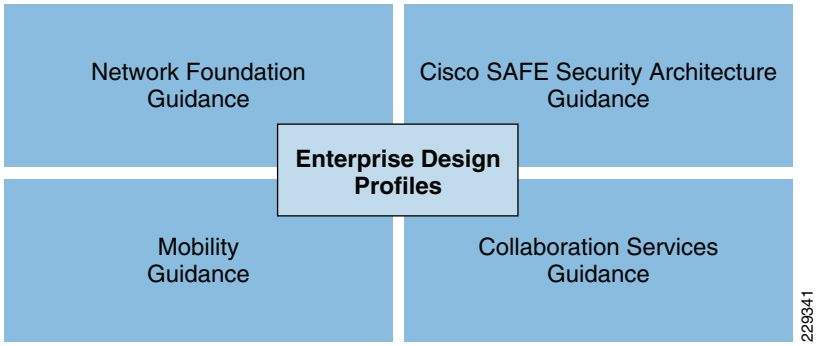
The Enterprise Design Profile delivers the foundational network design that all enterprise services, applications, and solutions use to interact and communicate with one another. The Enterprise Design Profile is constructed in a fashion that supports all the applications and services that will ride on it. Additionally, these profiles must be aware of the type of traffic traversing and treat each application or service with the correct priority based on the needs and importance of that application.

The Small Enterprise Design Profile is made up of the following four distinct components:

- Network Foundation guidance
- Cisco SAFE Security Architecture guidance
- Mobility guidance
- Collaboration Services guidance such as Unified Communications

Each of these critical foundation components have been carefully designed and tuned to allow for a secure environment that provides for business continuity, service awareness and differentiation, as well as access flexibility. See Figure 1-1.

