VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
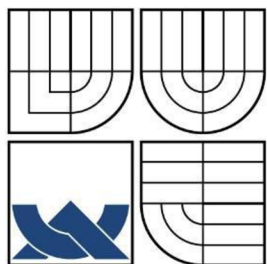DEPARTMENT OF TELECOMMUNICATIONS

ENTERPRISE NETWORK DESIGN AND SIMULATION – CISCO VIRTUAL LAB
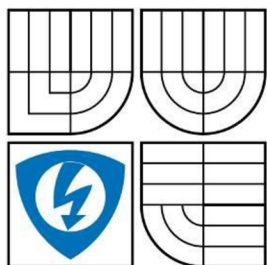
DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE   Bc. KAROL OLLÉ
AUTHOR

BRNO 2008

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

NÁVRH A SIMULACE PODNIKOVÉ SÍTĚ - VIRTUÁLNÍ LABORATOŘ CISCO
ENTERPRISE NETWORK DESIGN AND SIMULATION – CISCO VIRTUAL LAB

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE   Bc. KAROL OLLÉ
AUTHOR

VEDOUCÍ PRÁCE   Ing. MICHAL SOUMAR
SUPERVISOR

BRNO 2008

**VYSOKÉ UČENÍ
TECHNICKÉ V BRNĚ**

**Fakulta elektrotechniky
a komunikačních technologií**

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student: Ollé Karol, Bc.   *ID:* 50445
Ročník: 2   *Akademický rok:* 2007/08

NÁZEV TÉMATU:

Návrh a simulace podnikové sítě, virtuální laboratoř Cisco

POKYNY PRO VYPRACOVÁNÍ:

Navrhněte rozsáhlou podnikovou síť (LAN/WAN). Dokumentace bude obsahovat nákresy topologie z pohledu druhé vrstvy ISO/OSI (IEEE 802.1D, VTP), směrování několika směrovacími protokoly a bezpečnostní pravidla pro konfiguraci aktivních prvků.
Použitý (emulovaný) hardware jsou Cisco směrovače řady 1700, 2600, 3600, 3700 a 7200, firewall Cisco PIX.
Síť realizujte prostřednictvím virtualizačních nástrojů Dynamips/Dynagen, PEMU a její činnost monitorujte např. nástrojem Nagios. Výstupem je virtuální síť pro pokusné a studijní účely.

DOPORUČENÁ LITERATURA:

[1] Teare, D., Paquet, C. Building Scalable Cisco Internetworks (BSCI): Authorized Self-Study Guide. 3rd Edition. Cisco Press, 2006. 864 s. ISBN 1-58705-223-7.
[2] Froom, R, Sivasubramanian, B., Frahim, E. Building Cisco Multilayer Switched Networks (BCMSN): Authorized Self-Study Guide. 4th Edition. Cisco Press, 2007. 984 s. ISBN 1-58705-273-3.
[3] Teare, D. Designing for Cisco Internetwork Solutions (DESGN): Authorized CCDA Self-Study Guide (Exam 640-863). Second Edition. Cisco Press, 2007. 960 s. ISBN 1-58705-272-5.

Termín zadání: 11.2.2008   *Termín odevzdání:* 28.5.2008

Vedoucí projektu: Ing. Michal Soumar

prof. Ing. Kamil Vrba, CSc.
předseda oborové rady

LICENČNÍ SMLOUVA
POSKYTOVANÁ K VÝKONU PRÁVA UŽÍT ŠKOLNÍ DÍLO

uzavřená mezi smluvními stranami:

1. **Pan**
   Jméno a příjmení: Karol Ollé
   Bytem: Kostelecká 1828, 54701 Náchod
   Narozen/a (datum a místo):   28.09.1982 v Bratislavě
   (dále jen „autor")

<div align="center">a</div>

2. **Vysoké učení technické v Brně**
   Fakulta elektrotechniky a komunikačních technologií
   se sídlem Údolní 244/53, 602 00 Brno
   jejímž jménem jedná na základě písemného pověření děkanem fakulty:
   prof. Ing. Kamil Vrba, CSc.
   (dále jen „nabyvatel")

<div align="center">

Článek 1
Specifikace školního díla

</div>

1. Předmětem této smlouvy je vysokoškolská kvalifikační práce (VŠKP):
   diplomová práce
   (dále jen VŠKP nebo dílo)

   Název VŠKP: ENTERPRISE NETWORK DESIGN AND
                   SIMULATION – CISCO VIRTUAL LAB
   Vedoucí/ školitel VŠKP: Ing. Michal Soumar
   Ústav: Telekomunikací

   VŠKP odevzdal autor nabyvateli v:
   tištěné formě   – počet exemplářů 2
   elektronické formě – počet exemplářů 2

2. Autor prohlašuje, že vytvořil samostatnou vlastní tvůrčí činností dílo shora popsané a specifikované. Autor dále prohlašuje, že při zpracovávání díla se sám nedostal do rozporu s autorským zákonem a předpisy souvisejícími a že je dílo dílem původním.
3. Dílo je chráněno jako dílo dle autorského zákona v platném znění.
4. Autor potvrzuje, že listinná a elektronická verze díla je identická.

Článek 2
Udělení licenčního oprávnění

1. Autor touto smlouvou poskytuje nabyvateli oprávnění (licenci) k výkonu práva uvedené dílo nevýdělečně užít, archivovat a zpřístupnit ke studijním, výukovým a výzkumným účelům včetně pořizovaní výpisů, opisů a rozmnoženin.
2. Licence je poskytována celosvětově, pro celou dobu trvání autorských a majetkových práv k dílu.
3. Autor souhlasí se zveřejněním díla v databázi přístupné v mezinárodní síti ihned po uzavření této smlouvy.
4. Nevýdělečné zveřejňování díla nabyvatelem v souladu s ustanovením § 47b zákona č. 111/ 1998 Sb., v platném znění, nevyžaduje licenci a nabyvatel je k němu povinen a oprávněn ze zákona.

Článek 3
Závěrečná ustanovení

1. Smlouva je sepsána ve třech vyhotoveních s platností originálu, přičemž po jednom vyhotovení obdrží autor a nabyvatel, další vyhotovení je vloženo do VŠKP.
2. Vztahy mezi smluvními stranami vzniklé a neupravené touto smlouvou se řídí autorským zákonem, občanským zákoníkem, vysokoškolským zákonem, zákonem archivnictví, v platném znění a popř. dalšími právními předpisy.
3. Licenční smlouva byla uzavřena na základě svobodné a pravé vůle smluvních stran, s plným porozuměním jejímu textu i důsledkům, nikoliv v tísni a za nápadně nevýhodných podmínek.
4. Licenční smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma smluvními stranami.

V Brně dne 28. 05. 2008

…………………..   …………………….
 Nabyvatel   Autor

Anotace

Tématem této diplomové práce (dále jen DP) je návrh rozsáhlých podnikových sítí podle doporučení stanovených společností Cisco. Dále je realizována simulace navržené topologie prostřednictvím programů s otevřeným zdrojovým kódem a dohled nad sítí prostřednictvím programu Nagios.

Úvodní část obsahuje stručné seznámení se základním rozdělením sítě do jednotlivých funkčních bloků.

Druhá část se zabývá popisem jednotlivých funkčních bloků a jejich rolí v rámci celé síťové topologie. Bloky jsou dále rozděleny na jednotlivá zařízení a jsou popsány služby, které tato zařízení musí poskytovat.

Třetí část DP se snaží zmapovat základní požadavky na služby, které jsou kladeny na dnešní síťové infrastruktury. Hlavní důraz je kladen na dostupnost všech nabízených služeb sítě. Jsou vyjmenovány jednotlivé protokoly druhé až třetí vrstvy OSI modelu, které zabezpečují stálou dostupnost sítě v případě selhání aktivních prvků.

Čtvrtá část DP se věnuje popisu návrhu síťové topologie WAN.

Pátá část obsahuje popis bezpečnostních rizik, která ohrožují dostupnost sítě, tak i popis útoků, které mají za cíl krádež identity uživatele.

V šesté části DP jsou popsány programové nástroje pro zprávu sítí (Nagios, Cisco Security Device Manager) a programy, které simulují Cisco přepínače, směrovače (Dynamips and Dynagen, GNS3) a Cisco PIX firewall (PEMU).

Sedmá kapitola se zabývá konkrétním návrhem rozsáhlé sítě s použitím principů, které byly zmíněny v předcházejících kapitolách. Navržená infrastruktura je dále realizována pomocí simulačních programů a tato virtuální síť dovoluje demonstrovat nastavení a chování všech popsaných protokolů a zařízení.

V závěrečném shrnutí je nejdůležitější poznatek, že návrh a konfigurace rozsáhlé sítě a její realizace ve virtuálním prostředí je funkční a použitelná pro pokusné účely i pro studijní účely.

Klíčová slova: LAN, VLAN, STP, VTP, OSPF, návrh sítě, Dynamips, Dynagen, PEMU, Nagios, Cisco, IOS.

Abstract

This Master's Thesis (further only MT) deals with subject of enterprise network design according to recommendations of Cisco company. As part of the thesis is developed simulation of enterprise network, according to created concept. The virtual lab is realized by open-source programs and monitored by Nagios software.

The first part contains brief introduction to network designs and description of hierarchical network design.

The second part describes building blocks of the network design and their role in hierarchical network. Each block is further divided into specific network devices and then there are described services that have to be provided by them.

The third part of MT deals with basic service demands which are expected from today's network infrastructures. The main focus is on availability of network services. There are specified information about second and third layer protocols of OSI model which are securing availability of all services provided by the network infrastructure in case of failure.

The following fourth part contains information about WAN design.

The fifth part describes security risks which can jeopardize network availability. It also contains description of attacks on network users.

The sixth part of MT contains brief description of software tools for network management and monitoring (Nagios, Cisco Security Device Manager) and programs for simulating Cisco routes and switches (Dynamips and Dynagen, GNS3) and Cisco PIX firewall simulation program (PEMU).

The seventh chapter deals with developed network design concept. The concept is deployed as virtual lab running under simulation programs. The virtual infrastructure allows demonstration of settings and behavior of all protocols and equipments described before.

In conclusion is the most important recognition that the network concept and its simulation as virtual lab is functional and it can be used for tests or educational purposes.

Keywords: LAN, VLAN, STP, VTP, OSPF, Network Design, Dynamips, Dynagen, PEMU, Nagios, Cisco, IOS.

Manifest

Prohlašuji, že svou diplomovou práci na téma „Návrh a simulace podnikové sítě - virtuální laboratoř Cisco" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

V Brně dne 28. 05. 2008   ………………………

                                                                      (Karol Ollé)

Acknowledgement

Děkuji vedoucímu diplomové práce Ing. Michalu Soumarovi, za velmi užitečnou metodickou pomoc, neúnavné vedení práce a obsahové nasměrování textu práce. V neposlední řadě pak za ochotu ke konzultacím a cenné rady při zpracování práce.

V Brně dne 28. 05. 2008

....
(Karol Ollé)

Index

ABR   Area Border Router
ACL   Access Control List
AIM   Advanced Integration Module
AM   Analog Modem
API   Application Programming Interface
ARP   Address Resolution Protocol
ATM   Asynchronous Transfer Mode
BPDU   Bridge Protocol Data Unit
CAM   Content Addressable Memory
CatOS   Catalyst Operating System
CCO   Cisco Connection Online
CEF   Cisco Express Forwarding
CERT   Computer Emergency Response Team
Cisco TAC   Cisco Technical Assistance Center
CISF   Catalyst Integrated Security Features
CLI   Command Line Interface
DAI   Dynamic ARP Inspection
DHCP   Dynamic Host Configuration Protocol
DoS   Denial of Service
DSL   Digital Subscriber Line
DTP   Dynamic Trunking Protocol
ECNM   Enterprise Composite Network Model
EIGRP   Enhanced Interior Gateway Routing Protocol
FIB   Forwarding Information Base
GAN   Global Area Network
GARP   General Attribute Registration Protocol
GLBP   Gateway Load Balancing Protocol
GNU   General Public License
GNS3   Graphical Network Simulator
HSRP   Hot Standby Router Protocol
HTTP   HyperText Transfer Protocol
I/O   Input/Output
IBNS   Identity-Based Networking Services
ICMP   Internet Control Message Protocol
ICSA   International Computer Security Association
ID   Identification
IGMP   Internet Group Management Protocol
IOS   Internetwork Operating System
IP   Internet Protocol
IPS   Intrusion Prevention System
IPSec   IP Security
IPSG   IP Source Guard
ISL   InterSwitch Link Protocol
ISP   Internet Service Provider
LACP   Link Aggregation Control Protocol
LAN   Local Area Network
LSA/SPF   Link-State Advertisement/Shortest Path First
MAC   Media Access Control
MAN   Metropolitan Area Network
Mbps   Megabit per second
MSFC   Multilayer Switch Feature Card
MST   Multiple Spanning-Tree

