International Journal of Engineering Sciences Paradigms and Researches (IJESPR)
(Vol. 22, Issue 01) and (Publishing Month: July 2015)
(An Indexed, Referred and Impact Factor Journal)
ISSN (Online): 2319-6564
www.ijesonline.com

Network Admission Control & Quality of Service in Small Enterprise Networks

Dr. Rajeev Yadav[1], Er. Shreya Sharma[2], Er. Geet Kalani[3] and Dr. Avinash Sharma[4]

[1]Professor in CSE, RCEW, Jaipur, Rajasthan (India)
yadavrajeev6@gmail.com

[2]Asstt. Professor, RCEW, Jaipur, Rajasthan (India)
shreyashrma444@gmail.com

[3]Asstt Professor, RCEW, Jaipur, Rajasthan (India)
kalanivmrgg@gmail.com

[4]Principal RCEW, Jaipur, Rajasthan (India)
principal@rcew.ac.in

Abstract

This paper presents a design model for small enterprise networks including the network admission control criteria. Network Admission Control (NAC) refers to Cisco's version of Network Access Control, which restricts access to the network based on identity or security posture. Network Admission Control is the connection establishment, after that QoS comes in consideration. To maintain the QoS in Small Enterprises Network a modular design profile also given as a solution for sites of varying sizes.

Keywords: *Network Admission Control, QoS, QoS Toolset, Admission Control.*

I. Introduction

Admission Control is a validation process in communication systems where a check is performed before a connection is established to see if current resources are sufficient for the proposed connection. Network Admission Control (NAC) refers to Cisco's version of Network Access Control, which restricts access to the network based on identity or security posture. When a network device (switch, router, wireless access point, DHCP server, etc.) is configured for NAC, it can force user or machine authentication prior to granting access to the network. In addition, guest access can be granted to a quarantine area for remediation of any problems that may have caused authentication failure. This is enforced through an inline custom network device, changes to an existing switch or router, or a restricted DHCP class. A typical (non-free) WiFi connection is a form of NAC. The user must present some sort of credentials before being granted access to the network. In its initial phase, the Cisco Network Admission Control (NAC) functionality enables Cisco routers to enforce access privileges when an endpoint attempts to connect to a network. This access decision can be on the basis of information about the endpoint device, such as its current antivirus state. The antivirus state includes information such as version of antivirus software, virus definitions, and version of scan engine. A basic form of NAC is the 802.1X standard as shown in Figure 1.1.

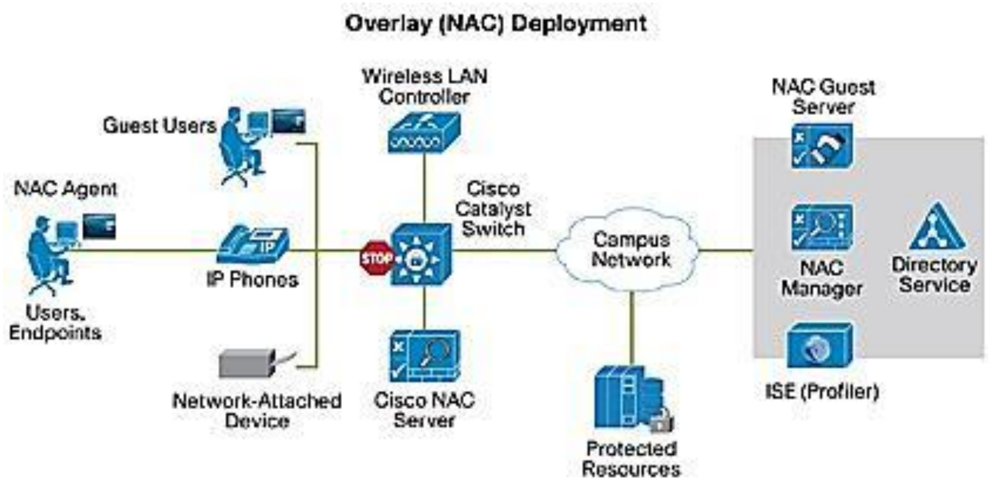

Figure 1.1 Basic Form of NAC

QoS is the measure of transmission quality and service availability of a network (or internetworks). Service availability is a crucial foundation element of QoS. The network infrastructure must be designed to be highly available before you can successfully implement QoS. The target for High Availability is 99.999 % uptime, with only five minutes of downtime permitted per year. The transmission quality of the network is determined by the following factors:

