IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-7, Issue-6, June 2019 E-ISSN: 2347-2693

Simulation of Wide Area Network for Multiple Offices Connectivity Using Enhanced Interior Gateway Routing Protocol (EIGRP)

[1*]Amanze B.C., [2]Nwoke B.C , [3]Agoha U.K

[1,2]Dept. of Computer Science, Imo State University, Owerri, Imo State, Nigeria
[3]Dept. of Computer Science, Imo State University, Owerri, Imo State, Nigeria

DOI: https://doi.org/10.26438/ijcse/v7i6.10451050 | Available online at: www.ijcseonline.org

Accepted: 10/Jun/2019, Published: 30/Jun/2019

Abstract- Wide Area Network (WAN) is a critical important functionality of modern businesses because latency, jitter and packet loss associated with WAN often causes performance of applications to degrade, the outage of WAN link often causes one or more sites to be offline and the lead time to either install a new WAN link or to increase the capacity of existing WAN link can be quite lengthy. This paper focuses on the summary of the key components of some of the emerging approaches to WAN architecture and design and concludes with a call to action that outlines a project plan that network organizations can use to evolve their WAN. The motivation for this paper is to reduce the cost of transmission lines and equipment and improve network performance and response time. The approach taken in the design is based on approaching the high availability service problem from three perspectives; network resiliency, device resiliency and operational resiliency. Top down methodology which considers requirement analysis before technology selection is used. Packet tracer and operating Cisco IOS software are the design tools employed in the implementation of this paper.

Keyword: WAN, EIGRP, QoS and Top Down Methodology.

I. INTRODUCTION

Over the decades, enterprise network design and implementation have undergone different changes and various design considerations has been established. This chapter tries to review various concepts in line with the subject matter. Enterprise networks are the bedrock of communication in enterprises. They allow communication between several sites of a single company. Enterprise networks have evolved dramatically in the last two decades. The evolution has been fuelled by advances in Digital Signal Processing (DSP) technology, optical communications, packet technology, traffic and network convergence, etc. Voice and real-time video, unlike data, are time sensitive and traditionally can only be carried by Pulse Code Modulation (PCM) coded medium [1]. The data network is not optimized for time-sensitive traffic. Traditionally, voice traffic is transported using a channel capacity of 64 Kbps (EO) and multiple channels are used to support video, which is image intensive. This means that for any enterprise network to support voice, video or data traffic, lease lines, which are multiples of DSO/EO, would be purchased from traditional telephone companies.

In the last decade, advances in DSP led to sophisticated codes, and lower bit rates such as 8, 16 and 32 kbps are now being used to code voice using Code Excitable linear Predictor (CELP). The coding of data [2], video [3]: [4] and [5] [6] and voice [7]; [8] has constituted a major active area in the past few decades, but most recently variations of JPEG and MPEG were developed for moving picture and audio. These coders ensure the transmission of hi-fi music and the synchronization of moving pictures with the associated audio.

Traditionally, voice and data have separate networks, but the advances in DSP and packet technologies have led to convergent traffic sources and network.

So, enterprise network architecture has evolved from separate networks for each traffic type, for each enterprise site to a converged network per site. Data switches are essential for enterprise network connectivity. The X.25 was the first of the many data switches one have today. X.25 was developed at the time of poor transmission media and it contains an error control mechanism, which in turn slows the processing of data. As the transmission medium improved, the frame Relay (FR) was developed. FR and Asynchronous Transfer Mode (ATM) switches use virtual links to connect enterprise networks together. Though packet networks are not optimized for voice traffic, voice over packets or IP thrives in the enterprise networks. The Voice over Internet Protocol (VoIP) in an enterprise network environment emulates the traditional circuit-switched voice quality levels very well. Most companies that span several geographic-areas use their own VoIP in their enterprise network for employees to make voice calls to their different branch offices. Moreover, Quality of Service (QoS) is guaranteed in an enterprise environment because all the network elements are owned by the same corporation. Established QoS mechanisms such as Differentiated Service (DiffServ), Integrated Services (InlServ) and Multi- Protocol Labelling Switch (MPLS) can be combined, as suggested elsewhere [9]; [10]; [11] in enterprise network environments such that quality is guaranteed.