NAC	Network Admission Control
NAT	Network Address Translation
NM	Network Module
NNTP	Network News Transfer Protocol
NPE	Network Processing Engine
NSF	Non-Stop Forwarding
OOP	Object-Oriented Programming
OSPF	Open Shortest Path First
PAgP	Port Aggregation Protocol
PC	Personal Computer
PoE	Power over Ethernet
POP3	Post Office Protocol Version 3
PPP	Point-to-Point Protocol
PSTN	Public Switched Telephone Network
PVC	Permanent Virtual Circuit
PVST+	Per VLAN Spanning-Tree Protocol Plus
QoS	Quality of Service
RIP	Routing Information Protocol
RSTP	Rapid Spanning-Tree Protocol
SDM	Security Device Manager
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNAC	Systems and Network Attack Center
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Stateful SwitchOver
STP	Spanning-Tree Protocol
TCAM	Ternary Content Addressable Memory
UDLD	Uni-Directional Link Detection
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
VTP	VLAN Trunking Protocol
WAN	Wide Area Network
WIC	WAN Interface Card

Table of Contents

List of Figures

Icons and Symbols

VLAN XXX - VLAN Description

- Network/Zone Cloud

- Switch (Catalyst 6500)

- Router (with Firewall)

- Router

- Router
(not in Management scope)

- Switch

- Switch (Multilayer)

- Firewall

- Frame Relay Switch

- Universal Gateway

- VPN Concentrator

12 - VLAN /
STP VLAN root /
secondary root

T - Trunk

Po 1 - Port-Channel

Fa1/1 - Device Interface

- Server

- Web Server

- Management
Console

- Notebook

- Workstation

- Frame Relay Link

- Ethernet Link

- Serial Link

- PC 01 / OSPF Area

- PC 02

- PC 03 / OSPF Area

- PC 04 / OSPF Area

- PC 05

- PC 06

5

- Cisco 3620 2-slot Modular
Router-AC with IP Software (Front)

- Catalyst 3560-48PS

- Cisco Catalyst 2948G
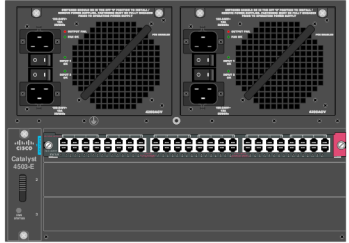
- Cisco Catalyst 4503-E
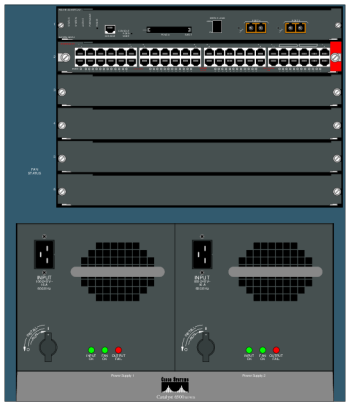
- Cisco Catalyst 6506
Chassis (Rear)

- Cisco 7204VXR, 4-slot chassis,
1 AC Supply w/IP Software

- PIX Firewall 525 Chassis
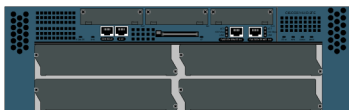
- Cisco 3700 Series 4-slot
Application Service Router

Preamble

To successfully run virtual lab, which is deployed as part of the Master's Thesis, is necessary to possess Cisco licensed software, original serial keys, and IOS (Internetwork Operating System) images. Person or an institution which wish to create a virtual lab based on this thesis has to be owner of CCO (Cisco Connection Online) account to access necessary resources at http://cisco.com/.

Therefore all Cisco certified materials, software, images, and keys will not be published and are not provided on attached DVD.

1   Introduction

Objectives of the Master's Thesis are to introduce modern design of enterprise networks and as part of the Thesis a virtual lab is deployed as a demonstration of basic ideas introduced in theoretical part.

Most ideas and design concepts mentioned in the Thesis are following Cisco Systems, Inc. guidelines. Cisco company references have been chosen because it is considered as today's leader in network technologies. The guidelines, called the ECNM (Enterprise Composite Network Model) [8], represents a modular, hierarchical approach to network design. The ECNM is referenced by Cisco as optimal design approach with reduced complexity.

A hierarchical network design allows building a modular, deterministic, and scalable foundation to address service needs of the intranet datacenter or WAN (Wide Area Network).

To simplify scaling of the standard hierarchical model, the ECNM has been developed, which divides an enterprise network design into physical, logical, and functional areas of service (*Figure 1*). Each functional area within campus model contains building access, building distribution, and building core layers.
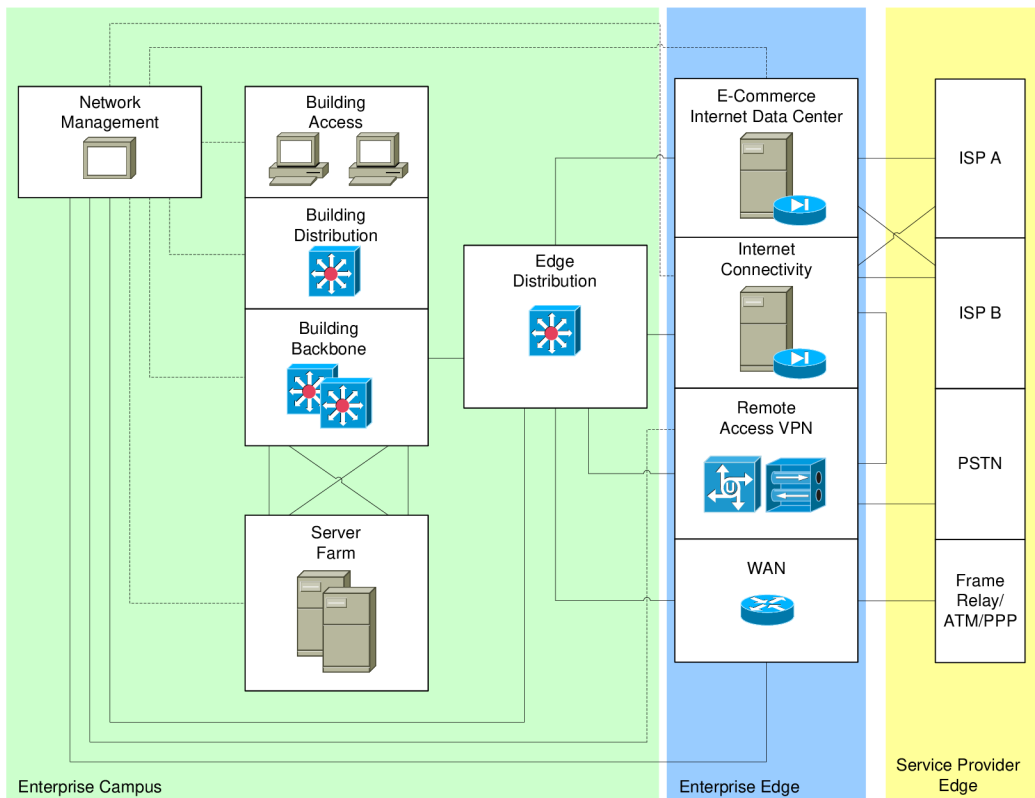
Figure 1   Enterprise Composite Network Model

8

The ECNM is characterized by the following features:

- The ECNM is deterministic network with clearly defined boundaries between modules.

- The ECNM supports continued growth by making each module discrete.

- Allows adding new modules.

- Supports adding new services and solutions without changing underlying network structure.

2 Designing Multi-Layer Campus Networks

Cisco shows in Enterprise Data Center guidelines [8] that the campus network is the foundation of the enterprise data network. If the foundation services and reference design in an enterprise network are not well designed, then application that depends on those services will eventually suffer performance and reliability challenges. However, if design principles and implementation best practice are taken into consideration, the foundation will be reliable and well engineered, and the network will support changes and growth.

2.1 Campus Design Requirements

The building blocks of the network design will be used to provide a solid foundation for the network to grow and support emerging applications [2]. This topic examines the requirements for these building blocks (Figure 2).
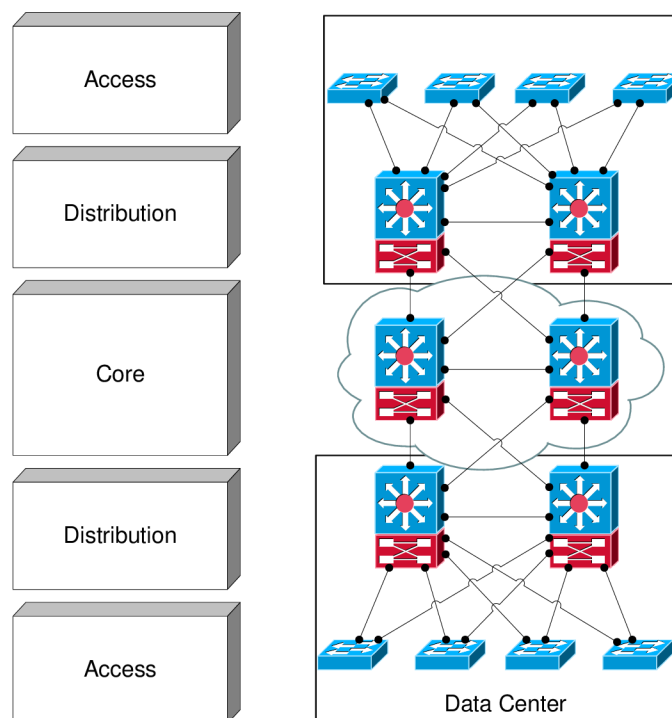
Figure 2   Multilayer Network Design

Multilayer or hierarchical network design allows building a modular, deterministic, and scalable foundation with building blocks that allow the network to meet evolving needs. A modular design makes the network easy to scale, understand and troubleshoot by promoting deterministic traffic patterns. Cisco introduced the hierarchical design model [8] in 1999.

The building block components are the access layer, the distribution or aggregation layer, and the core or backbone layer.

In a hierarchical design, the capacity, features, and functionality of each device are optimized for its position and role it plays in the network. The number of flow and their associated bandwidth requirements increase as each flow travels aggregation points and moves up the hierarchy from access to distribution to core. Functionality is distributed at each layer. The hierarchical design avoids the need for a fully meshed network.

Modular networks are easy to replicate, redesign, and expand because is not needed to redesign the whole network each time a module is added or removed. Building blocks can be put in service or taken out of service without impacting the rest of the network. This flexibility facilitates troubleshooting, problem isolation, and network management.

Summary of Multilayer Network Design benefits:

- Offers hierarchy (each layer has specific role).

- Modular topology (building blocks).

- Easy to grow, understand, and troubleshoot.

- Creates small fault domains (clear demarcations and isolation).

- Promotes load balancing and redundancy.

- Promotes deterministic traffic patterns.

- Incorporates balance of both layer 2 and layer 3 technology, leveraging the strength of both.

- Utilizes layer 3 routing for load balancing convergence, scalability and control.

2.1.1 Access Layer

The access layer (*Figure 3*) provides entry into the network for end stations, such as PCs, phones, and printers. This layer is redundantly attached to the distribution or aggregation layer switches for high availability, and is connected through layer 2 or layer 3 functionality. If the connection between the distribution layer switches is a layer 3 connection, all uplinks can actively forward traffic.
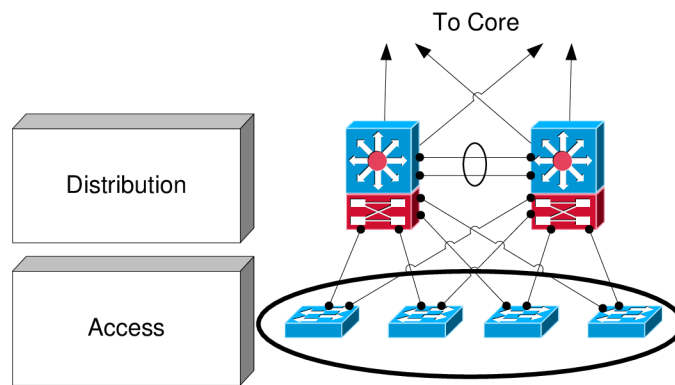
Figure 3   Definition of Access Layer

Access layer services:

- Aggregates network end-point layer 2 / layer 3 features environment; convergence, security, QoS (Quality of Service), IP (Internet Protocol) multicast, etc.

- Intelligent network services: QoS, trust boundary, broadcast suppression, IGMP (Internet Group Management Protocol) snooping.

- Intelligent network services: PVST+ (Per VLAN Spanning Tree Protocol Plus), Rapid PVST+, EIGRP (Enhanced Interior Gateway Routing Protocol), OSPF[1] (Open Shortest Path First), DTP (Dynamic Trunking Protocol), PAgP (Port Aggregation Protocol), LACP (Link Aggregation Control Protocol), UDLD (Uni-Directional Link Detection), etc.