- **Loss:** A relative measure of the number of packets that were not received compared to the total number of packets transmitted. Loss is typically a function of availability. If the network is Highly Available, then loss during periods of non-congestion would be essentially zero. During periods of congestion, however, QoS mechanisms can determine which packets are more suitable to be selectively dropped to alleviate the congestion.
- **Delay:** The finite amount of time it takes a packet to reach the receiving endpoint after being transmitted from the sending endpoint. In the case of voice, this is the amount of time it takes for a sound to travel from the speaker's mouth to a listener's ear.
- **Delay variation (Jitter):** The difference in the end-to-end delay between packets. For example, if one packet requires 100 ms to traverse the network from the source endpoint to the destination endpoint and the following packet requires 125 ms to make the same trip, then the delay variation is 25 ms.

Need of QoS: A communications network forms the backbone of any successful organization. These networks transport a multitude of applications, including realtime voice, high-quality video and delay-sensitive data. Networks must provide predictable, measurable, and sometimes guaranteed services by managing bandwidth, delay, jitter and loss parameters on a network.

QoS technologies refer to the set of tools and techniques to manage network resources and are considered the key enabling technology for network convergence. The objective of QoS technologies is to make voice, video and data convergence appear transparent to end users. QoS technologies allow different types of traffic to contend inequitably for network resources. Voice, video, and critical data applications may be granted priority or preferential services from network devices so that the quality of these strategic applications does not degrade to the point of being unusable. Therefore, QoS is a critical, intrinsic element for successful network convergence. QoS tools are not only useful in protecting desirable traffic, but also in providing deferential services to undesirable traffic such as the exponential propagation of worms.

QoS Tool Set: The main categories of the toolset are

- Admission Control tools
- Classification and Marking tools
- Policing and Markdown tools
- Scheduling tools
- Link-specific tools
- Auto QoS tools

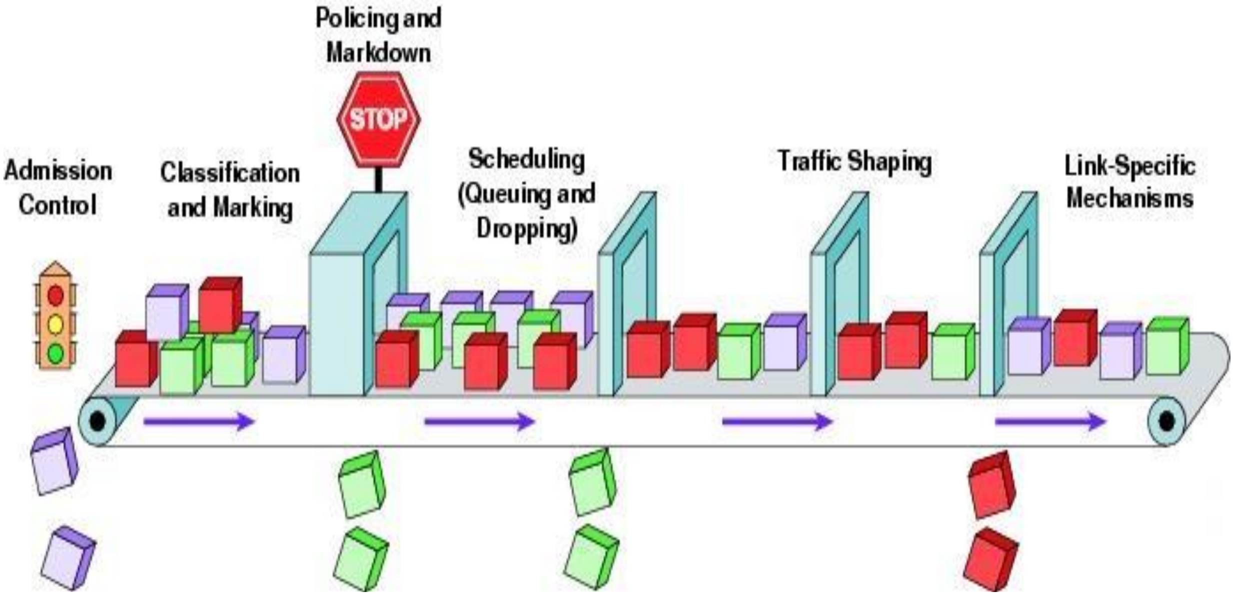

Figure 1.2 QoS Toolset

Figure 1.2 is a complete toolset of QoS features and solutions for addressing the diverse needs of voice, video and multiple classes of data applications. QoS technology lets complex networks control and predictably service a variety of networked applications and traffic types. We can effectively control bandwidth, delay, jitter, and packet loss with these mechanisms. By ensuring the desired results, the QoS features lead to efficient, predictable services for business-critical applications.