Figure 1-1 Small Enterprise Design Profile Design Components

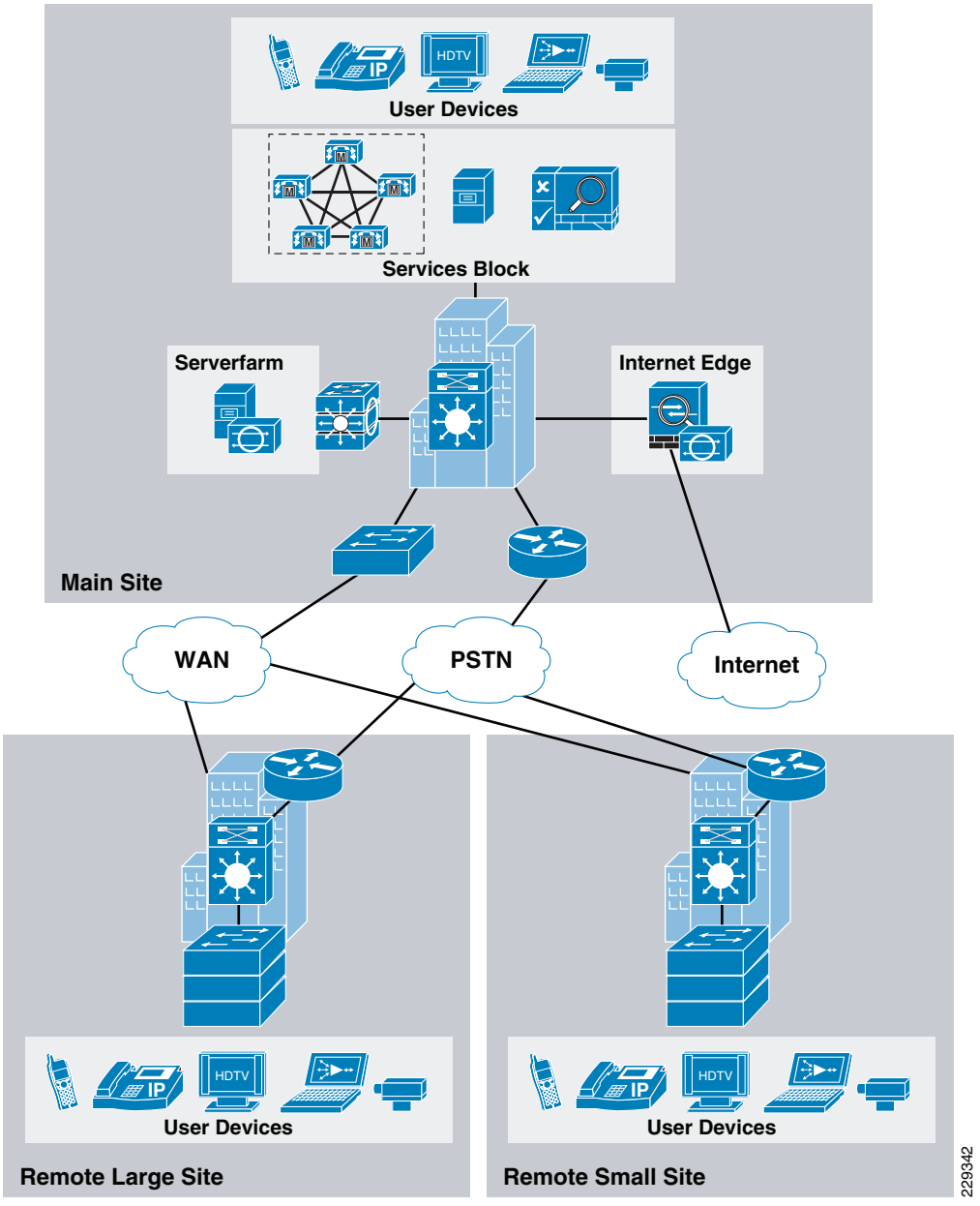


Small Enterprise Design Profile

The design used for the Small Enterprise Design Profile is intended to represent as many small-size Enterprise network environments as possible. To accomplish this, a modular design is used representing sites of varying sizes (see Figure 1-2). The Small Enterprise Design Profile is built upon a network foundation consisting of a main site, where the majority of the critical applications reside.

Connected through a Metro Ethernet WAN are remote sites of varying sizes. The remote small site is designed to support up to 100 employees. The remote large site is designed to support up to 500 employees. Each site can coexist in a small Enterprise network or can be treated as separate modules. Design guidance for remote sites of varying sizes provides flexibility, modularity, and scalability as the Enterprise grows. Additionally, it is expected that half of all network can be accessed wired and wirelessly.

Figure 1-2 Small Enterprise Design Profile Design



Main Site Design

The main site design represents a centralized services site that interconnects the remote sites regardless of size. The main site consists of a main building core connected to a serverfarm and service block design. The remote large site and the remote small site connect to the main site via a 100Mbps Metro Ethernet link. Because many Enterprise services and applications are centrally located within the main site rather than each remote site, high network availability must be maintained. The main site is connected to outside entities such as the partners, vendors, customers, and the Internet using the Internet edge components. All the remote sites within the small enterprise system also connect to the main site and use the main site to connect outside the Enterprise.

Remote Large Site Design

The remote large site design has been developed for Enterprise sites that have up to 500 employees. The remote large site is connected to the main site via a 100Mbps Metro Ethernet link. While this site connects to the main site where most Enterprise services and applications are centralized, this site also uses resilient application services features to maintain critical services such as Digital Media Signage, Video Surveillance, and SRST in case of a WAN failure. For resiliency, this site is designed with a dual switch and dual aggregation links.

Remote Small Site Design

The remote small site profile represents a site supporting up to 100 employees. The core and distribution layers in the remote site network are collapsed into one and use Cisco's Catalyst Stackwise switching technology for redundancy. The remote small site is connected to the main site via a 10Mbps Metro Ethernet link and like the remote large site, resilient application service features are used to maintain critical services in case of a WAN failure.

Access Devices

The devices that connect to the Small Enterprise Design Profile network include phones, cameras, displays, laptops, desktops, mobile phones, and personal devices (iPod, MP3, etc). Half of all the devices are expected to connect to the network using 802.11 ABGN wireless access.

The Small Enterprise Design Profile consists of four major components. The sections below provide a brief description of each of these components.

Network Foundation Design Considerations

The Small Enterprise Design Profile Network Foundation guidance is made up of routers and switches deployed in a three-tier hierarchical model that uses Cisco IOS to provide foundational network technologies needed to provide a highly available, application-aware network with flexible access. LAN and WAN guidance is provided under this component.

