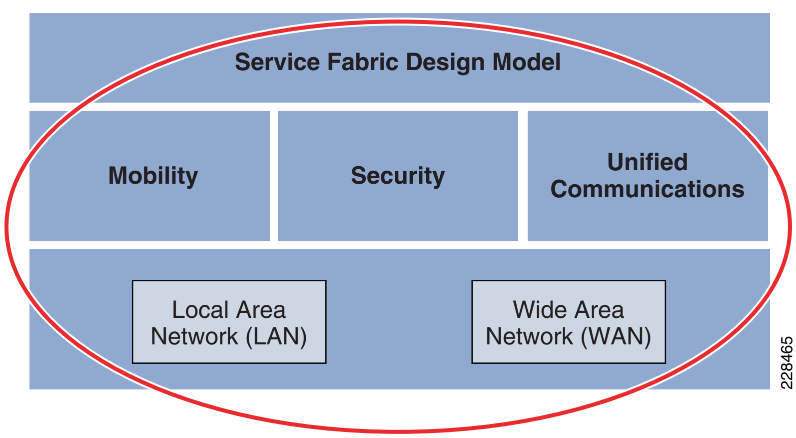
CHAPTER 2

Community College Reference Design—Service Fabric Design Considerations

The service fabric is the foundational network which all Community College services, applications, and solutions use to interact and communicate with one another. Service fabric is the most important component of the Community College reference design. If it fails, all applications, solutions, and technologies employed in the Community College reference design will also fail. Like the foundation of a house, the service fabric must be constructed in a fashion that supports all the applications and services that will ride on it. Additionally, it must be aware of what is type of traffic is transversing and treat each application or service with the right priority based on the needs and importance of that application.

The service fabric is made up of four distinct components local and wide area network (LAN/WAN), security, mobility, and unified communications. Each of these critical foundation components must be carefully designed and tuned to allow for a secure environment that provides business continuity, service awareness and differentiation, as well as access flexibility. See Figure 2-1.

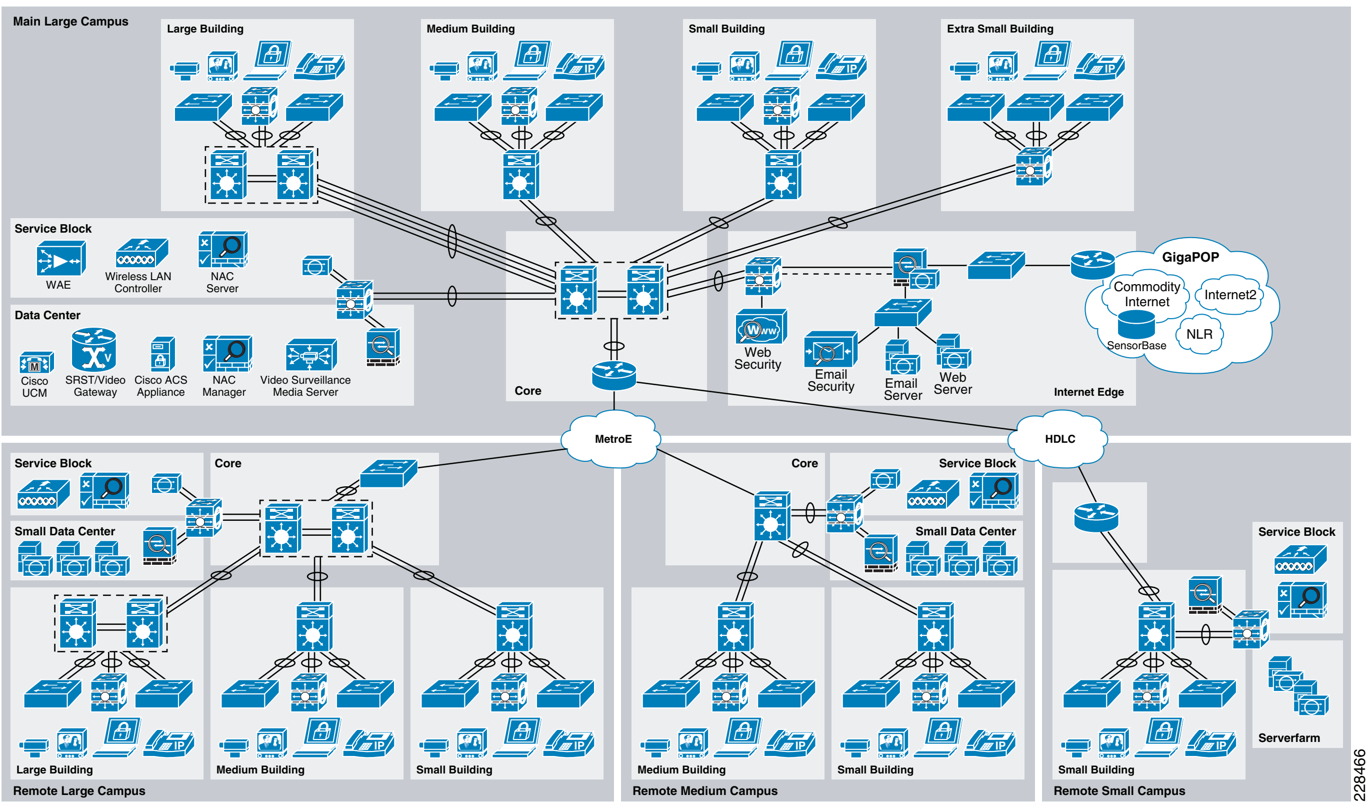
Figure 2-1 Service Fabric Foundation Network