Admission Control Tools: After performing the calculations to provision the network with the required bandwidth to support voice, video and data applications, you must ensure that voice or video do not oversubscribe the portion of the bandwidth allocated to them. While most DiffServ QoS features are used to protect voice from data, Call Admission Control (CAC) tools are used to protect voice from voice and video from video.

CAC tools fall into the following three main categories:

- **Local:** Local CAC mechanisms are a voice gateway router function, typically deployed on the outgoing gateway. The CAC decision is based on nodal information such as the state of the outgoing LAN/WAN link that the voice call traverses if allowed to proceed. Local mechanisms include configuration items to disallow more than a fixed number of calls. If the network designer already knows that no more than five VoIP calls will fit across the outgoing WAN link's LLQ configuration because of bandwidth limitations, then it would be recommended to configure the local gateway node to not allow more than five simultaneous calls.

- **Measurement-Based:** Measurement-based CAC techniques look ahead into the packet network to gauge the state of the network to determine whether or not to allow a new call. This usually implies sending probes to the destination IP address, which could be the terminating gateway or endpoint, or another device in between. The probes return to the outgoing gateway or endpoint information on the conditions found while traversing the network to the destination. Typically, loss and delay characteristics are the interesting elements of information for voice CAC decisions. The outgoing device then uses this information in combination with configured information to decide if the network conditions exceed a given or configured threshold.

- **Resource-Based:** There are two types of resource-based mechanisms: those that calculate resources needed and/or available, and those that reserve resources for the call. Resources of interest include link bandwidth, DSPs and DS0 timeslots on the connecting TDM trunks to a voice gateway, CPU power and memory. Several of these resources could be constrained at one or more nodes that the call traverses to its destination.

Classification and Marking Tools: The first element to a QoS policy is to classify/identify the traffic that is to be treated differently. Following classification, marking tools can set an attribute of a frame or packet to a specific value. Such marking (or remarking) establishes a trust boundary that scheduling tools later depend on. Classification and marking tools set this trust boundary by examining any of the following:

- Layer 2 parameters—802.1Q Class of Service (CoS) bits, Multiprotocol Label Switching Experimental Values (MPLS EXP)
- Layer 3 parameters—IP Precedence (IPP), Differentiated Services Code Points (DSCP), IP Explicit Congestion Notification (ECN), source/destination IP address
- Layer 4 parameters— L4 protocol (TCP/UDP), source/destination ports
- Layer 7 parameters— application signatures via Network Based Application Recognition (NBAR)

Policing and Markdown Tools: Policing tools (policers) determine whether packets are conforming to administratively-defined traffic rates and take action accordingly. Such action could include marking, remarking or dropping a packet. A basic policer monitors a single rate: traffic equal to or below the defined rate is considered to conform to the rate, while traffic above the defined rate is considered to exceed the rate. On the other hand, the algorithm of a dual-rate policer (such as described in RFC 2698) is analogous to a traffic light. Traffic equal to or below the principal defined rate (green light) is considered to conform to the rate. An allowance for moderate amounts of traffic above this principal rate is permitted (yellow light) and such traffic is considered to exceed the rate. However, a clearly-defined upper-limit of tolerance is set (red light), beyond which traffic is considered to violate the rate.

Scheduling Tools: Scheduling tools determine how a frame/packet exits a device. Whenever packets enter a device faster than they can exit it, such as with speed mismatches, then a point of congestion, or bottleneck, can occur. Devices have buffers that allow for scheduling higher-priority packets to exit sooner than lower priority ones, which is commonly called queueing.

Queueing algorithms are activated only when a device is experiencing congestion and are deactivated when the congestion clears. The main IOS software queuing tools are Low Latency Queueing (LLQ), which provides strict priority servicing and is intended for realtime applications such as VoIP; and Class-Based Weighted Fair Queuing (CBWFQ), which provides bandwidth guarantees to given classes of traffic and fairness to discrete traffic flows within these traffic classes.