- Automatic phone discovery, conditional trust boundary, PoE (Power over Ethernet), auxiliary VLAN (Virtual Local Area Network), etc.

- Spanning-Tree toolkit[2]: Portfast, UplinkFast, BackboneFast, LoopGuard, BPDUGuard, BPDUFilter, RootGuard etc.

- Cisco Catalyst[3] integrated security[4] features IBNS (Identity-Based Networking Services) (802.1x), CISF (Catalyst Integrated Security Features): port security, DHCP (Dynamic Host Configuration Protocol) snooping, DAI (Dynamic ARP Inspection), IPSG (IP Source Guard), etc.

2.1.2   Distribution Layer

The distribution layer (*Figure 4*) provides aggregation for wiring closet switches and uplinks to the core. This layer is used to terminate access-layer VLANs from the access-layer switch. The distribution layer plays a key role in containing

---

[1] Open Shortest Path First
   http://ietf.org/html.charters/ospf-charter.html
[2] Campus Network Multilayer Architecture and Design Guidelines
   http://cisco.com/en/US/docs/solutions/Enterprise/Campus/campover.html
[3] Cisco Switches
   http://cisco.com/go/switches
[4] Cisco security solutions
   http://cisco.com/go/security

failures if layer 3 switching is used to communicate with other distribution-layer switches. The distribution layer also eliminates the need for the core to support high-density peering relationships for access-layer switches. This reduces the need for process-intensive operations in the core.

It should be configured HSRP (Hot Standby Router Protocol), VRRP (Virtual Router Redundancy Protocol), or GLBP (Gateway Load Balancing Protocol) at this layer to provide first-hop redundancy. Protocols like EtherChannel[5] increase availability in the distribution layer by building aggregating links. Load balancing across equal cost routes provides optimal use of bandwidth. Using layer 3 routing in the distribution and core layers does not produce blocking links, and therefore optimizes link utilization.
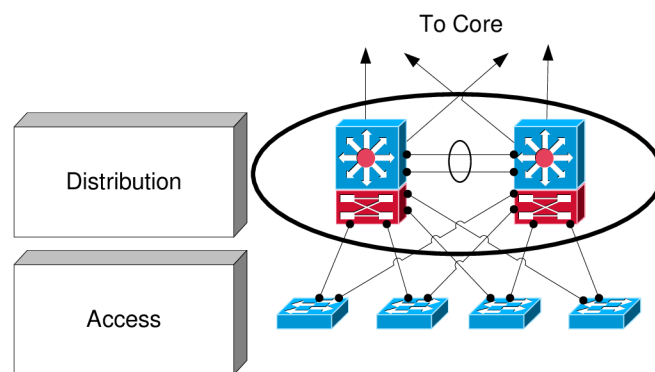
Figure 4   Definition of Distribution Layer

Many enterprises enforce QoS (Quality of Service) and security policies in the distribution layer because it is easy to make a common group profile and apply it to all access switches. Hardware-enabled QoS is required when access-layer switches are aggregated.

Distribution Layer services:

- Availability, load balancing, and QoS are important consideration at this layer.

- Aggregates wiring closets (access layer) and uplinks to core.

- Uses layer 3 switching in the distribution layer.

- Protects core from high density peering and problems in access layer.

- Route summarization, fast convergence, redundant path load sharing.

- HSRP or GLBP to provide first-hop redundancy.

---

[5] Understanding EtherChannel Load Balancing and Redundancy on Catalyst Switches
http://www.cisco.com/en/US/tech/tk389/tk213/technologies_tech_note09186a0080094714.shtml

2.1.3 Core Layer

In a small campus, the core and distribution layers can be collapsed into one layer. Unfortunately, collapsing these layers limits future grow and scalability. For optimum core layer convergence, build triangles instead of squares, so that equal-cost redundant paths can be taken advantage of for best deterministic convergence. Redundant equal-cost load sharing links can converge in milliseconds, ensuring that the network recovers quickly when topology changes occur.
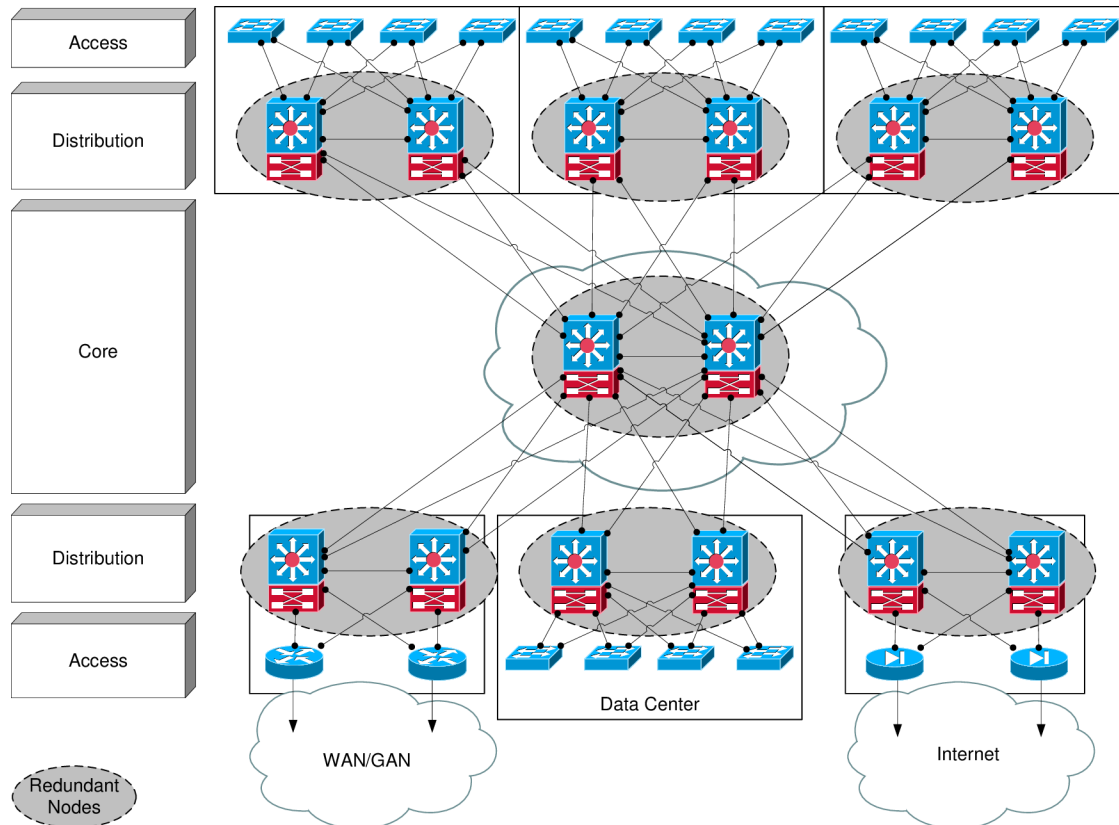
Figure 5   Definition of Core Layer

When designing core topologies (*Figure 5*), consider the benefits of topologies with point-to-point links. With point-to-point links, any topology change is propagated almost immediately to the underlying protocols. Any topology that relies on indirect notification and timer-based detection will converge in seconds due to its non-deterministic nature.

It should be considered whether to use two switches with dual or single SuperVisors, or one switch with dual SuperVisor. Dual SuperVisors with SSO[6] (Stateful SwitchOver) and NSF[7] (Non-Stop Forwarding) can cause longer convergence than single SuperVisor in a fully redundant topology. SSO and NSF are designed to maintain layer 3 links during a convergence event. When the links stay

---

[6] Stateful SwitchOver
  http://cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s22/sso120s.htm
[7] Cisco NSF and Timer Manipulation for Fast Convergence
  http://cisco.com/en/US/products/ps6550/products_white_paper09186a00801dce40.shtml

up, there is an outage that is only as long as SSO requires to activate the standby SuperVisor. This outage is one to three seconds[8].

In non-redundant topologies, such as topologies with single switches in the core or distribution layer, or topologies that are not fully meshed, SSO, NSF and redundant SuperVisors can provide significant resiliency improvements. While one to three seconds of outage is not desirable, one to three seconds is better than the period of time it takes someone to physically replace a SuperVisor and recover the SuperVisor configuration.

Core Layer services:

- Network backbone connects building blocks.
- Performance and stability vs. complexity.
- Aggregation point for distribution layer.
- Separate core layers helps in scalability during future growth.
- Should be technology-independent.

---

[8] Cisco Nonstop Forwarding with Stateful Switchover Deployment Guide
http://cisco.com/en/US/products/ps6550/products_white_paper0900aecd801dc5e2.shtml

3   *Campus Design Foundation Services*

This topic describes the foundation services that are required to build a stable and flexible network.

Several foundation services must be implemented to achieve optimum convergence in the access, distribution and core layers of the network. These foundation services cover layer 2 and layer 3 functionality, and are optimized either at one, or three of these layers.

Foundation services:

- Layer 3 routing protocols.

- Layer 2 redundancy

    - Spanning-Tree[9]

    - PVST+

    - RSTP (Rapid Spanning-Tree Protocol)

- UDLD (Uni-Directional Link Detection).

- Trunking protocols (ISL/802.1q)

- Load balancing

    - Etherchannel link aggregation

    - CEF (Cisco Express Forwarding) equal cost load balancing

- First hop redundancy protocols

    - VRRP, HSPR and GLBP

- QoS (Quality of Service)

3.1   *Layer 3 Routing protocols*

Design recommendations for layer 3 foundation services [1] include:

- Build triangles instead of squares for deterministic convergence; unlike triangles, squares will always trigger a routing protocol update during link failure. Triangles will not cause routing protocol convergence to occur during link failure.

- Control peering across the access layer links; layer 3 peer relationships are established many times across the access nodes of distribution layer switches. This process wastes memory and bandwidth and should be minimized.

- Summarize at the distribution layer; this approach creates boundaries for EIGRP (Enhanced Interior Gateway Routing Protocol) queries and OSPF

---

[9] 802.1D MAC Bridges
http://ieee802.org/1/pages/802.1D-2003.html

LSA/SPF (Link-State Advertisement/Shortest Path First) propagation and optimizes the routing protocols for campus convergence.

- Optimize CEF (Cisco Express Forwarding) for best utilization of redundant layer 3 paths; this method reduces the effect of CEF polarization and provides optimum utilization of redundant paths.

3.2 Alternative Paths

To ensure that the access layer switches do not become the transit nodes in the case of a link or switch failure, install redundant link to the core and use layer 3 links between the distribution layer switches. If a link on the switch were to fail the layer 3 routing protocol would know of the alternate path and be able to switch the traffic without the access layer having to be a transit point (*Figure 6*).
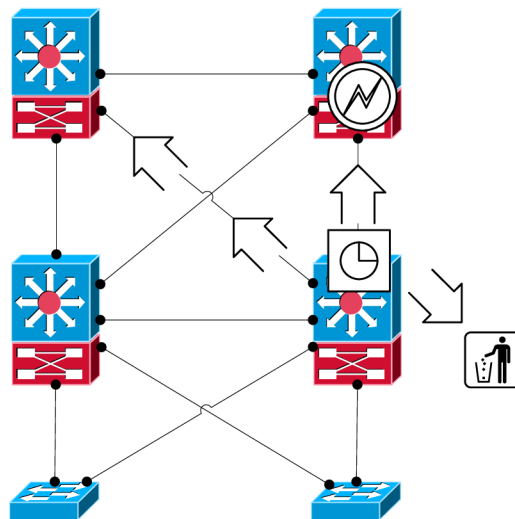
Figure 6   Link/Switch failure

Adding a redundant path to the network makes it easier to use route summarization. Route summarization could be used at the distribution layer to minimize the number of routing entries in the routing table and to limit the effect of link failure on the rest of the network. To ensure that the access layer does not become a transit point for traffic that would ultimately be dropped, a link is provided between the distribution layer switches.

3.3 CEF Load Balancing

Traffic from the access layer flows across the distribution and core layers and into the data center. As it proceeds, it crosses multiple redundant paths in the campus network. To prevent CEF (Cisco Express Forwarding) polarization from causing under-utilization of the redundant paths, it is necessary to verify the decision input for the CEF hashing algorithm at the core and distribution layer.

3.4   Spanning-Tree

Design recommendations for layer 2 foundation services (*Figure 7*) include:

- If spanning is necessary, use Rapid PVST+ (Rapid Per VLAN Spanning-Tree Protocol Plus) to span VLANs.

- To protect against user-side loops, use Rapid PVST+.

- To protect against unexpected STP (Spanning-Tree Protocol) participation, use the spanning tree toolkit.

- To protect against one-way up-up connections, use UDLD[10] (Uni-Directional Link Detection).

- Use VTP[11] (VLAN Trunking Protocol) transparent mode, set trunks to on-on with no negotiate, and prune unused VLANs.