Service Fabric Design Model

The model used for the Community College reference design service fabric is based around the desire to represent as many community college environments as possible. To do that a modular design is used, represented by campuses and buildings of varying sizes (see Figure 2-2). The campuses are made up of one or more building, depending on the campus size profile; buildings are also sized with the determining factor being the number of users or connections to the network in that building as well as physical size. When representing a classroom, an average size of 35 students per classroom or lab is used. Additionally, it is expected that half of all network can be accessed via wireless. This approach allows the network architect to essentially build their own community college environment by mixing the different campus and building profiles provided.

Figure 2-2 Community College Reference Design Overview



Main and Large Campus Design

The main and large campus designs are meant to represent significantly sized campuses containing the largest student, faculty, and staff populations. The profile of the main/large campus is made up of six buildings, the buildings range in size from large to extra small. The buildings will connect back to the resilient core via multiple 10Gb Ethernet links. The core will also connect to a data center design and service block. The large campus will connect to the main campus via a 1Gb Metro Ethernet link. The main campus and large campus are almost identical, with the exception that the main campus is connected to outside entities such as the Internet, Internet2 (I2), regional networks, and the National Lambda Rail using the Internet edge components, and will also have all other campuses within its community college system connecting to it.

Medium Campus Design

The medium campus design is targeted at community colleges campuses that have approximately 3 buildings ranging in size from medium to small. The buildings will connect to the medium campus core via multiple 10Gb links, and the core will also connect to a small data center and service block. The medium campus is connected to the main campus via a 100mb Metro Ethernet link. This link interconnects the medium campus to the other campuses as well as external networks such as the Internet and I2.

Small Campus Design

The small campus profile represents a campus made up of just one building; in this case, the core and distribution networks are collapsed into one. The small campus is connected to the main campus via a fractional DS3 with a 20mb bandwidth rating. This link interconnects the small campus to the other campuses as well as external networks such as the Internet and I2.

Building Profiles

There are four building profiles: large, medium, small, and extra small. All buildings have access switches that connect users. The buildings also have distribution switches that connect the access switches together as well as connect the building itself to the core network.

Large Building Design

The large building is designed for 1600 Ethernet access ports ranging in bandwidth from 100mb to 1Gb. The ports are distributed over four different floors, each floor having 400 access ports. There are 80 wireless access points using the IEEE 802.1 ABGN standards, there are 20 access points per floor; additionally, there are 6 outdoor mesh access points to cover the outdoor skirt of the building. The large building is made up of 80 classrooms, 30 professor offices, 10 administrative offices, and 40 college professionals collectively this represents 160 phones for the large building.