Link-Specific Tools: Link-specific tools include the following:

- **Shaping Tools:** A shaper typically delays excess traffic above an administratively-defined rate using a buffer to hold packets and shape the flow when the data rate of the source is higher than expected.
- **Link Fragmentation and Interleaving Tools:** With slow-speed WAN circuits, large data packets take an excessively long time to be placed onto the wire. This delay, called serialization delay, can easily cause a VoIP packet to exceed its delay and/or jitter threshold. There are two main tools to mitigate serialization delay on slow (768 kbps) links: Multilink PPP Link Fragmentation and Interleaving (MLP LFI) and Frame Relay Fragmentation.
- **Compression Tools:** Compression techniques, such as compressed Real-Time Protocol,

minimize bandwidth requirements and are highly useful on slow links. At 40 bytes total, the header portion of a VoIP packet is relatively large and can account for nearly two-thirds or the entire VoIP packet.

- **Transmit Ring (Tx-Ring) Tuning:** The Tx-Ring is a final interface First-In-First-Out (FIFO) queue that holds frames to be immediately transmitted by the physical interface. The Tx-Ring ensures that a frame is always available when the interface is ready to transmit traffic, so that link utilization is driven to 100 % of capacity. The size of the Tx-Ring is dependent on the hardware, software, Layer 2 media, and queueing algorithm configured on the interface. The Tx-Ring may have to be tuned on certain platforms/interfaces to prevent unnecessary delay/jitter introduced by this final FIFO queue.

AutoQoS Tools: The richness of the QoS toolset inevitably increases its deployment complexity. To address customer demand for simplification of QoS deployment, has developed the Automatic QoS (AutoQoS) features. AutoQoS is an intelligent macro that allows an administrator to enter one or two simple AutoQoS commands to enable all the appropriate features for the recommended QoS settings for an application on a specific interface.

AutoQoS VoIP, the first release of AutoQoS, provides best-practice QoS designs for VoIP on Catalyst switches and IOS routers. By entering one global and/or one interface command, depending on the platform, the AutoQoS VoIP macro expands these commands into the recommended VoIP QoS configurations (complete with all the calculated parameters and settings) for the platform and interface on which the AutoQoS is being applied. For Campus Catalyst switches, AutoQoS automatically performs the following tasks:

- Enforces a trust boundary at IP Phones.
- Enforces a trust boundary on Catalyst switch access ports and uplinks/downlinks.
- Enables Catalyst strict priority queuing for voice and weighted round robin queuing for data traffic.
- Modifies queue admission criteria.
- Modifies queue sizes as well as queue weights where required.

II. Small Enterprise Design Profile

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
- 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 1.3.

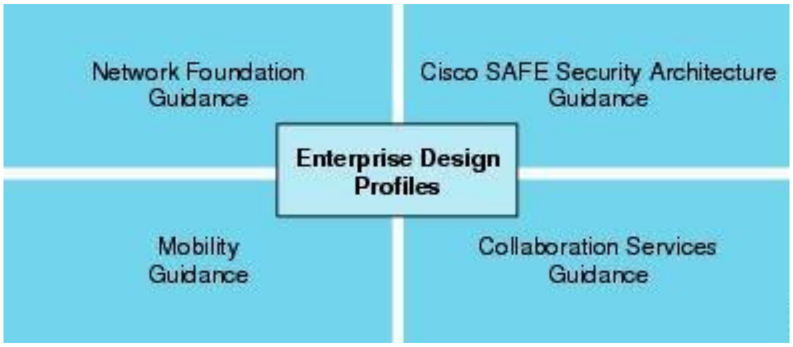
Network Foundation Guidance
Cisco SAFE Security Architecture Guidance
Enterprise Design Profiles
Mobility Guidance
Collaboration Services Guidance

Figure 1.3 Small Enterprise Design Profile Design Components

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 1.4). 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.