LAN Design Considerations

Hierarchical network design model components:

- *Core layer*—The site backbone consisting of a Layer-3 core network interconnecting to several distributed networks and the shared services block to access local and global information.
- *Distribution layer*—The distribution layer uses a combination of Layer-2 and Layer-3 switching to provide for the appropriate balance of policy and access controls, availability, and flexibility in subnet allocation and VLAN usage.
- *Access layer*—The Demarcation point between network infrastructure and access devices. Designed for critical network edge functionality to provide intelligent application and device aware services.

High Availability Design Considerations

To ensure business continuity and prevent catastrophic network failure during unplanned network outage, it is important to identify network fault domains and define rapid recovery plans to minimize the application impact during minor and major network outages.

The Small Enterprise Design Profile design ensures network survivability by employing three major resiliency methods that serve to mitigate most types of failures. The appropriate resiliency option should be selected given the network system tier, role, and network service type:

- *Link resiliency*—Provides redundancy during physical link failures (i.e., fiber cut, bad transceivers, incorrect cablings, etc.)
- *Device resiliency*—Protects network during abnormal node failure triggered by hardware or software (i.e., software crashes, non-responsive supervisor etc.)
- *Operational resiliency*—Enables higher level resiliency capabilities, providing complete network availability even during planned network outage conditions.

Routing Protocol Selection Criteria

Routing protocols are essential for any network, because they allow for the routing of information between buildings and sites. Selecting the right routing protocol can vary based on the end-to-end network infrastructure. The routers and switches support many different routing protocols that will work for Small enterprise network environments. Network architects must consider all the following critical design factors when selecting the right routing protocol to be implemented throughout the internal network:

- *Network design*—Proven protocol that can scale in full-mesh site network designs and can optimally function in hub-and-spoke WAN network topologies.
- *Scalability*—Routing protocol function must be network and system efficient that operates with a minimal number of updates, recomputation independent of number of routes in the network.
- *Rapid convergence*—Link state versus DUAL recomputation and synchronization. Network reconvergence also varies based on network design, configuration, and a multitude of other factors which are beyond the routing protocol.
- *Operational considerations*—Simplified network and routing protocol design that can ease the complexities of configuration, management, and troubleshooting.