II. STATEMENT OF THE PROBLEM

The establishment of communication and or interaction of various business sites (main office, branch office and sales outlets) for the purpose of resource sharing is the focus of this paper. Each location/site/branch is IP addressable requiring management, monitoring and control. Poor design and implementation of enterprise network presents significant burden to the network administrator and often poor service availability to the concerned organization. The traditional approach to packet switching (X.25), used in-band signaling, and includes end-to-end and well as per-hop flow control and error control. This approach results in considerable overhead. These were typically DS0 (56 Kbps!) connections, and then the more expensive T1/E1 or T3/E3 connections, and given their significant expense, fractional T1 or T3 lines as well.

Traditionally, this was done using private lines, or circuit switching over a leased line. However, this method has several drawbacks, mainly that it becomes prohibitively expensive as the size of the network increases - both in terms of miles and number of LANs. The reason for the high-cost is that high-speed circuits and ports must be setup on a point-to-point basis between an increasing numbers of bridges. Also, circuit-mode connectivity results in a lot of wasted bandwidth for the burst traffic that is typical of LANs. On the other hand, traditional X.25 oriented packet switching networks entailed significant protocol overheads and have historically been too slow - primarily supporting low-speed terminals at 19.2 kbps and lower. Frame relay provides the statistical multiplexing interface of X.25, without its overhead. Besides, it can handle multiple data sessions on a single access line, which means that hardware and circuit requirements are reduced. Frame relay is also scalable - implementations are available from low bandwidths (eg, 56 kbps), all the way up to T1 (1.544 Mbps) or even T3 (45 Mbps) speeds.

III. OBJECTIVES OF THE STUDY

The objectives of this paper are as follows;

1 To present the design overview of wide area network including the description of best design consideration, topologies, configuration design guidelines and other considerations relevant to the design of highly available, full service, enterprise switching network.

2 To address the need for increased desire for mobility, the drive for heightened security and the need to accurately identify and segment users, devices and networks in other to present how business partner and work with other branches or organization.

3 To focus on the overall cisco guidelines that addresses enterprise network using latest advanced service technologies from cisco and is based on the best practice design and implementation principles that have been tested in enterprise system environment.

4 To introduce the key architectural components and services that are necessary to deploy a highly available, secure and service rich enterprise network.

5 To serve as a guide to direct readers to more specific campus design best practices and configuration examples.

IV. SIGNIFICANCE OF THE STUDY

Businesses have growing impact in this age of globalization. They are said to be major social and economic contributor to any country's economy because they provide increasing production and employment growth [12]. This increasing popularity has placed enormous pressure on both small, medium and large scale enterprises to enhance the way they run their businesses in order to be more competitive in the current global environment. In order to achieve this competitiveness, they need the right information and more importantly at the right time. Hence they need a concentrated formulation and implementation of information system strategies in order to exploit the benefits of the system. They cannot achieve this except through the adoption of enterprise networking.

Considering the nature of businesses today, their various enterprise outlets/branches need an organized combination of its people, hardware, software, communication networks and data resources that collects, transforms and disseminates information within and among organization. This combination and or communication will make information readily available irrespective of ones location as if they are local.

Successful design of enterprise network will provide a bedrock for other enterprise technologies such as Virtual private network (VPN), Data center (Installation of various servers), cloud resources, Voice over internet protocol (VoIP) etc. For example, though packet networks are not optimized for voice traffics, voice over packets or IP thrives in the enterprise networks. Voice over internet protocol (VoIP) in an enterprise environment emulates the traditional circuit switched voice quality levels very well. Companies that span several floors, buildings or geographic locations use VoIP in their enterprise network for employees to make voice calls across their different branch offices.

Frame relay network reduces the cost of transmission lines and equipment and improves network performance and response time. Designed for transmission lines with a low error rate, frame relay networks provide minimal internal checking, and consequently, error detection and recovery is implemented in the attached user systems. Training costs are significantly minimal as communications or IT personnel learn to manage Frame relay as Data Link Connections (DLCs), in a fashion similar to how they have managed leased lines; virtual circuit replace physical circuits when packet-switching techniques are used. Workstations and workgroups can send mail and access servers over the internetwork riding over Frame relay.