- Match PAgP[12] (Port Aggregation Protocol) settings between CatOS and Cisco IOS software.
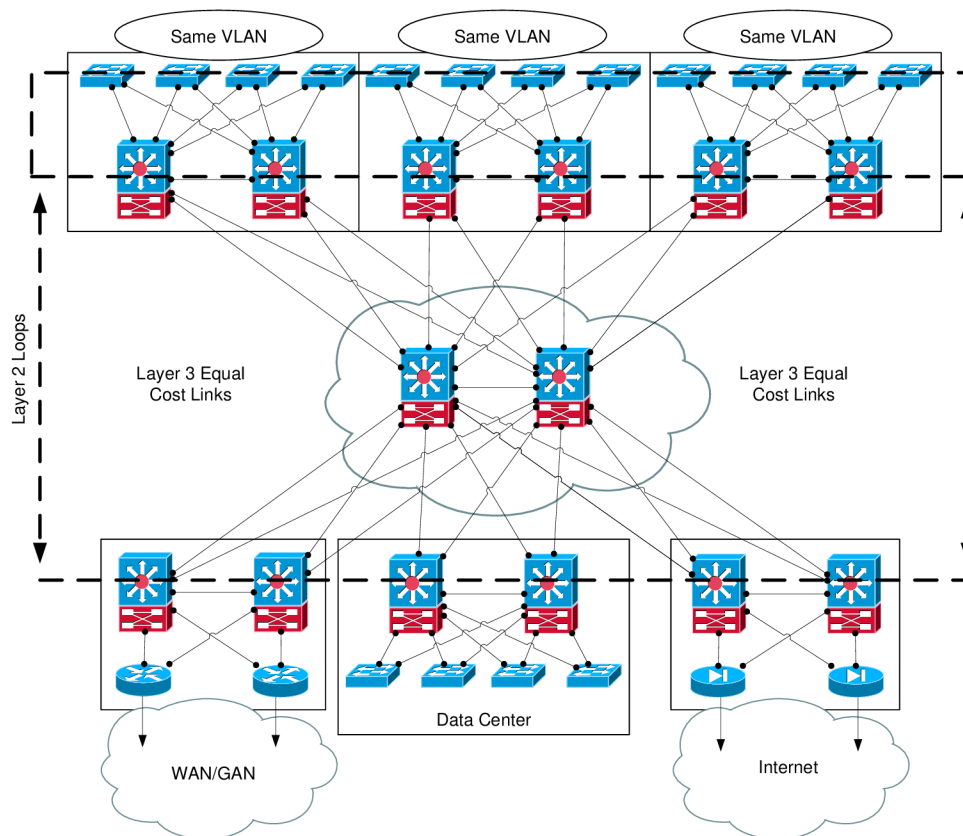
Figure 7   Spanning-Tree Configuration

---

[10] Cisco Systems UniDirectional Link Detection Protocol
http://ietf.org/internet-drafts/draft-foschiano-udld-03.txt
[11] Understanding VLAN Trunk Protocol
http://cisco.com/warp/public/473/21.html
[12] Port Aggregation Protocol
http://ieee802.org/3/trunk_study/april98/finn_042898.pdf

The Cisco Spanning-Tree toolkit includes:

- PortFast: Bypasses the listening-learning phase for an access port (supported by MST (Multiple Spanning Tree) and Rapid PVST+).

- UplinkFast: Provides 3-5 seconds of convergence after link failure.

- BackboneFast: Cuts convergence time by max age for indirect failure.

- LoopGuard: Prevents the alternate or root port from becoming designated in the absence of BPDU (Bridge Protocol Data Unit) (supported by MST and Rapid PVST+).

- RootGuard: Prevents external switches from becoming root (supported by MST and Rapid PVST+).

- BPDUGuard: Disables the PortFast enabled port if BPDU is received (supported by MST and Rapid PVST+).

- BPDUFilter: Do not send or receive BPDU on PortFast enabled ports (supported by MST and Rapid PVST+).

3.5   UDLD

Fiber optic interconnections are common in campus environment. Physical misconfigurations in these interconnections can occur, causing a link to appear to be up-up when there is actually a mismatched set of transmit and receive pairs. When these physical misconfigurations occur, protocols such as STP (Spanning-Tree Protocol) can cause network instability. UDLD detects these physical misconfigurations and disables the ports in question.

UDLD Configuration:

- Typically deployed on any fiber optic interconnection.

- Use UDLD aggressive mode for best protection.

- Turn on in global configuration to avoid operational errors and misses.

3.6   Trunks

Switch interconnections carry multiple VLANs. When configuring switch-to-switch interconnections, the DTP[13] (Dynamic Trunking Protocol) should be set to on-on with *no negotiate* to avoid DTP protocol negotiation. This approach can save seconds of outage when restoring a failed link or node.

---

[13] Dynamic Trunking Protocol
http://cisco.com/en/US/tech/tk389/tk390/tk181/tsd_technology_support_sub-protocol_home.html

Trunk Configuration:

- Typically deployed on interconnection between access and distribution layers.

- Use VTP transparent mode to decrease potential for operational error.

- Hard set trunk mode to on and encapsulation negotiate off for optimal convergence.

- Change the native VLAN to something unused to avoid VLAN hopping.

- Manually prune all VLANs except those needed.

- Disable trunk on host ports.

3.7   Port-Channel

Port-Channel is typically deployed in the distribution-to-core, and core-to-core interconnections. To achieve maximum utilization of channel members, tune the load balancing function of layer 3 and layer 4. When connecting a Cisco IOS software device to CatOS device, make sure that the PAgP settings are the same on both sides, as defaults for these devices are different.

3.8   First-Hop Redundancy

In a hierarchical network design, default gateway redundancy is an important component of convergence. Both HSRP and GLBP can be tuned to achieve 900 milliseconds convergence[14] for link or node failure in the layer 2 and layer 3 boundary of the distribution hierarchical model.

HSRP is a Cisco proprietary protocol. VRRP (Virtual Router Redundancy Protocol) provides multi-vendor interoperability, and GLBP facilitates uplink load balancing.

3.9   Spanning VLANs

When a layer 2 link is inserted between two distribution switches, the switches can communicate directly. HSRP hellos are exchanged via the distribution-to-distribution link, and if the uplink to Access A fails (*Figure 8*), the duration of the outage is dependent on how quickly the backup link can move from blocking to forwarding state. Uplink Fast or Rapid PVST+ provides a state transition of about 1 second duration. 802.1d can take as long as 50 seconds to finish effect state transition. After the link goes active, traffic is forwarded over the distribution-to-distribution link to the HSRP primary (active) switch, and then to the core.

---

[14] High Availability Campus Recovery Analysis
http://cisco.com/application/pdf/en/us/guest/netsol/ns432/c649/cdccont_0900aecd801a89fc.pdf
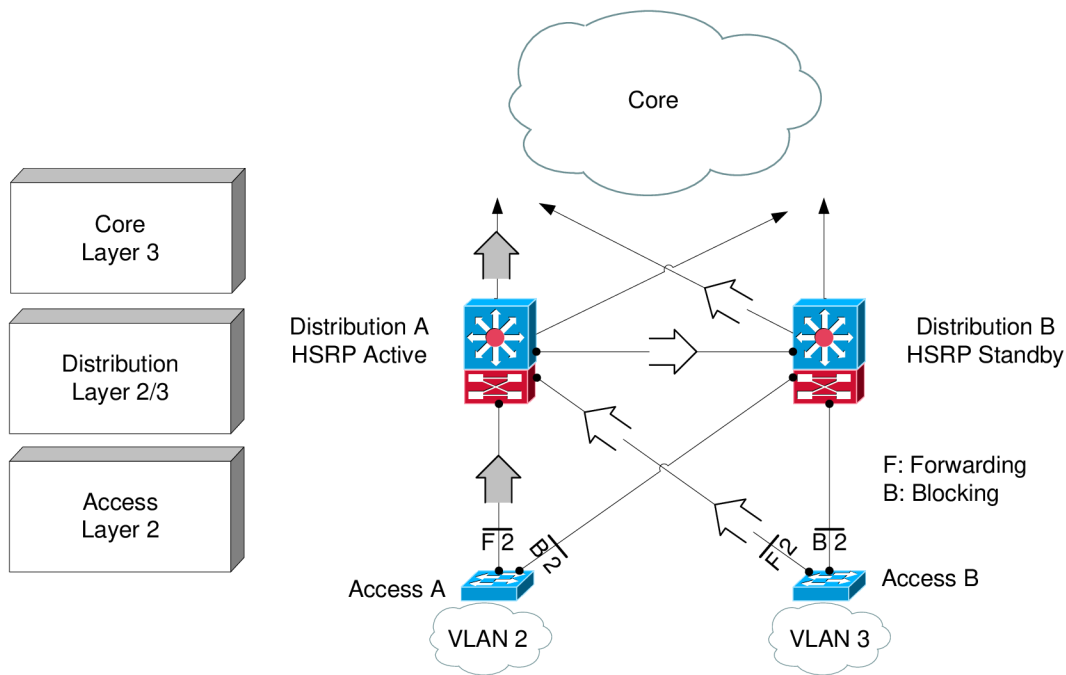
Figure 8   Spanning VLANs

This process results in non-optimal path, which is better than having no link at all.

3.10   QoS (Quality of Service)

Switches use hardware QoS policies (*Figure 9*). Routers use software QoS policies. QoS policies can be used to protect more than just voice and video traffic. Experience has shown that internet worms and DoS (Denial of Service) attacks have the ability to flood links, even in a high-speed campus environment. With QoS policies, the network administrator can protect critical applications while providing a lower class of service for suspected traffic.
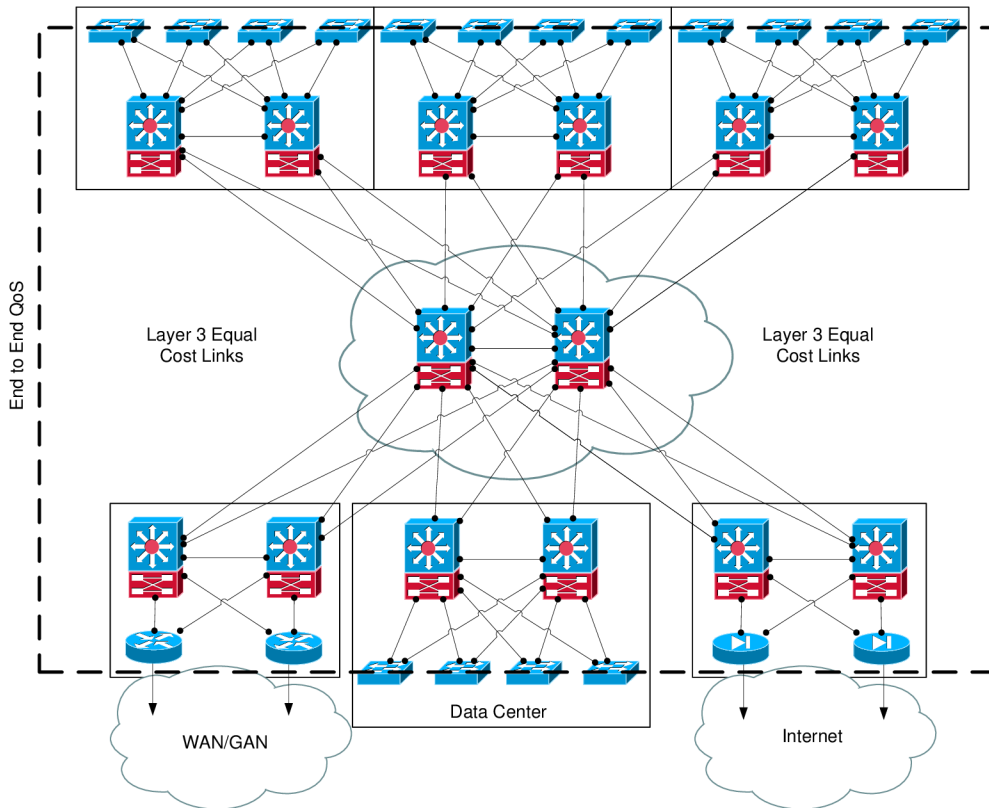
Figure 9   *QoS boundaries*

Topic Campus Services would be much longer and deeper in details if this would be a goal of the Thesis. Therefore the chapter has described only main services and not in deep details. For more Campus provided services and detailed explanations please refer to Cisco Validated Design Program site [8].

4 Designing WAN Networks

Modern WAN architectures require additional network capabilities to support current growing bandwidth demands of applications. Requirements for deploying VoIP (Voice over IP) and video conferencing include high availability, IP multicast, and QoS. Today, most enterprises rely on private WAN connections such as Frame Relay, ATM, or leased-line services. When deploying a traditional Frame Relay or ATM-based private WAN, however, network operations must implement point-to-point or hub-and-spoke architectures that make provisioning and management of moves, adds, or changes on the network complex. Also, the operational expense for a private WAN can sometimes be higher than IP-based WAN technologies. The goal is to have reliable connectivity that is secure, can be easily updated, and can scale to meet evolving needs.