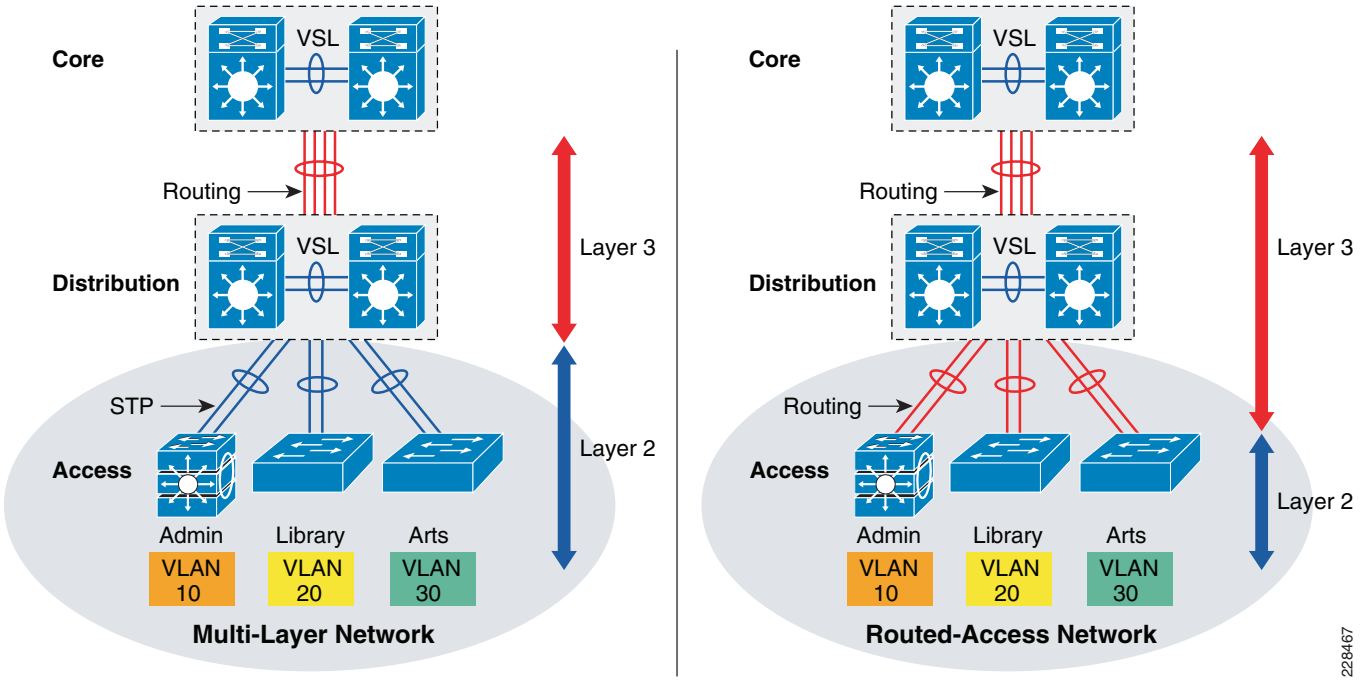
Access Layer Design Considerations

The access layer represents the entry into the network, consisting of wired and wireless access from the client to the network. The switch that the client connects to will ultimately connect to the network distribution layer of and the method communication here must be considered in any design. Traditional Layer 2 connectivity is prevalent in most networks today; however, it comes at some cost in administration, configuration, and timely resiliency. The emerging method of connectivity is a Layer 3 connection, commonly referred to as *routed-access*.

Performing the routing function in the access-layer simplifies configuration, optimizes distribution performances, and allows for the use of well known end-to-end troubleshooting tools. Implementing a Layer 3 access-layer in lieu of the traditional Layer 2 access replaces the required Layer 2 trunks with a single point-to-point Layer 3 link. Pushing Layer 3 routing functionality one tier down on Layer 3 access switches changes traditional multilayer network topology and the forwarding path. Implementing a routed access layer does not require any physical or logical link reconfiguration or changes.

See Figure 1-3.

Figure 1-3 Control Function in Multi-Layer and Routed-Access Network Design



At the network edge, Layer 3 access switches provides an IP gateway function and serve as a Layer-2 demarcation point to locally connected endpoints that can be logically segmented into multiple VLANs.

LAN Foundational Services

The Small Enterprise Design Profile uses essential foundational services to efficiently disseminate information that is used by multiple clients, as well as identify and prioritize different applications traffic based on their requirements. Designing the foundational services in a manner consistent with the needs of the Small enterprise network system is paramount. Some of the key foundational services discussed include the following:

- Multicast routing protocol design considerations
- Designing QoS in the site network

WAN Design Considerations

WAN Transport

In order for sites to communicate with one another and/or to communicate outside the Enterprise network system, network traffic must traverse over a WAN. WAN transport differs greatly from LAN transport due to variables such as the type of connection used, the speed of the connection, and the distance of the connection. The service fabric design model covers the following WAN transport design considerations:

- Internet
- Metro Ethernet

WAN Foundational Services

Similar to the LAN, the WAN must employ essential foundational services to ensure the proper transport and prioritization of community college services. WAN foundation services considered are as follows:

- Routing protocol design
- Quality-of-service (QoS)
- WAN resiliency
- Multicast

Cisco SAFE Security Architecture Design Considerations

Security of Small Enterprise Design Profile is essential. Without it, Enterprise solutions, applications, and services are open to be compromised, manipulated, or shut down. The Small Enterprise Design Profile was designed with built-in security by leveraging the proven design and deployment guidelines of the Cisco SAFE security architecture. The following are the primary security design considerations:

- *Network Foundation Protection (NFP)*—Ensuring the availability and integrity of the network infrastructure, protecting the control and management planes.
- *Internet perimeter protection*— Ensuring safe connectivity to the Internet, and protecting internal resources and users from malware, viruses, and other malicious software. Protecting users from harmful content. Enforcing E-mail and web browsing policies.
- *Serverfarm protection*—Ensuring the availability and integrity of centralized applications and systems. Protecting the confidentiality and privacy of user information and records.
- *Network access security and control*—Securing the access edges. Enforcing authentication and role-based access for employees and users residing at the main and remote sites. Ensuring systems are up-to-date and in compliance with the network security policies.
- *Network endpoint protection*—Protecting servers and Enterprise-controlled from viruses, malware, botnets, and other malicious software. Enforcing E-mail and web browsing policies for users.