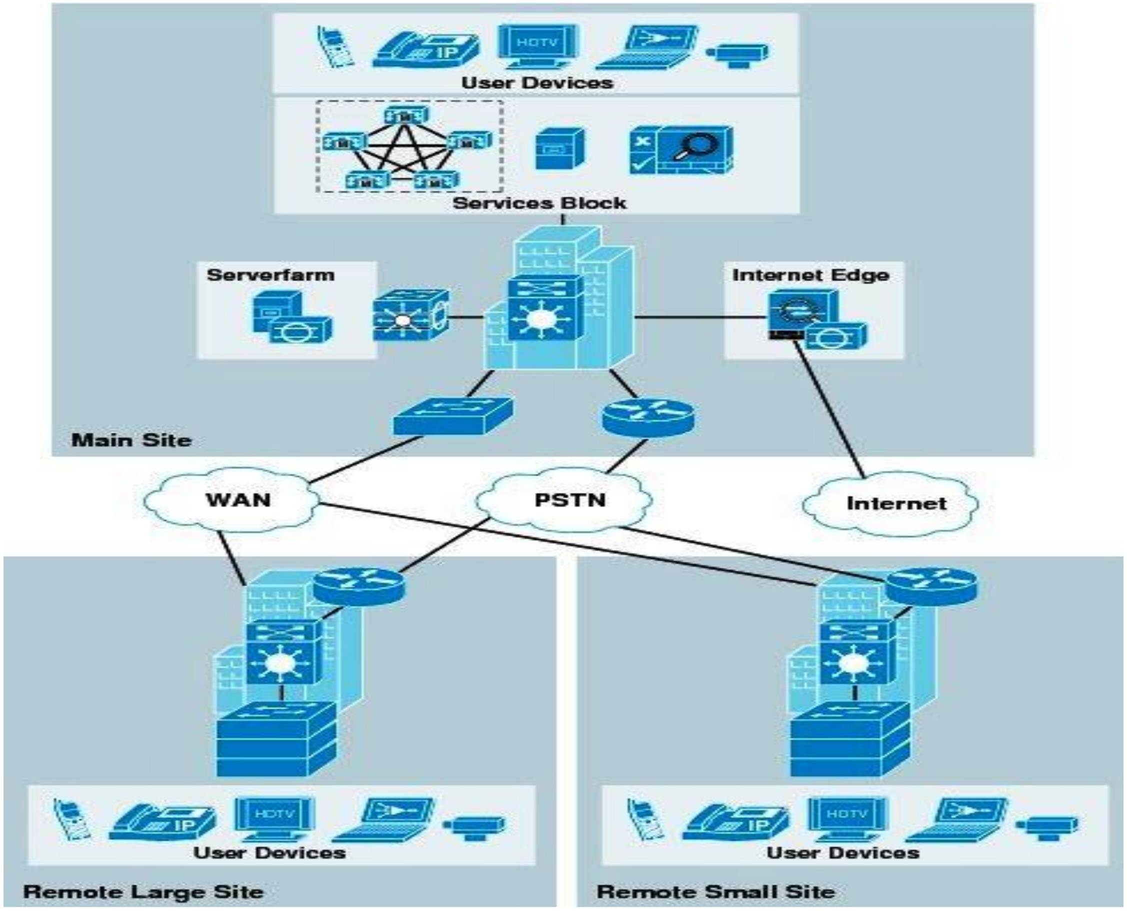

Figure 1.4 Small Enterprise Design Profile Design

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

III. Network Foundation Design Considerations

a) 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.

b) High Availability Design Considerations:

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.

c) 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.

d) 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.