The replacement of leased lines carrying Synchronous Data Link Control traffic by frame relay DLCs provides Systems Network Architecture (SNA) users with the opportunity to save twice and improve performance. Users save first by replacing a leased line (typically 19.2K or 56K bps) with a lower-cost Frame relay connection and, second, by sharing the Frame relay connection with another application. When the Frame relay connection provides more bandwidth to the application than was previously available, performance can be improved as well.

Today's communications networks are built using high-speed digital trunks that inherently provide high throughput, minimal delay, and a very low error rate. Such transmission networks supply highly reliable service without the overhead of error control functions. Frame relay is a packet-mode transmission network service that exploits these network characteristics by minimizing the amount of error detection and recovery performed inside the network.

V. ENTERPRISE NETWORK ARCHITECTURE DESIGN

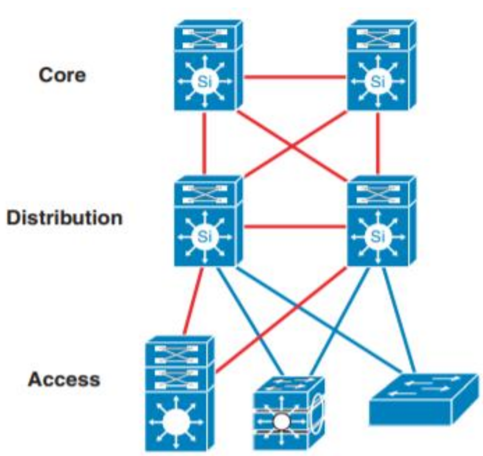

Figure 1: The Layers of Campus Hierarchy

Access

The access layer is the first tier or edge of the enterprise network. It is the place where end devices (PCs, printers, cameras, and the like) attach to the wired portion of the campus network. It is also the place where devices that extend the network out one more level are attached. IP phones and wireless access points (APs) being the prime two key examples of devices that extend the connectivity out one more layer from the actual campus access switch. The wide variety of possible types of devices that can connect and the various services and dynamic configuration mechanisms that are necessary, make the access layer one of the most feature-rich parts of the campus network. The access layer provides the intelligent demarcation between the network infrastructure and the computing devices that leverage that infrastructure. As such it provides a security of Quality of Service and policy trust boundary, it is the first layer of defence in the network security architecture and the first point of negotiation between end devices and the network infrastructure.

Distribution

The distribution layer in the campus design has a unique role in that it acts as a services and control boundary between the access and the core. Both access and core are essentially dedicated special purpose layers. The access layer is dedicated to meeting the functions of end-device connectivity and the core layer is dedicated to providing non-stop connectivity across the entire campus network. The distribution layer on the other hand serves multiple purposes. It is an aggregation point for all of the access switches and acts as an integral member of the access-distribution block providing connectivity and policy services for traffic flows within the access-distribution block. It is also an element in the core of the network and participates in the core routing design. Its third role is to provide the aggregation, policy control and isolation demarcation point between the campus distribution building block and the rest of the network. Going back to the software analog. The distribution layer defines the data input and output between the subroutine (distribution block) and the mainline (core) of the program. It defines a summarization boundary for network control plane protocols (E1GRP. OSPF. Spanning Tree) and serves as the policy boundary between the devices and data flows within the access- distribution block and the rest of the network.

Core

The campus core is in some ways the simplest yet most critical part of the campus. It provides a very limited set of services and is designed to be highly available and operate in an always-on mode. In the modern business world, the core of the network must operate as a non-stop 7*24*365 service. The key design objectives for the campus core are based on providing the appropriate level of redundancy to allow for near immediate data-flow recovery in event of any component (switch, supervisor, line card, or fibre) failure.

V. ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL (E1GRP)

EIGRP is an advanced distance vector routing protocol that was developed by Cisco. It is suited for many different topologies and media. In a well-designed network, it scales well and provides extremely quick convergence time with minimal overhead. EIGRP is a popular choice for routing protocol on Cisco devices. It combines the advantages of link-state and distance vector routing protocol. The following are outstanding features of EIGRP;

Rapid Convergence: It uses Diffusing Update Algorithm (DUAL) to achieve rapid convergence. As a computational engine that runs EIGRP, DUAL resides at the center of the routing protocol, guaranteeing loop free paths and back-up paths throughout the routing domain.