Mobility

Mobility is an essential part of the Small Enterprise Design Profile. Most users will connect wirelessly to site networks and other devices will also rely on the mobile network. In designing the mobility portion of the service fabric, the following design criteria were used:

- *Accessibility*—Enables employees and guests to be accessible and productive, regardless of where they meet. This design element provides for easy, secure guest access to guests such as contractors, vendors and other visitors.
- *Usability*—In addition to extremely high WLAN transmission speeds made possible by the current generation of IEEE 802.11n technology, latency sensitive applications (such as IP telephony and video-conferencing) are supported over the WLAN using appropriately applied QoS. This gives preferential treatment to real-time traffic, helping to ensure that video and audio information arrives on time.
- *Security*—Segment authorized users and block unauthorized users. Extend the services of the network safely to authorized parties. Enforce security policy compliance on all devices seeking to access network computing resources. Employees enjoy rapid and reliable authentication through IEEE 802.1x and Extensible Authentication Protocol (EAP), with all information sent and received on the WLAN being encrypted.
- *Manageability*—Network administrators must be able to easily deploy, operate, and manage hundreds of access points within multiple Enterprise network site deployments. A single, easy to understand WLAN management framework is desired to provide small and large Enterprise systems with the same level of wireless LAN management scalability, reliability and ease of deployment that is demanded by traditional enterprise business customers.
- *Reliability*—Provide adequate capability to recover from a single-layer fault of a WLAN accessibility component or controller wired link. Ensure that wireless LAN accessibility is maintained for employees and guest visitors in the event of common failures.

Collaboration Services Design Considerations

Adoption of IP technology has led to a fundamental change in designing networks. No longer are networks used solely to provide data communication between computers and servers. IP technology has extended beyond the data network and is now used extensively for Unified Communications and Video communication as well. Unified Communications, IP Video Surveillance and Digital Media systems were validated in the Small Enterprise Design Profile.

Unified Communications Design Considerations

Call Processing Considerations

How calls are processed in the Small Enterprise Design Profile environment is an important design consideration. Guidance in designing scalable and resilient call processing systems is essential for the successful deployment of a unified communications system. Considerations include the following:

- *Scale*—The number of users, locations, gateways, applications, and so forth
- *Performance*—The call rate

- *Resilience*—The amount of redundancy

Gateway Design Considerations

Gateways provide a number of methods for connecting an IP telephony network to the Public Switched Telephone Network (PSTN). Design considerations for gateways include the following:

- PSTN trunk sizing
- Traffic patterns
- Interoperability with the call processing system

Dial Plan Considerations

Dial plan is one of the key elements of a unified communications system, and an integral part of all call processing agents. Generally, the dial plan is responsible for instructing the call processing agent on how to route calls. Specifically, the dial plan performs the following main functions:

- Endpoint addressing
- Path selection
- Calling privileges
- Digit manipulation
- Call coverage

Survivability Considerations

Voice communications are a critical service that must be maintained in the event of a network outage and for this reason the service fabric must take survivability into consideration. Guidance on how the Small Enterprise Design Profile is equipped and designed to keep voice communications active in the event of an outage is provided.

IP Video Surveillance Design Considerations

Video surveillance systems have proven their value in a wide range of applications. Video documentation of critical incidents enhances employee safety and better protects valuable assets. However, traditional analog Closed-circuit TeleVision (CCTV) surveillance systems have many limitations—they are unable to store recorded video in local and remote locations or provide video access to mobile or remote users.