Medium Building Design

The medium building was designed for 800 Ethernet access ports ranging in bandwidth from 100mb to 1Gb. The ports are distributed over two different floors, each floor having 400 access ports. There are 40 wireless access points using the IEEE 802.11 ABGN standards, there are 20 access points per floor; additionally, there are four outdoor mesh access points to cover the outdoor skirt of the building. The medium building is made up of 40 classrooms, 15 professor offices, 5 administrative offices, and 20 college professionals collectively this represents 80 phones for the medium building.

Small Building Design

The small building is designed for 200 Ethernet access ports ranging in bandwidth from 100mb to 1Gb. The ports are all located on one floor. There are 10 wireless access points using the IEEE 802.1 ABGN standards; additionally, there are 2 outdoor mesh access points to cover the outdoor skirt of the building. The small building is made up of 10 classrooms, 8 professor offices, 2 administrative offices, and 10 college professionals collectively this represents 30 phones for the small building.

Extra Small Building Design

The extra small building is designed for 48 100mb Ethernet access ports. The ports are all located on one floor. There are 3 wireless access points using the IEEE 802.1 ABGN standards; additionally, there is 1 outdoor mesh access point to cover the outdoor skirt of the building. The extra small building is made up of 3 classrooms and 7 other phones, totaling 10 phones for the extra small building.

Access Devices

The devices that connect to the Cisco Community College reference design 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 service fabric consists of four major components. The sections below provide a brief description of each of these components.

LAN/WAN Design Considerations

The service fabric LAN/WAN is made up of routers and switches deployed in a three-tier hierarchical model that use Cisco IOS to provide foundational network technologies needed to provide a highly available, application-aware network with flexible access.

LAN Design Considerations

Hierarchical network design model components:

- *Core layer*—The campus 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*—Demarcation point between network infrastructure and access devices. Designed for critical network edge functionality to provide intelligent application and device aware services.

Routing Protocol Selection Criteria

Routing protocols are essential for any network, because they allow for the routing of information between buildings and campuses. Selecting the right routing protocol can vary based on the end-to-end network infrastructure. The service fabric routers and switches support many different routing protocols that will work for community college 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 campus 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.

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 service fabric design must ensures network survivability by following three major resiliency methods pertaining to most types of failures. Depending on the network system tier, role, and network service type the appropriate resiliency option should be deployed:

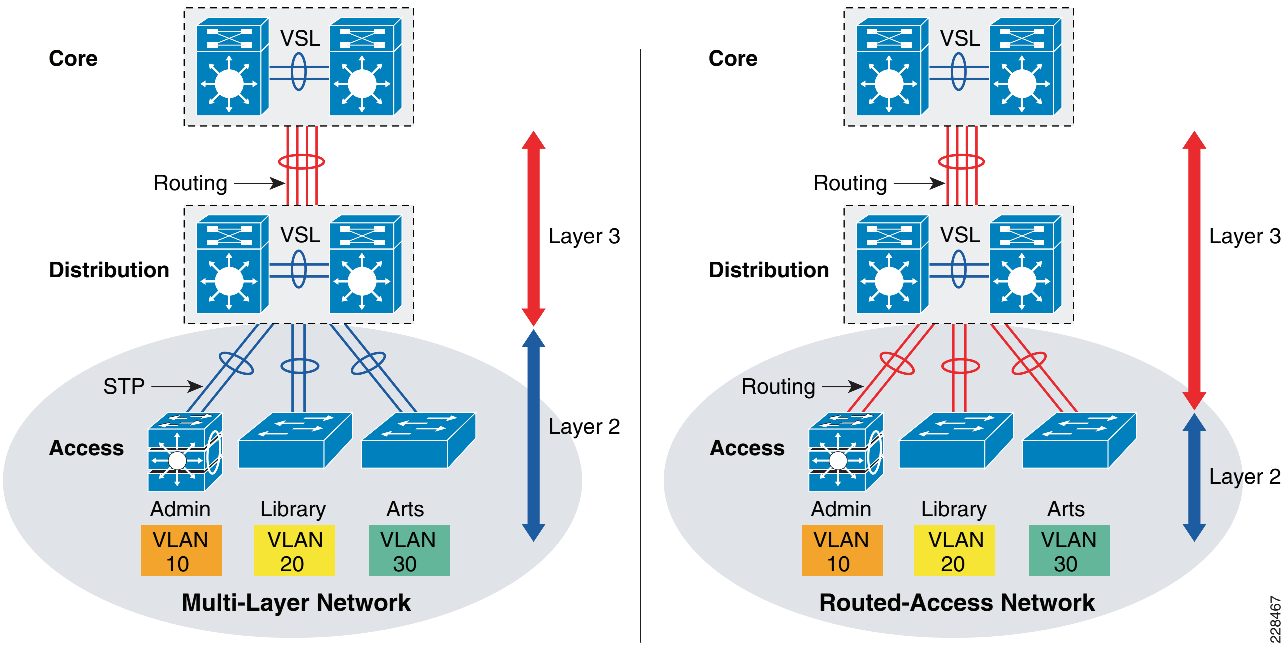
- *Link resiliency*—Provides redundancy during physical link failures (i.e., fiber cut, bad transceivers, incorrect cablings, etc.)
- *Device resiliency*—Protects network during abnormal node failure triggered by hardware or software (i.e., software crashes, non-responsive supervisor etc.)
- *Operational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