Reduced Bandwidth Usage: it uses terms "'partial" and "bounded" when referring to its updates. It does not make periodic updates. The term "partial" means that the update only includes information about the route changes. EIGRP sends this incremental update when the state of the destination changes instead of sending the entire contents of the routing table. The term "bounded" refers to the propagation of partial updates that are sent only to those routers that the changes affect. By sending only the routing information needed and only to those routers that need it, EIGRP minimizes the bandwidth that is required to send EIGRP updates.

Multiple Network Layer Support: EIGRP supports AppleTalk, IPv4, IPv6 and Novell Internetwork Packet Exchange (IPX) all of which use Protocol Dependent Modules (PDMs). PDMs are responsible for protocol requirements that are specific to the network layer.

Classless Routing: because EIGRP is a classless routing protocol, it advertises a routing mask for each destination network. The routing mask feature enables EIGRP to support discontinuous sub networks and Variable Length Subnet Mask (VLSM).
Less overhead: it uses multicast and unicast rather than broadcast. Multicast EIGRP packets use the reserved multicast address 224.0.0.10. As a result, end stations are unaffected by routing updates and request for topology information.

Load Balancing: EIGRP supports unequal metric load balancing as well as equal metric load balancing which allows administrators to better distribute traffic flow in their networks.

Easy Summarization: it allows administrators to create summary routes anywhere within the network rather than rely on the traditional distant vector approach of performing classily route summarization only at major network boundaries.

VI. ANALYSIS OF THE EXISTING SYSTEM

Over the decades, enterprise network design has seen various technology (design) considerations all in attempt to solve problems of network availability, scalability, cost, security, speed, topology, reliability and above all flexibility.

Routers, switches and network cables are the integral components needed to set up enterprise networks, though other devices like servers (data centre), printers. IP phones and PCs are needed. But how these later devices function will highly depend on the strategic placement, design consideration, configuration and management. The placement, specifications and configuration of these (routers, switches and cables) are critical to the overall performance of the entire network.

6.1 WAN Connection Establishment in Existing System.

Point-to-point (PPP) is used to connect LANs to service provider WAN's and to connect LAN segments within the enterprise network. A LAN-to-WAN point- to-point connection is also referred to as serial connection or leased line connection. This traditional approach to designing a branch office WAN is to have T1 access to service provider's network at each branch office and to have one or more higher speed links at each data centre. In this design, it is common to have all or some of the company's internet traffic be backhauled to a data centre before being handed off to the internet.

6.2 Problems of the existing system

The existing system design has failed to leverage a common set of engineering and architectural principles; hierarchy, modularity, resiliency and flexibility. The engineers fail to understand how each applies to the overall design and how each principle fits in the context of the others. Their design tools and methodology resemble the 'connect-the-dots' game that children usually play. Here internetworking devices are placed on palette and connected using a LAN or WAN media. Hence steps of analysing customers' requirements and selecting devices and media based on those requirements are skipped. The following factors are therefore driving the need to seek alternative WAN design;

1. Application performance problem.
2. Inability to address security issues.
3. Poor network availability.
4. Inability to achieve high level of fault and change isolation.
5. Inability to classify IP packets and implement packet filtering through access control.

6. High cost of implementation.
7. Lack of flexibility, that is, inability to adapt to change without forklift upgrade.

VII. ANALYSIS OF THE CURRENT SYSTEM

In most enterprise business environments, campus networks are no longer new additions to the network. In general, campus networks have evolved through first and second generation build-out cycles and the expected lifecycle for campus networks have increased considerably. At the same time, these networks have become larger and more complex, while the business environment and its underlying communication requirements continue to evolve. Network administrators face unprecedented change in their network environments. The traditional WAN was once a well-controlled perimeter of static-point-to-point connections to the data centre. Most, if not all applications were hosted inside the enterprise, and measures of success focussed on network uptime.

Organizations must therefore adapt to mobile cloud world where more and more applications are hosted in multiple places, including the public cloud and infrastructure-as-a-service (IaaS) cloud. Applications are also distributed across data centres, requiring more data transfers over the WAN. Users expect access from any device, from anywhere and at any time. And the nature of applications is changing becoming more immersive and bandwidth intensive.
Cloud and mobility open a host of security concerns, which are amplified for businesses that are also considering direct internet access for software as a service (SaaS) and mobile devices. The internet of things (IoT) only compounds this problem. And of course, network IT budget and resources will likely remain flat at best. To remain competitive and meet growing business demand, organisations must modernize their WAN for the world of mobility and cloud. Cisco intelligent WAN follows structured approach to optimize application performance without compromising security, reliability and other principles of good design.