Network-centric video surveillance components include the following:

- *Cisco Video Surveillance Manager*—Enables IT administrators and security personnel to view, manage and record video locally and remotely using the IP network and a standard Internet browser. Video can be securely accessed anywhere, at any time, enabling faster response, investigation and resolution of incidents. Video can be recorded and stored locally off and at the main site allowing it to be managed and aggregated with video from multiple locations.
- *Cisco Video Surveillance Media Server*—A highly scalable and reliable video management platform that manages, replicates, distributes and archives video systems.

- *Cisco Video Surveillance Operations Manager*—A web-based user interface that authenticates and manages access to video feeds. It is a centralized administration tool for the management of Media Server hosts, Virtual Matrix hosts, cameras, encoders, and viewers.
- *Cisco Video Surveillance Media Virtual Matrix*—Monitors video feeds in command center and other 24-hour monitoring environments. It allows operators to control the video being displayed on multiple local and remote digital monitors.

Digital Media Systems

- *The Cisco Digital Media Suite*—A comprehensive portfolio of digital signage, desktop video, and enterprise TV components and applications that can be centrally managed. The Cisco Digital Media Suite is comprised of three distinct subsystems.
- *Cisco Digital Signs*—Provides scalable centralized management and publishing of compelling digital media to networked, on-premise digital signage displays. It enables the disseminations news and emergency information to large screens connected to the Enterprise existing network. The same content to all signs in the network can be delivered.
- *Cisco Cast*—Uses the same hardware as Cisco Digital Signs, but has different usage models. With Cast, all control switches to the end user via a remote control—and with the latest release, IP phones, smartphones, and touch screens—can be used to control what content comes to the screen. Cast has three user interfaces, one to access VoDs, one for scrolling through live channels, and a channel guide,
- *Cisco Show and Share*—Enables employees to create, capture, and receive live and pre-recorded video on their desktop computers.Digital media can be browsed, searched, and viewed over the network through a unique, easy-to-use Cisco video portal experience—anywhere, anytime.

The components of the Cisco Digital Media Suite include the following:

- *Cisco Digital Media Manager (DMM)*—The central management application for all Cisco Digital Media Suite products. It is used to manage, schedule, and publish compelling digital media for Cisco Digital Signs, Cisco Cast and Cisco Show and Share. As an integrated part of the Cisco Digital Media Suite, this web-based media management application enables content owners to easily upload, catalogue, edit, package, and publish digital media content for live or on-demand playback.
- *Scientific Atlanta Encoder*—Encodes live video input into a MPEG-2 or MPEG-4 multicast stream for Cisco Digital Signs and Cisco Cast.
- *Digital Media Encoders (DME) for Cisco Show and Share*—Register with the DMM and broadcast live video to the Streaming Server using RTSP. Recorded video may be archived to the Content Repository.
- *Streaming Server for Cisco Show and Share*—Provides stream splitting capabilities, allowing many clients to view a single live stream from a DME or pre-recorded source (live rebroadcast).
- *Show and Share User Interface*—Provides the web-based interface for clients. All navigation and authentication is completed through this server.
- *Web Server/Content Repository*—Holds all VoDs referenced by the Show and Share server. All VoD streaming requests to the Show and Share server are redirected to this server. The web server/content repository is also the component that holds all VoDs referenced by the DMM for Cisco Digital Signs and Cisco Cast. For Digital Signs and Cast, all VoD streaming requests issued to the DMP are serviced from this server.
- *Digital Media Player (DMP) for Cisco Digital Signs and Cisco Cast*—Decodes and displays unicast (prerecorded content streamed over http or RTSP) and multicast streamed video as well as flash content (live content from the Scientific Atlanta encoder or other multicast encoder).

- *Cisco LCD Professional Series Displays*—An integral part of the Digital Media System (DMS) suite of products and are used to display information, Cisco LCD displays are available in different sizes and models and offer full 1080p resolution.

Summary

The Small Enterprise Design Profile delivers validated network design and deployment best practices to evolve small enterprise networks into Borderless networks. Enterprise Design Profile applies the best practices from a collection of Cisco Validated Designs (CVD) and integrates these best practices into a customer-based design profile.

For the existing network, the Small Enterprise Design Profile provides guidance for the evolution of the Enterprise network to a Borderless Network. For new networks, the Small Enterprise Design profile steps you from planning your Enterprise network to using technology to enable and solve your business needs.