For more details please refer to Cisco Enterprise WAN/MAN design guides [8]. The description of the involved issues would extend beyond Master's Thesis assignment.

5 Security Issues within the Campus

Security is a critical aspect of any network design [3]. Network data must be protected at all times, whether in-transmit or at rest. This topic describes the issues relating to security and explains how the network devices can mitigate them.

Network security is a primary concern of enterprises and commercial network administrators. In the past, physical security represented the main element of risk. Currently, the regular release of Internet-based viruses, worms, and other attack tools have increased the risk and shifted the focus to protecting business productivity. A firewall between the network and the Internet was previously sufficient. Today, network managers are moving to integrate end-to-end security throughout the network. New security policies and capabilities are beginning to permeate every location and device within the network.

The network has become a critical integration point for IP-enabled application and communications systems such as voice over IP. With security becoming more important than ever, a key place to examine new security concerns is within capabilities to protect the switches and users attached to them.

Security vulnerabilities of email and attachments are prevalent. There are also many other security threats that must be taken into consideration:

- The tailgater: an individual who penetrates the physical security of the building by walking in behind an authorized user. Once inside, the tailgater attaches to the network and downloads confidential information or launches an internal attack.

- The infected laptop: laptop computers can potentially become a security hole for worms and viruses. Laptops are used not only on the corporate network, but also externally on less secure environments. These usage patterns allow worms and viruses to be easily spread even if there was no intention on the part of the user.

- The unauthorized device: it is now easier than ever for users to attach unauthorized devices to the network, especially with unsecured wireless access points.

- The mass infection: DoS (Denial of Service) attacks flood the network with superfluous traffic, preventing authorized network devices from responding to legitimate network requests.

- The disgruntled employee: often known as the man-in-the-middle, the user activates publicly available software to spy on the data of other employees. This includes data and voice traffic using DHCP spoofing, IP spoofing and ARP poisoning attacks.

Network hardware and software tools provide protection against these types of attacks and if underway, mitigate the attacks as quickly and successfully as possible.

5.1   MAC Flooding Attack

The switch uses the CAM (Content-Addressable Memory) table to build up a layer 2 forwarding table based on MAC (Media Access Control) addresses. This CAM table does not have an infinite amount of space. Capitalizing on this limitation, MAC-based attacks force a switch to learn bogus MAC addresses (*Figure 10*). The attack floods the CAM table and stops the switch from learning additional real addresses for forwarding purposes. When encountered, the MAC addresses that can not be entered in the CAM table become unknown MAC addresses that are flooded throughout the network. Although this is standard behavior for the switch, this behavior can result in poor network and end-station performance.
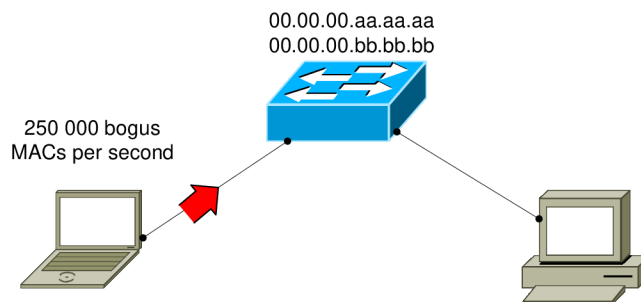
Figure 10   MAC Flooding Attack

The port security feature [2] on the Cisco Catalyst switch helps to prevent these types of attacks by limiting the number of MAC addresses that can be learned on specific port. This ensures that only a small number of MAC addresses are learned at given port and the port is locked down if other unverified MAC addresses are encountered. Another element of port security is the Broadcast Suppression or Storm Control feature that sets a threshold for the number of broadcast and multicast packets an interface can transmit into the network.

5.2   Malicious DHCP Server

One of the ways an intruder can gain control of a switched network is by spoofing the DHCP server and sending out false addresses and default gateway information. By spoofing the real DHCP server, the bogus DHCP server intercepts any requests from DHCP clients (*Figure 11*), and takes the first step in malicious plan to gain illegitimate access to information.
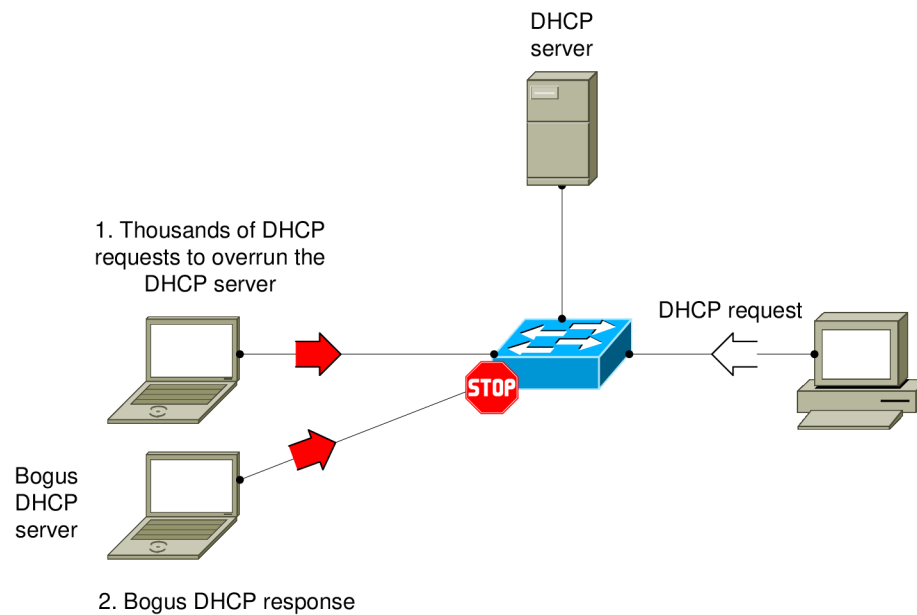
Figure 11   Malicious DHCP Server

To prevent this type of attack from occurring, a feature on the Cisco Catalyst switches called DHCP Snooping [2] ensures that only certain ports on a switch can process DHCP information other than a DHCP request. The feature defines trusted ports which can send DHCP requests and acknowledgements, and un-trusted ports which can only forward a DHCP request. Trusted ports are those that connect to either the DHCP server or to switched ports such as uplinks. If a malicious user inserts a bogus DHCP server on an un-trusted port, the switch shifts that interface down. In addition, this feature enables the switch to build up a DHCP binding table that maps clients MAC address, IP address, VLAN, and port ID. This table can then be used as a foundation for other switch features that prevent future attacks from succeeding.

5.3   ARP Poisoning

End stations use ARP (Address Resolution Protocol) packets to discover the MAC address of their default gateway. Unfortunately, a security hole exists in ARP. A router or end-station is allowed to send out a gratuitous ARP, which is an unsolicited ARP reply. This process is often called ARP poisoning (*Figure 12*). Using gratuitous ARPs, a malicious user can spoof the default gateway or any other device in the network, thereby placing itself in a unique position to receive data packets he/she would not normally be able to view. This type of attack is difficult to detect from the end-station or default gateway perspective as these elements are not aware that their traffic is being incorrectly directed, or that they are not receiving the traffic destined for these locations.
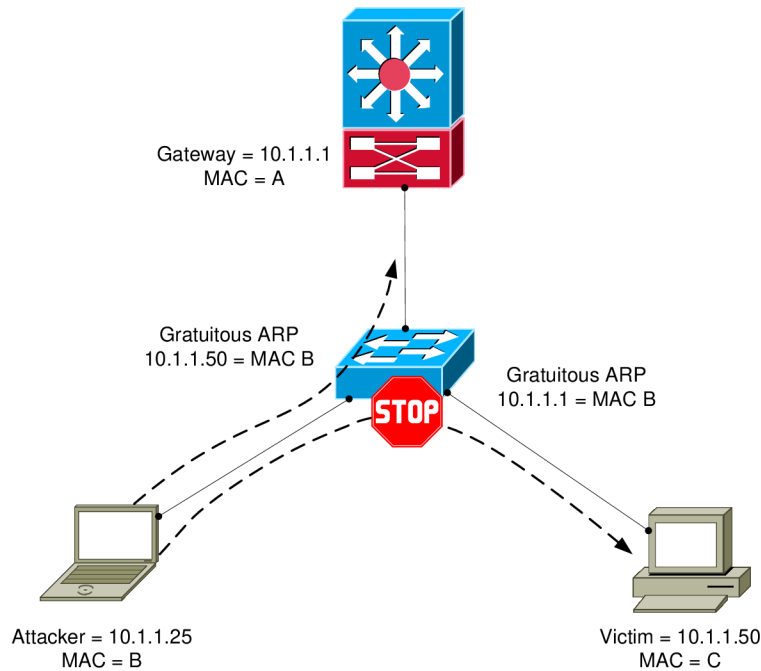
Figure 12   ARP Poisoning

Cisco Catalyst switches offer a feature called DAI (Dynamic ARP Inspection), which helps to prevent this type of attack from occurring [1]. Like DHCP snooping, DAI uses concept of trusted and un-trusted ports to decide which ARP packets are to be inspected, DAI intercepts all ARP packets and examines them for proper MAC-to-IP bindings, by inspecting the DHCP binding table that was build when DHCP snooping was enabled. For trusted ports, no examination is performed; for un-trusted ports, an ARP examination takes place and the table is compared with DHCP binding table. Unmatched ARP packets are dropped.

DAI allows to watch the DHCP request as it populates a MAC-to-IP address table. If GARPs (General Attribute Registration Protocol) are seen or IP-to-MAC address changes, then the port should be lock down with the errdisable [9] command.

For non-DHCP MAC and IP addresses, can be writen ARP ACLs (Access Control List) to protect those devices.

5.4   Spoofed IP Address

To prevent malicious users from spoofing an IP (Internet Protocol) address and gaining access to the network, the Cisco Catalyst switch can also use IP Source Guard [2] feature. The IP Source Guard feature uses the DHCP snooping table to check the binding of an IP address to a MAC address, its port and its associated VLAN. The switch accomplishes this task by automatically configuring an ACL (Access Control List) in the Cisco Catalyst TCAM (Ternary Content Addressable Memory) that limits a port to the configured IP address handed to the end-station by the DHCP server. If any inconsistencies appear, the port is disabled.

There are many other possible types of attacks and security holes in the network environment, most of them are due to poor design or misconfiguration. Also IOS or CatOS software, as any other software, has bugs. Cisco is publishing list of known vulnerabilities at Cisco Bug Tookit[15] (the tool is accessible only with active CCO account).

For list of known network issues and attacks, the CERT (Computer Emergency Response Team) site [10] is provided as reference point..

---

[15] Cisco Bug Tookit
https://cisco.com/go/bugs

6 Management, Monitoring and Simulation Tools

Subject management and monitoring of enterprise networks is very complex because is not covering only networking issues, but also complex programming and database knowledge. Following chapter could be considered as brief-show of these tools.

Monitoring tools:

- Tivoli Netview (commercial)
- OpenView (commercial)
- Netcool (commercial)
- Nagios (open-source)
- Eyeofthestorm (commercial)
- Syslog (open-source)
- Syslog-NG (open-source/commercial)

Performance monitoring tools:

- VitalSuite (commercial)
- eHealt (commercial)
- CACTI (open-source)
- Aurora (commercial)

Configuration management:

- CiscoWorks (commercial)
- Voyance (commercial)
- RANCID (open-source)

Simulation tools:

- RouterSim (commercial)
- OPNET (commercial)
- Dynamips and Dynagen (open-source)
- GNS3 (open-source)
- PEMU (open-source)

and many others.

Monitoring and management tools for the virtual lab I did chose open-source solution Nagios and Cisco SDM (Security Device Manager). SDM is not listed above because it is not a tool for permanent monitoring or mass management; it could be considered as graphical interface for simplified device configuration.

As network simulation tool is probably well known OPNET. But this tool is designed for simulations of network environments from high point of view (meaning application flows and their behavior in long terms and variable loads), it is not designed to simulate particular hardware and running real software developed by the vendor.

Therefore I have chosen simulation projects Dynamips and Dynagen, GNS3 and PEMU. All three tools are developed as open-source projects.