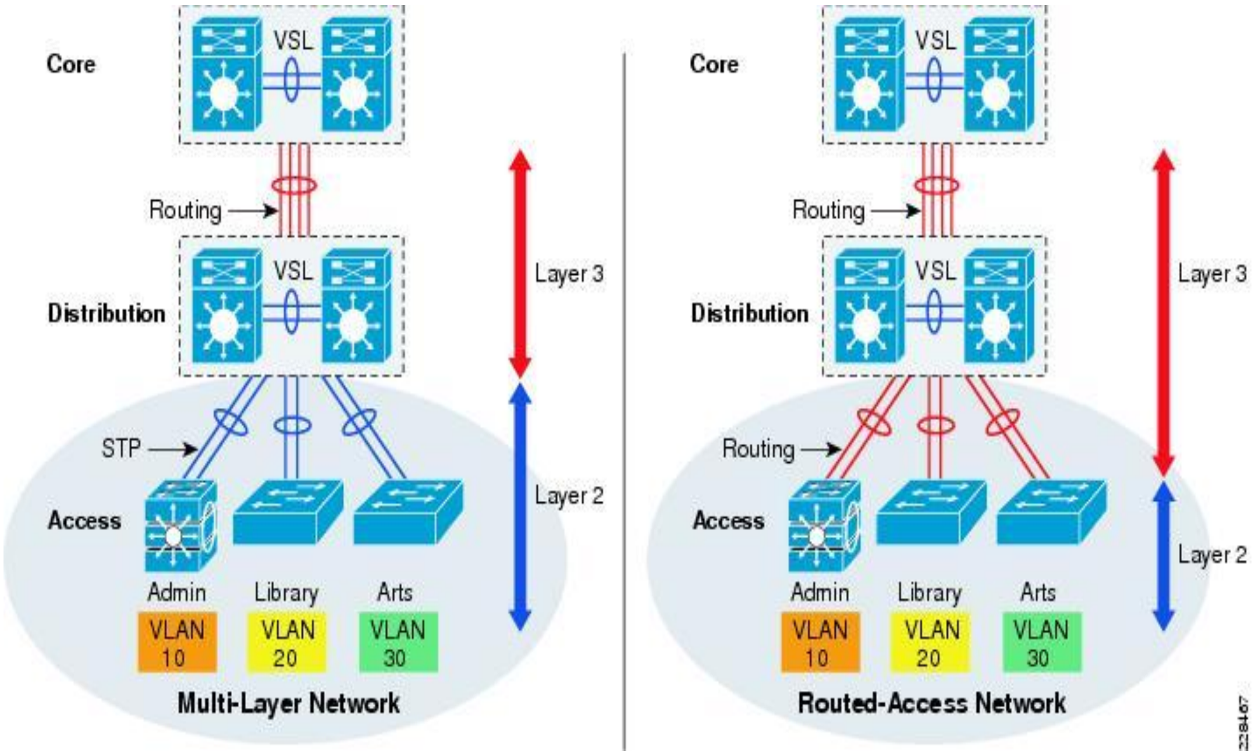

Figure 1.5 Control Function in Multi-Layer and Routed-Access Network Design

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 as shown in Figure 1.5.

e) 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

f) WAN Design Considerations:

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

IV. Security Architecture Guidance

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 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.

V. Mobility Guidance

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.

VI. Collaboration Services Design Consideration

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.

a) 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

b) 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:

•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.

•Video Surveillance Media Server: A highly scalable and reliable video management platform that manages, replicates, distributes and archives video systems.

•**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.

•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.

c) Digital Media Systems:

•Digital Media Suite: A comprehensive portfolio of digital signage, desktop video, and enterprise TV components and applications that can be centrally managed. Digital Media Suite is comprised of three distinct subsystems.

•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.

•Cast: Uses the same hardware as 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,

•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 video portal experience—anywhere, anytime.

VII. Conclusion

The Small Enterprise Design Profile and NAC deliver validated network design and deployment best practices to evolve small enterprise networks into Borderless networks. For the existing network, the Small Enterprise Design Profile & NAC provides guidance for the evolution of the Enterprise network to a Borderless Network. For new networks, the Small Enterprise Design profile & NAC steps you from planning your Enterprise network to using technology to enable and solve your business needs.

References

[1] Joel Snyder, Network access control vendors pass endpoint security testing - Alcatel-Lucent, Bradford, Enterasys, ForeScout, McAfee go above and beyond, Network World , June 21, 2010

[2] RFC 791 “Internet Protocol Protocol Specification”

[3] http://www.networkcomputing.com/data-protection/229607166?pgno=3

[4] RFC 2474 "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers

[5] IEEE 802.16 Task Group ‘m,’ “IEEE 802.16m Evaluation Methodology Document,” Jan. 2009.

[6] RFC 2597 "Assured Forwarding PHB Group"

[7] ITU-R M.1822 Rec., “Framework for Services Supported by IMT,” Oct. 2007.

[8] RFC 2697 "A Single Rate Three Color Marker"

[9] RFC 2698 "A Two Rate Three Color Marker"

[10] WiMAX Forum, “Network Architecture Stage 2–3,” Rel.1, v. 1.2, Jan. 2008; http://www.wimaxforum.org/technology/documents

[11] RFC 3168 "The Addition of Explicit Congestion Notification (ECN) to IP"

[12] Szigeti, Tim and Christina Hattingh. End-to-End QoS Network Design: Quality of Service in LANs, WANs and VPNs. Indianapolis: Press, 2004.

[13] IEEE Standard for Local and metropolitan area networks, Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems-Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum IEEE Computer Society and the IEEE Microwave Theory and Techniques Society, February 2006.

[14] IOS QoS Configuration Guide – IOS version 12.3

[15] C. Cicconetti, L. Lenzini, E. Mingozzi, C. Eklund, ”Quality of service support in IEEE 802.16 networks”, IEEE Networks, Vol. 20, No. 2, March-April 2006, Page(s):50 - 55.

[16] IOS Configuration Guide – Configuring Data Link Switching Plus - IOS version 12.3

[17] Understanding How Routing Updates and Layer 2 Control Packets Are Queued on an Interface with a QoS Service Policy

[18] http://www.ashimmy.com/2007/03/a_brief_history.html