The strength of the proposed system therefore is as explained below;

1 **Migration to hybrid WAN:** Building a transport independent architecture that enables the business connect to multiple access networks (Multiprotocol Label Switching (MPLS) and internet with a single overlay for operational simplicity.
2 **Protect and optimize application performance:** Provides organizations a platform to move to an application policy-based model that maximizes usage and improves the application experience through services that provide greater visibility, granular control and maximum optimization.
3 **Promote Greater Automation and Orchestration:** overcome network complexity with a software-based controller model that abstracts the network elements and services and allow IT to direct policy based on business intent with dramatically fewer resources.
4 **Proper Network Management:** Implementing a separate core provides fault isolation and backbone connectivity. Isolating the distribution and core into separate modules creates a clean delineation for change control between activities affecting end stations (PCs. phones, printers) and those that affect data centre. WAN or other parts of the network. It equally provides the ability to scale the size of the network as the network grows.
5 **Proper Security:** VLAN through logical addressing groups' users based on departments and no one outside the department can communicate with them. All remote access to the switches and routers will be through more secured SSI1 rather than telnet. Equally through ACL. Packet forwarding is logically controlled. Implementation of switch-port security ensures that unauthorized "plug ins" are automatically shut down. Unused ports in the switches and routers are shut down.
6 **High Network Availability;** By employing the guiding set of engineering principles such as hierarchy, modularity and flexibility in the design, high network availability is obtained.
7 **Ability to Achieve High Level of Fault and Change Isolation.** In addition to proper network management, implementation of a separate core aids in fault and change isolation. Network resiliency which is largely concerned with how the overall design implements topology redundancy, redundant links and devices, and how the control plane protocols EIGRP and STP are implemented equally helps in this regard.
8 **Ability to Classify IP Packets**: Incorporation of VLAN and ACL helps to classify IP packets and to properly filter packets.
9 **Low cost of Implementation:** Through inter-VLAN routing protocol, various departments irrespective of the location of their users are connected to separate switches and made to communicate. This greatly reduces the number of switches in use. Frame relay is used as a WAN protocol in place of highly costly ISPs PPP.
10 **Provision of Flexibility:** the design aids in the modification of portions of the network, addition new services, or increase capacity without going through a major fork-lift upgrade.

VIII. METHODOLOGY OF THE PROPOSED SYSTEM

Methodology is a systematic description of the steps taken to solve a problem. It therefore describes the collection of procedural, techniques, tools and documentation aids that is employed to solve a problem. Network professionals have the ability to create networks that are so complex that when problem arise; they cannot be solved using the same sought of thinking that was used to create the network. Each upgrade, patch or modification can also be created using complex and sometimes convoluted thinking. Hence' the result is networks that are hard to understand and troubleshoot. The methodology employed in this design is top-down network design methodology. This design methodology recognizes that customer's requirement embodies many business and technical goals including requirements for availability, scalability, affordability, security and manageability. Many customers also want to specify a required level of network performance otherwise called service level. To meet these needs, difficult network design choices and trade-offs must be made when designing the logical network before any physical devices or media is selected. Top-down network design is a methodology for designing networks that begin with the upper layers of OSI reference model before moving to the lower layers. It focuses on application, presentation, session and data transport before selection of routers, switches and media that operate at the lower layers. It includes exploring divisional and group structures to find the people for whom the network will provide services and from whom you should get valuable information to make the design succeed.