6.1   Cisco Security Device Manager

Cisco SDM is a web-based (*Figure 13*) device-management tool for Cisco routers.
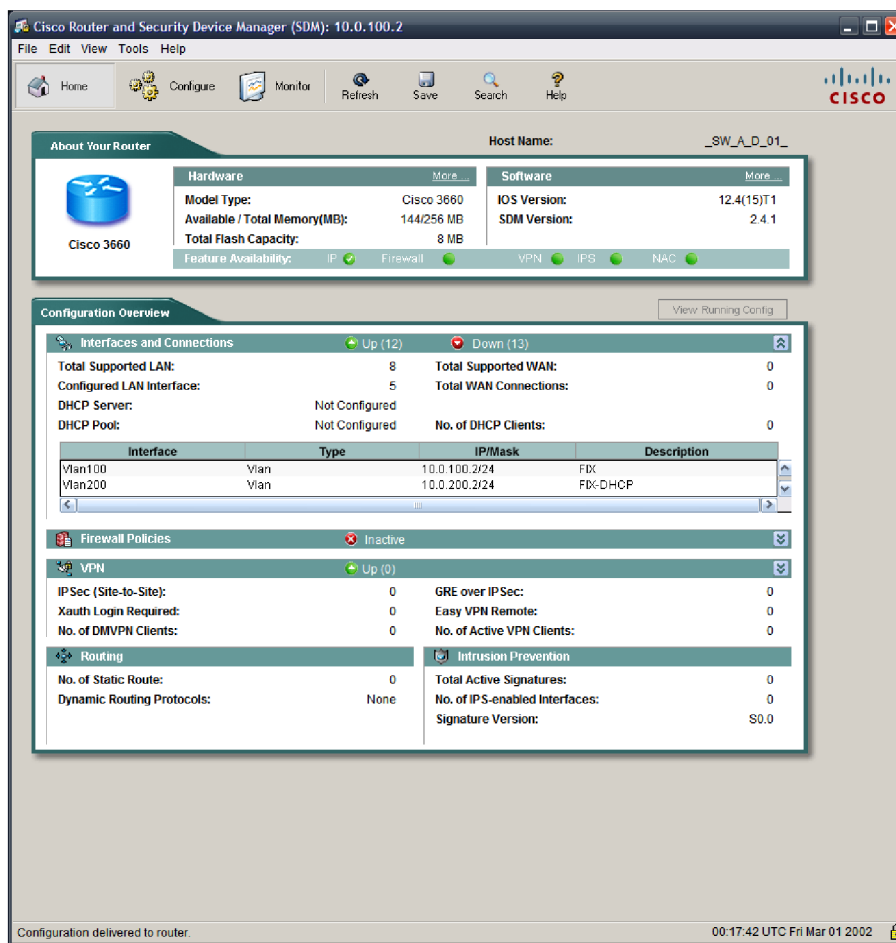
Figure 13   SDM

Cisco SDM supports a wide range of Cisco IOS Software releases and is available for download on Cisco router models from Cisco 830 Series to Cisco 7301. It ships preinstalled on all new Cisco 850 Series, Cisco 870 Series, Cisco 1800 Series, Cisco 2800 Series, and Cisco 3800 Series integrated services routers.

Cisco SDM can be used for deployment of Cisco routers for integrated services such as dynamic routing, WAN access, WLAN, firewall, VPN, SSL VPN, IPS, and QoS.

SDM can be used for SDM-generated configurations, already approved by the Cisco TAC. Configuration checks built into Cisco SDM reduce misconfigurations. SDM can be used for monitoring router performance statistics, system logs, and firewall logs in real time.

Cisco SDM offers configuration support for LAN and WAN interfaces, NAT (Network Address Translation), stateful firewall and application policy, IPS, IPSec VPN, QoS, and NAC policy features. Cisco SDM also offers security auditing capability to check and recommend changes to router's configuration based on ICSA Labs and Cisco TAC recommendations.

The Cisco SDM using for access a router SSL (Secure Sockets Layer) and SSHv2 (Secure Shell) Protocol connections (*Figure 14*). When deployed at a branch office, a Cisco SDM-enabled router can be configured and monitored from corporate headquarters.

SSL connection   Internet   SLL connection

Remote user configuring   Cisco Router
Router using Cisco SDM   With Cisco SDM
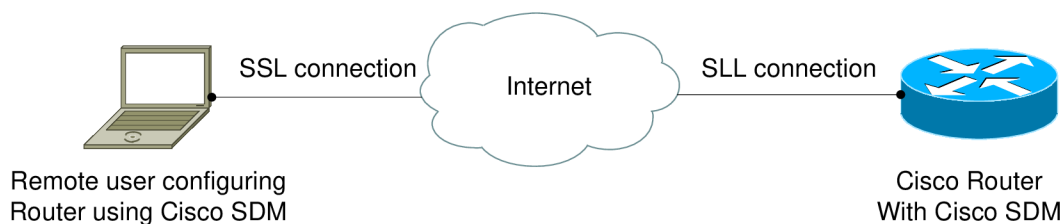
Figure 14   Connection to SDM

6.1.1 Router Security Audit

When deploying a new router, a Cisco IOS Software firewall can be configured to follow recommendations by the ICSA (International Computer Security Association) and the TAC (Cisco Technical Assistance Center). Firewall wizard allows deployment of high, medium, or low application firewall policy settings.
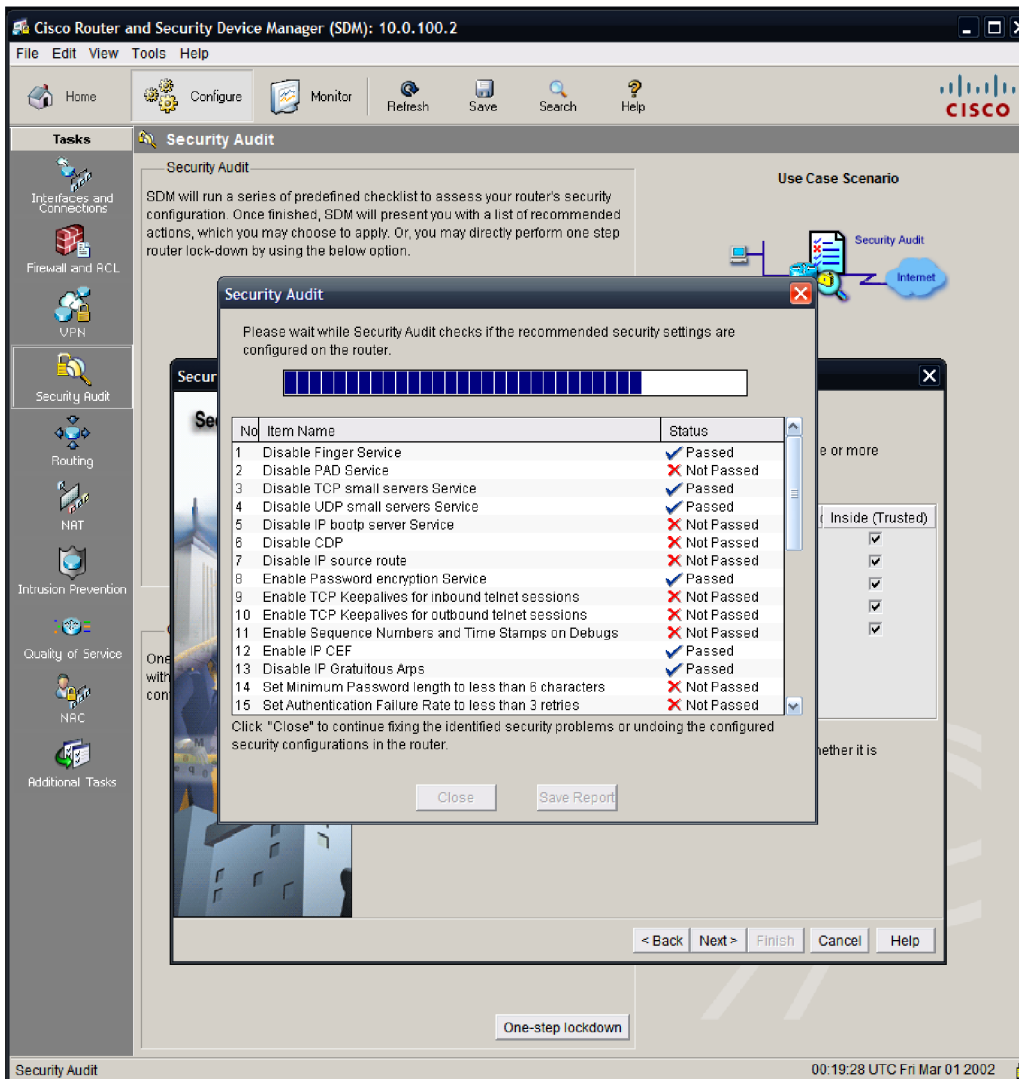
Figure 15   *Security audit*

When invoked on an already configured router, Cisco SDM allows to perform security audits (*Figure 15*) to evaluate the strengths and weaknesses of the router configurations against common security vulnerabilities.

The Cisco SDM also can be used for day-to-day operations such as monitoring, fault management, and troubleshooting.

For more details and download of SDM please refer to [11]; requires login and service contract.

6.2   Nagios

Nagios is a host and service monitor of network environment. It has been designed to run under the Linux operating system. The monitoring daemon runs intermittent checks on hosts and services that are specified using external plugins which return status information to Nagios. When problems are encountered, the daemon can send notifications out to administrative contacts (email, instant message, SMS, etc.). Current status information, historical logs, and reports can all be accessed via a web browser.

Nagios is licensed under the terms of the GNU (General Public License) Version 2 as published by the Free Software Foundation.

Ethan Galstad is the creator and lead developer of the Nagios and the main Nagios plugin developers are Ton Voon, Benoit Mortier, Holger Wiess, and Thomas Guyot-Sionnest.

Nagios features are listed below:

- Monitoring of network services (SMTP, POP3, HTTP, NNTP, ping, etc.).

- Monitoring of host resources (processor load, disk and memory usage, running processes, log files, etc.).

- Monitoring of environmental factors such as temperature.

- Simple plugin design that allows users to easily develop their own host and service checks.

- Ability to define network host hierarchy, allowing detection of and distinction between hosts that are down and those that are unreachable.

- Contact notifications when service or host problems occur and get resolved (email, pager, or other user-defined method).

- Optional escalation of host and service notifications to different contact groups.

- Ability to define event handlers to be run during service or host events for proactive problem resolution.

- Support for implementing redundant and distributed monitoring servers

- External command interface that allows on-the-fly modifications to be made to the monitoring and notification behavior through the use of event handlers, the web interface, and third-party applications.

- Retention of host and service status across program restarts.

- Scheduled downtime for suppressing host and service notifications during periods of planned outages.

- Ability to acknowledge problems via the web interface.

- Web interface for viewing current network status, notification and problem history, log file, etc.

- Simple authorization scheme that allows restrict what users can see and do from the web interface.

For more details and download of Nagios please refer to [12].

6.3 Dynamips and Dynagen

Dynamips is a Cisco router emulator written by Christophe Fillot. It emulates 1700, 2600, 3600, 3700, and 7200 hardware platforms, and runs standard IOS images. Dynamips provides a simple virtual switch; it does not emulate Catalyst switches (although it does emulate the NM-16ESW).

Dynagen is a text-based front-end for Dynamips, which uses the Hypervisor mode for communication with Dynamips. Dynagen simplifies building and working with virtual networks:

- Uses a simple configuration file for specifying virtual router hardware configurations.

- Simple syntax for interconnecting routers, bridges, frame-relay and ATM, and Ethernet switches.

- Can work in a client/server mode, with Dynagen running on a workstation communicating with Dynamips running on a back-end server. Dynagen can also control multiple Dynamips servers simultaneously for distributing large virtual networks across several machines. Or Dynamips and Dyngen can run on the same system.

- Provides a management CLI for listing devices, starting, stopping, reloading, suspending, resuming, and connecting to the consoles of virtual routers.

Dynagen is written in Python, and is therefore compatible with any platform for which there is a Python interpreter. The design is modular, with a separate OOP API for interfacing with Dynamips. Other Python applications could be written that use this API for programmatically provisioning virtual networks, or to provide other front-ends.

Dynagen uses a single network file to store the configuration of all the routers, switches, and interconnections that make up a virtual lab. This file uses a simple .ini file-like syntax.