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 up to the network distribution, and the layer of communication used 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 function one tier down on Layer 3 access switches changes traditional multilayer network topology and the forwarding path. The implementing of a Layer 3 access does not require any physical or logical link reconfiguration or changes. See Figure 2-2.

Figure 2-3 Control Function in Multi-Layer and Routed-Access Network Design



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

LAN Service Fabric Foundational Services

The service fabric uses essential foundational services to efficiently disseminate information that are 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 community college system is paramount. Some of the key foundational services discussed include the following:

- Multicast routing protocol design considerations
- Designing QoS in campus network

WAN Design Considerations

WAN Transport

In order for campuses to communicate with one another and/or to communicate outside the community college system, network traffic must traverse over a WAN. WAN transport differs greatly from LAN transport due to the 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:

- MPLS/VPN
- Internet

- Metro Ethernet

WAN Service Fabric Foundational Services

Similar to the LAN, the WAN must deploy essential foundational services to ensure the proper transport and prioritization of community college services, the WAN Service Fabric Foundation Services considered are as follows:

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

Security Design Considerations

Security of the Community College reference design service fabric is essential. Without it, community college solutions, applications, and services are open to be compromised, manipulated, or shut down. The service fabric was developed with the following 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, Internet2 and National LambdaRail (NLR) networks and protecting internal resources and users from malware, viruses, and other malicious software. Protecting students, staff and faculty from harmful content. Enforcing E-mail and web browsing policies.
- *Data center protection*—Ensuring the availability and integrity of centralized applications and systems. Protecting the confidentiality and privacy of student, staff and faculty records.
- *Network access security and control*—Securing the access edges. Enforcing authentication and role-based access for students, staff and faculty residing at the main and remote campuses. Ensuring systems are up-to-date and in compliance with the CCVE institution's network security policies.
- *Network endpoint protection*—Protecting servers and school-controlled systems (computer labs, school-provided laptops, etc.) from viruses, malware, botnets, and other malicious software. Enforcing E-mail and web browsing policies for staff and faculty.

Each of these security design considerations are discussed in further detail in Chapter 6, "Community College Security Design."

Mobility

Mobility is an essential part of the community college environment. Most students will connect wirelessly to campus networks. Additionally, 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 students, staff and guests to be accessible and productive, regardless of whether they are meeting in a study hall, at lunch with colleagues in the campus cafeteria, or simply enjoying a breath of fresh air outside a campus building. Provide easy, secure guest access to college guests such as alumni, prospective students, 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. Faculty and other staff 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*—College network administrators must be able to easily deploy, operate, and manage hundreds of access points within multiple community college campus deployments. A single, easy to understand WLAN management framework is desired to provide small, medium and large community college 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 students, faculty, staff and visitors in the event of common failures.

Unified Communications

Call Processing Considerations

How calls are processed in the community college environment is an important design consideration, guidance on designing scalable and resilient call processing systems is essential for deploying a unified communications system. Some of the 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). Several considerations for gateways include the following:

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

Dial Plan Considerations

The dial plan is one of the key elements of an 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 for this reason the service fabric must take survivability into consideration.