Architecture of the Design

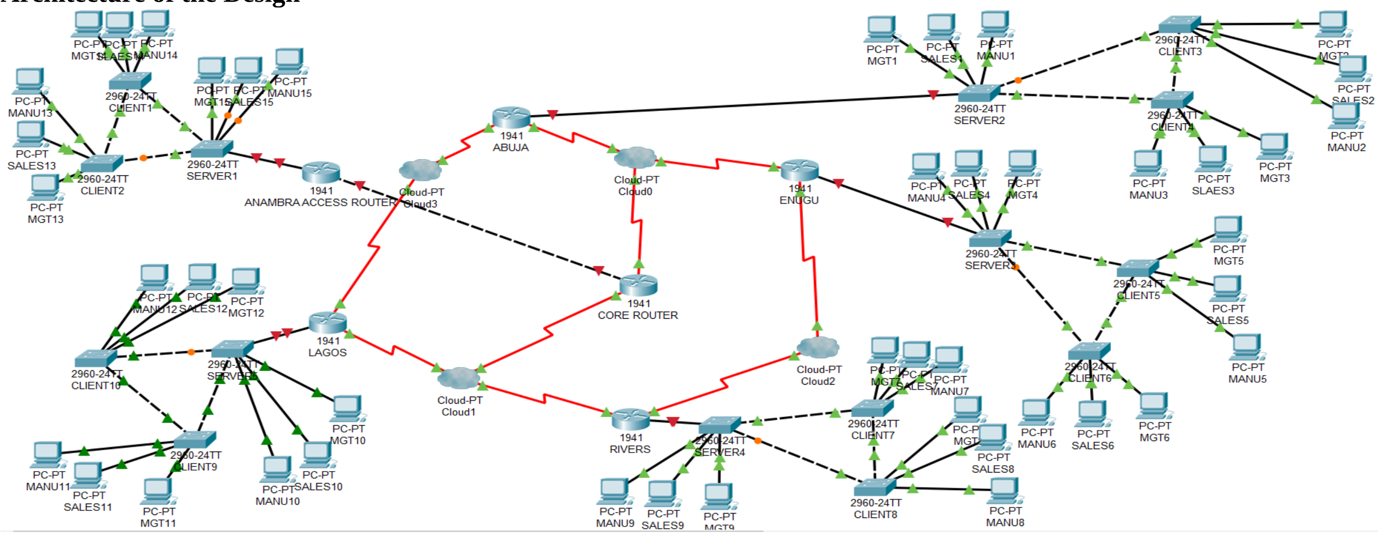

Figure 2: Architecture of the Design

Summary

The paper presents an overview of WAN implementation for multiple office connectivity using EIGRP for routing and frame relay as WAN protocol and includes descriptions of various design considerations, topologies, technologies, configuration, design, guidelines, and other considerations relevant to the design of highly available, full-service campus switching fabric. It is also intended to serve as a guide to direct readers to more specific WAN design best practices and the corresponding benefits of the design.

REFERENCES

[1] Black, U. (1997). Emerging Communications Technologies, 2nd ed., New Jersey: Prentice Hall.

[2] Pawlita, P.F. (1992). "Traffic measurements in data networks: recent measurement results and some implications", IEEE Trans. Comms., April, Vol. Com.30, N0.4

[3] Verbiest (1988). "Broadband ISDN and Asynchronous Transfer Mode (ATM)",@ IEEE Communications Magazine, September, Vol. 27, N0. 9

[4] Odinma-Okafor, A. (1991). "The characteristics of variable rate video signals", Ph.D Thesis in Telecommunications Engineering, The University of London.

[5] Odinma-Okafor, A. and Cosmas, J. (1992). "Impact of time series and counting process approaches to video source modelling", 9th UK Teletraffic Symposium, IEE, April.

[6] Grunenfelder, R., Cosmas, J., Manthorpe, S. and Odinma-Okafor, A. (1990). "The characterization of video codecs as autoregressive moving average processes and related queuing system performance", IEEE J –SAC, April, Vol. 9, N0. 3, pp. 284-293.

[7] Brady P.T. (1965). "A technique for investigating on-off patterns of speech", Bell Syst. Tech. Journal, Vol. XIV, January.

[8] Gruber, J.G. (1992). "A comparison of measured and calculated speech temporal parameters relevant to speech activity detection", IEEE Trans. Comms. April, Vol. COM-30, N0. 4

[9] Milonas, A.C. (2000). "Enterprise networking for the new millennium", Bell Labs. Tech. Journal, January – March, vol. 5, N0. 1, pp. 73-93.

[10] Weiss, W. (1998). "QoS with differential services", Bell Labs Tech. Journal, October –December, pp. 48-62.

[11] Odinma, A.C. and Oborkhale, L. (2006). Quality of Service Mechanisms and Challenges for IP Networks, PJST, May, Vol. 7, N0. 1.

[12] Cisco (2010). Interconnecting Cisco Networking Devices: Part 2, Vol. Version 1.1, United Kingdom.