Following lines show example of simple Lab configuration:

test.net

```
ghostios = true
# Ghostios option can significantly reduce the amount of real host RAM
needed for labs with multiple routers running the same IOS image. With this
feature, instead of each virtual router storing an identical copy of IOS in
its virtual RAM the host will allocate one shared region of memory that
they will all utilize.

sparsemem = true
# The feature does not conserve real memory, but instead reduces the amount
of virtual memory used by router instances. This can be important, because
```

33

```
OS limits a single process to 2 GB of virtual memory on 32-bit Windows, and
3 GB on 32-bit Linux.

autostart = false
# By default, all routers are automatically started when a lab is launched.
The autostart keyword overrides this behavior, and the lab must manually be
started.

[localhost]
# The first section specifies the host that is running Dynamips. In this
case, I intend to run Dynamips on the same machine as Dynagen.

    [[7200]]
# Section is indented, and double bracketed. This means that what follows
is configuration that applies to the Dynamips server specified in the
section above. All whitespace is actually ignored. The double-bracket is
what really means that this section is nested under the [localhost]
section.
The [[7200]] section defines all the defaults that will be applied to any
7200 router instance I create.

    image = \Program Files\Dynamips\images\c7200-js-mz.122-40.image
# The image keyword specifies the location on the system running Dynamips
(in this example my local machine) of the image I want to use by default
for all router instances. Here I'm pointing to a 122-40 image on a Windows
system.

    npe = npe-400
    ram = 160
# Each of our router instances is going to use an NPE-400, and allocate 160
MB of RAM.

    [[ROUTER R1]]
# Now, I'm defining a virtual router instance with the ROUTER keyword. The
string following this keyword is the name I'm assigning to this router, in
this case "R1".

    s1/0 = R2 s1/0
# This line states that I'm going to take R1 Serial 1/0 interface, and
connect it to R2 Serial 1/0 interface (via virtual back-to-back serial
cable). Dynagen automatically installs a PA-8T adapter in Port 1 to
accommodate this connection on both R1 and R2.

    [[router R2]]
    f0/0 = NIO_gen_eth:\Device\NPF_{AAAE72B9-C26B-4FA5-87B2-B0D1166B7861}
# Dynamips can bridge virtual router interfaces (real host interfaces)
allowing the virtual network to communicate with the real world. On Windows
systems, the Winpcap library is used to accomplish this bridging. Interface
specification is a little more complex on Windows systems, so Dynamips
provides a command line switch to list the available interfaces on Windows
hosts. The Dynamips/Dynagen Windows installer includes a shortcut to this
utility.
```

In order to run virtual lab, there has to be Dynamips server running on a local machine (*Figure 16*).

34

Figure 16   Dynamips

On Windows, opening a .net file in explorer automatically launch Dynagen and the network is started (Figure 17).

Figure 17   Dynagen

As it was mentioned before, Dynamips has limited number of supported Cisco routers. Also WIC modules, cards, and (in case of Cisco 7200) NPEs. Complete list of supported hardware is posted on project site.

For more details and download of Dynamips and Dynagen please refer to [13] site.

6.4   GNS3

GNS3 (Graphical Network Simulator) is a graphical network simulator that allows design of network topologies and then run their simulations. At the moment GNS3 supports IOS routers, ATM/Frame Relay/Ethernet switches and PIX firewalls.

GNS3 is based on Dynamips, Pemu (including Pemuwrapper) and partially Dynagen, it is developed in python and through PyQt, the GUI part is made with the Qt library (used also in the KDE project). GNS3 also uses the SVG (Scalable Vector Graphics) technology to provide symbols for designed network topologies (*Figure 18*).
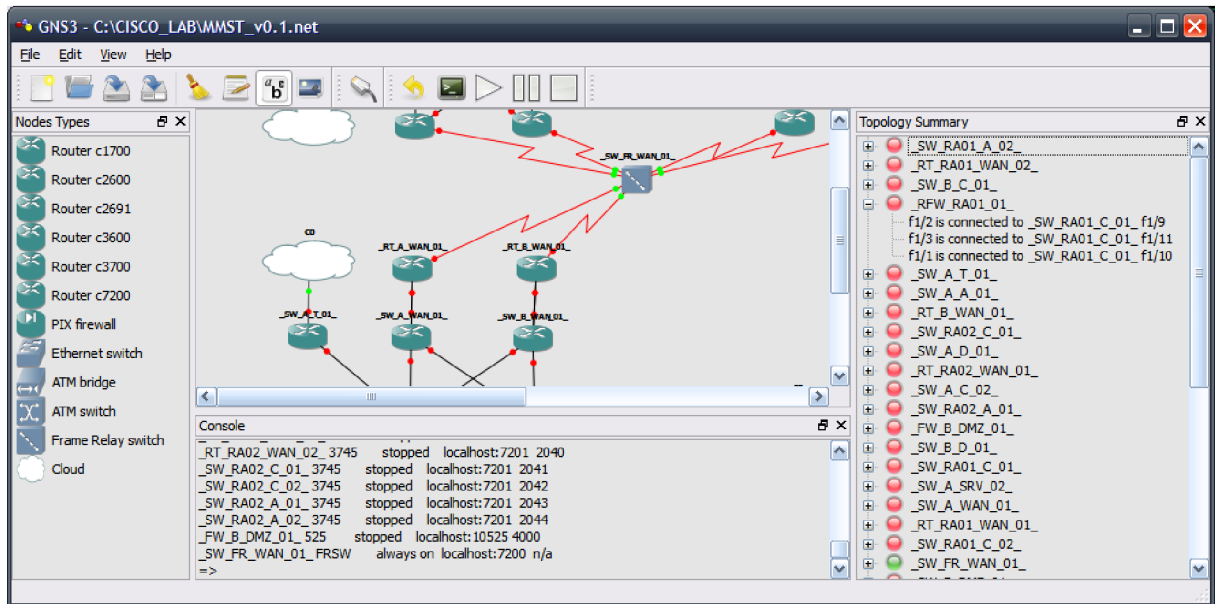
Figure 18   GNS3

Configuration file structure of GNS3 virtual lab is almost the same as in Dynamips project, so after small changes in the lab file, the same simulation can be started directly in Dynamips with no support of GNS3. Added information in the lab file are coordinates of icons on the layout.

The main advantage of GNS3 is intuitive drawing of a lab. Devices can be easily drag and drop into the lab and it is simple to create links between them. For example, writing a configuration file of more extensive simulation for Dynamips would take really long time; thanks to the graphical interface of GNS3 the same configuration can be done in couple minutes.

For more details about GNS3 project please refer to [14].

6.5 PEMU

PEMU, originally called PIXemu, is Cisco PIX 525 emulator based on project Qemu[16]. Original source code of the simulator has been posted by user "mmm123", at Hacki[17] forum.

The code is ported to MS Windows platform by user "Melifaro".

Following screenshots (Figure 19, Figure 20) and commands demonstrate how to run PEMU on MS Windows.
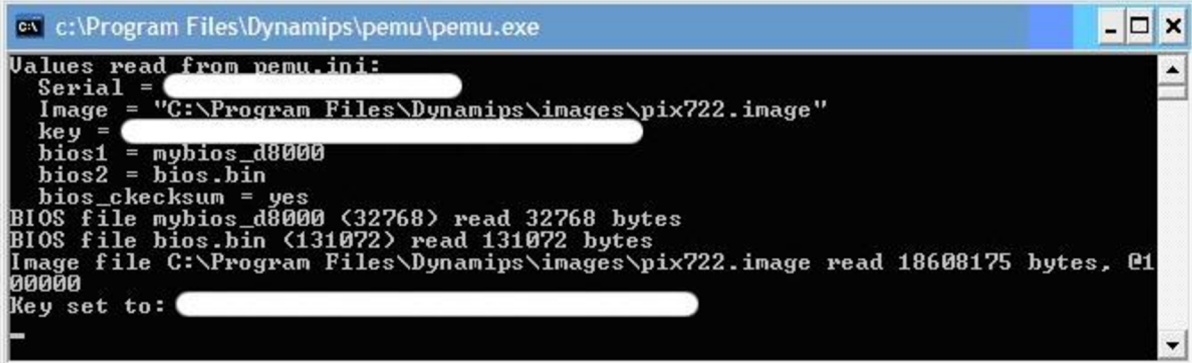
PEMU configuration file:

pemu.ini

```
serial=000000000
image=C:\Program Files\Dynamips\images\pix722.image
key=0x00000000,0x00000000,0x00000000,0x00000000
bios1=mybios_d8000
bios2=bios.bin
bios_checksum=1
```

Example of CLI command to start the PIX:

```
pemu.exe -net nic,vlan=1,macaddr=00:00:00:00:00:01 -net
tap,vlan=1,ifname=FW0 -net nic,vlan=2,macaddr=00:00:00:00:00:02 -net
tap,vlan=1,ifname=FW1 -serial telnet::10010,server,nowait -m 128
pix722.image
# For explanation of the PEMU start command please refer to PEMU help
"pemu.exe -h".
```


Figure 19   Pemu console

---

[16] Qemu
http://fabrice.bellard.free.fr/qemu/
[17] Hacki
http://7200emu.hacki.at/

Figure 20   Running PIX

For more details and download of PEMU please refer to [15].

7   Cisco Virtual Lab

As practical demonstration of Cisco network designs is realized Virtual Lab based on simulation tools Dynamips and Dynagen, GNS3 and PEMU.

The simulation acts as real network environment, so it is possible to manage and monitor devices and real data flow can pass the network.

As has been mentioned before, Dynamips can run only IOS images for specific Cisco routers; it is not possible to simulate Catalyst switches. But it is possible to add switching card to the router and then configure most of layer 2 services. The EtherSwitch NM-16ESW[18] is 16 port switch card which can support almost all needed switching features. This is the reason why in physical layouts are icons of switches, but on physical simulation layouts are icons of routers.

7.1   Lab Design

The main idea of the lab is to provide practical example of principles mentioned in previous chapters. The virtual environment has been chosen for its possible quick realization and zero-cost in comparing to setting up a real lab environment.

The simulation represents one fictional company with two remote offices. The connection between remotes sites and the Main site is realized by frame-relay technology with PVCs. Internet connection is available for Main site and Agency # 1; Agency # 2 has to use internet connectivity provided by the Main site.

Each of these three sites is configured for supporting on-site servers and their local or distant users (*Figure 21*).

Detailed view of application flows illustrates logical layout (*File Layouts_-_Low_levels_-_Logical_v1.0.pdf*), where is described IP plan for the whole lab and interconnection of subnets.

---

[18] Cisco EtherSwitch Modules for the 2600/3600/3700 Series Routers
http://cisco.com/en/US/prod/collateral/routers/ps259/product_data_sheet09186a00801aca3e.html
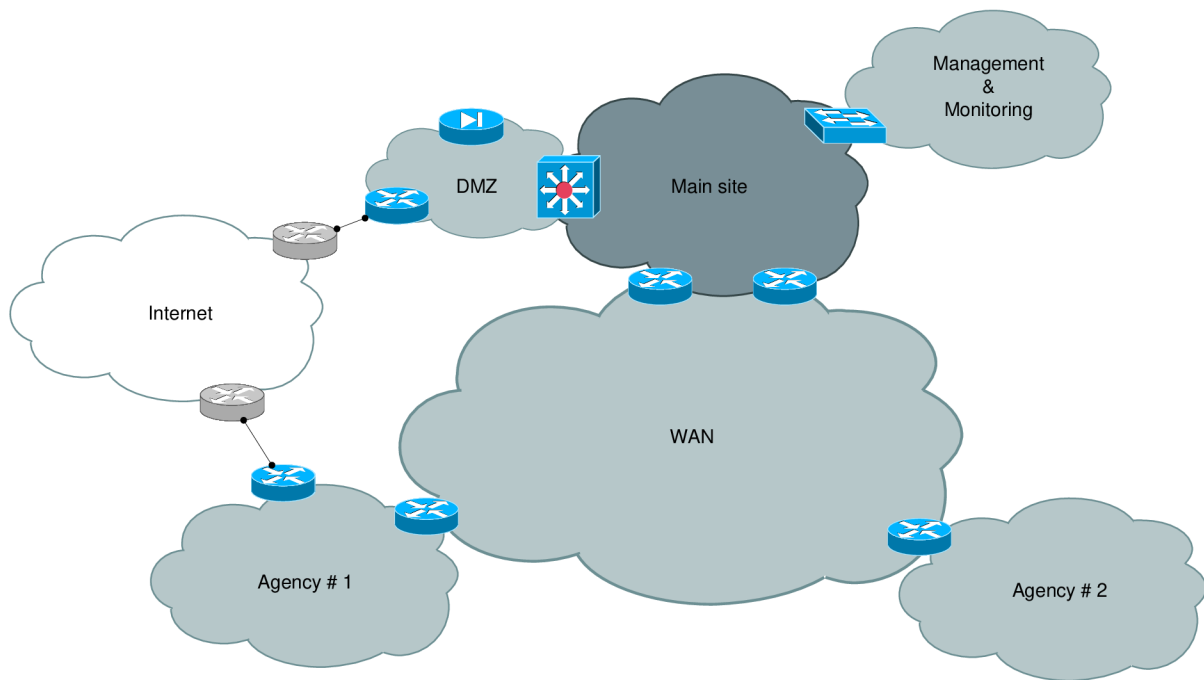
Figure 21   High level layout

7.1.1 Layers

Sites are subdivided into WAN, DMZ, Server Farm, Core, Distribution and Access layers. This division is represented by specific devices, where for the Main site[19] are:

- DMZ: _SW_B_DMZ_*
- Server Farm: _SW_A_SRV_*
- Core: _SW_A_C_*
- Distribution: _SW_A_D_*
- Access: _SW_A_A_*

In some devices are layers collapsed. For example equipment _SW_B_DMZ_01_ represents device in DMZ and Distribution layer. For remote sites the design is collapsed core, because networks for that size do not need dedicated devices, but cost effective solution.

Logical layout (*File Layouts_-_Low_levels_-_Logical_v1.0.pdf*) shows overview of the designed layers of each site. (Letter A stands for Access; D stands for Distribution; C stands for Core)

The second possible view at designed layers is from OSI model point of view. It means how the Physical, Data link and Network layers are set.

Detailed description of Physical layer illustrates low level physical layout (*File Layouts_-_Low_levels_-_Physical_v1.0.pdf*).

---

[19] A or B character represents two separate buildings

40

Description of the Data link layer (in this case STP and VTP protocols) shows STP and VTP layouts (*File Layouts_-_Low_levels_-_STP-VTP_v1.0.pdf*).

Routing configuration is described by routing layout (*File Layouts_-_Low_levels_-_Routing_v1.0.pdf*), which includes OSPF area overview.

7.1.2 VTP

VTP protocol is used for redistribution of configured VLANs (*Figure 22*), otherwise manual configuration of VLAN database for each switching device would be required. VTP servers on each site are configured two core switches, the rest of devices is configured as VTP clients or is using transparent mode.
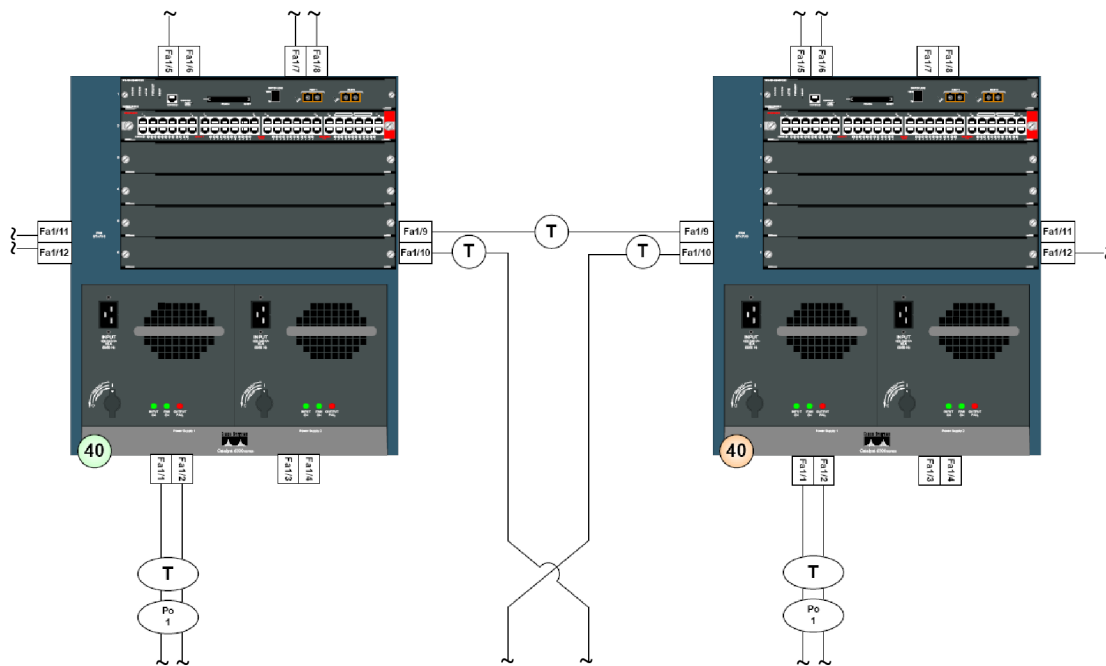
Figure 22   Core switches, segment of VTP layout

Bellow is dump of a VTP server status on Agency # 1. As domain name has been chosen "Agency1" and the domain using password authorization. The password is not just security measure; it is also protection against misconfigured devices which could delete the VLAN database for the site in case that the new devices will be connected to the network configured as server with lowest revision number.

*_SW_RA01_C_01_*

```
_SW_RA01_C_01_#sh vtp status
VTP Version                   : 2
Configuration Revision        : 3
Maximum VLANs supported locally : 68
Number of existing VLANs      : 16
VTP Operating Mode            : Server
VTP Domain Name               : Agency1
VTP Pruning Mode              : Disabled
VTP V2 Mode                   : Disabled
VTP Traps Generation          : Enabled
MD5 digest                    : 0xD3 0x0F 0xD5 0x02 0xE7 0xA1 0xDC 0x98
```

41

```
Configuration last modified by 10.1.1.129 at 3-1-02 00:13:14
Local updater ID is 10.1.1.129 on interface Vl11 (lowest numbered VLAN
interface found)
```

Detailed description of VTP is described on STP and VTP layout (*File Layouts_-_Low_levels_-_STP-VTP_v1.0.pdf*) together with logical layout (*File Layouts_-_Low_levels_-_Logical_v1.0.pdf*), the logical layout is important for understanding VLAN IP assignment.

Next output shows Agency # 1 device which is configured as client.

*_RFW_RA01_01_*

```
_RFW_RA01_01_#sh vtp status
VTP Version                    : 2
Configuration Revision         : 3
Maximum VLANs supported locally : 68
Number of existing VLANs       : 16
VTP Operating Mode             : Client
VTP Domain Name                : Agency1
VTP Pruning Mode               : Disabled
VTP V2 Mode                    : Disabled
VTP Traps Generation           : Enabled
MD5 digest                     : 0xD3 0x0F 0xD5 0x02 0xE7 0xA1 0xDC 0x98
Configuration last modified by 10.1.1.129 at 3-1-02 00:13:14
```

Print-out of VLAN database contains all VLANs what were configured on VTP server including all default VLANs (issued command *show vlan-switch* had to be used because it is used on router with switching module, the router does not support command *show vlan* as for example Catalyst switch series)

*_SW_RA01_C_01_*

```
_SW_RA01_C_01_#sh vlan-switch brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- ----------------------------
----
1    default                          active    Fa1/0, Fa1/2, Fa1/11,
Fa1/12

                                                Fa1/13, Fa1/14, Fa1/15
11   VLAN0011                         active
33   VLAN0033                         active
171  VLAN0171                         active
181  VLAN0181                         active
191  VLAN0191                         active
211  VLAN0211                         active
221  VLAN0221                         active
231  VLAN0231                         active
241  VLAN0241                         active
901  VLAN0901                         active
911  VLAN0911                         active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

As VTP layout illustrates, for interconnection of switches is used trunk mode. Native VLAN has been changed to bogus VLAN as part of security policy and for

WAN part are allowed only particular VLANs on the trunk. For tagging, devices are using standard IEEE 802.1q instead of Cisco proprietary ISL.

_SW_A_C_01_

```
_SW_A_C_01_#sh int Fa1/7 switchport
Name: Fa1/7
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Disabled
Access Mode VLAN: 0 ((Inactive))
Trunking Native Mode VLAN: 33 ((Inactive))
Trunking VLANs Enabled: 1,10,20,33,1002-1005
Trunking VLANs Active: 1,10
Protected: false
Priority for untagged frames: 0
Override vlan tag priority: FALSE
Voice VLAN: none
Appliance trust: none
```

Although Dynamips routers with switch module are allowing configuring switching services, as STP and VLAN, there are couple issues that should be considered in configuration.

First is setting-up VLAN database, old method has to be used, not recommend method, by configuring VLANs through *vlan database*. For that it has to be also manually specified file for storing these information by *vtp file nvram:vlan.dat*.

_SW_RA01_C_01_

```
_SW_RA01_C_01_#vlan data
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.

_SW_RA01_C_01_(vlan)#vtp server
Device mode already VTP SERVER.
_SW_RA01_C_01_(vlan)#vtp domain Agency1
Domain name already set to Agency1 .
_SW_RA01_C_01_(vlan)#vtp password Ag3nc11
Password already set to Ag3nc11.
_SW_RA01_C_02_(vlan)#vlan 11
VLAN 11 modified:
_SW_RA01_C_01_(vlan)#vlan 33
VLAN 33 modified:
~
_SW_RA01_C_01_(vlan)#apply
APPLY completed.
_SW_RA01_C_01_(vlan)#exit
Exiting....
_SW_RA01_C_01_#
```

Second issue is that Dynamips can not load the configuration of the vlan.dat file at startup. Therefore after a device is launched, the whole setting of *vlan database* has to be issued again (for every device).

43

7.1.3 OSPF

OSPF protocol is used as routing protocol for the virtual lab. Reasons for the decision to use this particular protocol are:

- OSPF is supported by all network vendors.
- It has similar convergence times as EIRGP protocol which is Cisco proprietary.
- OSPF is the most used routing protocol for LAN environment.

Bellow is listed output of OSPF protocol statuses for Agency # 1. The network has not been fully converged at the time of the print-out due to CPU requirements.

_RT_RA01_WAN_01_

```
_RT_RA01_WAN_01_#sh ip ospf neighbor

Neighbor ID       Pri    State          Dead Time    Address           Interface
10.255.1.30        0     FULL/  -       00:01:56     192.168.100.1
Serial2/1.1
10.254.1.1         1     FULL/BDR       00:00:06     10.1.1.1          Vlan11
10.254.1.3         1     FULL/DROTHER   00:00:07     10.1.1.129        Vlan11
```

_RT_RA01_WAN_01_

```
_RT_RA01_WAN_01_#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-
2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.1.1.1 to network 0.0.0.0


     172.16.0.0/30 is subnetted, 2 subnets
O       172.16.0.12 [110/11] via 10.1.1.129, 00:01:36, Vlan11
O       172.16.0.4 [110/65] via 192.168.100.1, 00:08:30, Serial2/1.1
     10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
C       10.1.1.0/24 is directly connected, Vlan11
O       10.1.190.0/24 [110/11] via 10.1.1.129, 00:01:37, Vlan11
O       10.1.220.0/24 [110/11] via 10.1.1.129, 00:01:37, Vlan11
O       10.255.1.30/32 [110/65] via 192.168.100.1, 00:08:30, Serial2/1.1
C       10.254.1.30/32 is directly connected, Loopback0
O       10.1.230.0/24 [110/11] via 10.1.1.129, 00:01:37, Vlan11
O       10.1.255.0/24 [110/11] via 10.1.1.1, 00:04:20, Vlan11
O       10.254.1.3/32 [110/11] via 10.1.1.129, 00:01:37, Vlan11
     192.168.100.0/24 is variably subnetted, 6 subnets, 2 masks
O       192.168.100.13/32 [110/64] via 192.168.100.1, 00:08:46, Serial2/1.1
O       192.168.100.9/32 [110/64] via 192.168.100.1, 00:08:46, Serial2/1.1
O       192.168.100.5/32 [110/64] via 192.168.100.1, 00:08:46, Serial2/1.1
C       192.168.100.0/30 is directly connected, Serial2/1.1
O       192.168.100.1/32 [110/64] via 192.168.100.1, 00:08:46, Serial2/1.1
C       192.168.100.128/30 is directly connected, Serial2/1.2
O    192.0.3.0/24 [110/11] via 10.1.1.1, 00:04:21, Vlan11
O*E2 0.0.0.0/0 [110/1] via 10.1.1.1, 00:04:21, Vlan11
```

Routing layout illustrates OSPF areas configuration (*File Layouts_-_Low_levels_-_Routing_v1.0.pdf*).

7.1.4 Redundancy

The main focus during designing network environment is on redundancy. It has to be considered on each layer.

The first physical redundancy is done in big scale; it means that entire building, in case of collapse, will be replaced by another building and production services and data will not be lost. Therefore the Main site is divided into two buildings.

Second physical redundancy focus is on devices. Each equipment has to be replaceable by another device in case of hardware problem. The network is designed that, if it is possible, there is more than one physical route to a destination. So in case of a device collapse, an outage will be counted in matter of minutes (depends on STP and OSPF recalculation) instead of hours of waiting for equipment replacement.

7.1.4.1 HSRP

First-hop redundancy is handled by HSRP protocol. The configuration, for example for VLAN 241, includes one virtual IP address which is gateway for the assigned subnet and two physical IPs configured as IP interfaces on HSPR routers. The virtual IP address is always located on active router, it means that the third layer protocols will route their flows to the active router.

*_SW_RA01_C_02_*

```
_SW_RA01_C_02_#sh standby brief
                    P indicates configured to preempt.
                    |
Interface    Grp   Pri P State   Active         Standby        Virtual IP
Vl11         0     100 P Standby 10.1.1.129     local          10.1.1.128
Vl171        0     110 P Active  local          10.1.170.2     10.1.170.1
Vl181        0     110 P Active  local          10.1.180.2     10.1.180.1
Vl191        0     100 P Standby 10.1.190.2     local          10.1.190.1
Vl211        0     100 P Standby 10.1.210.2     local          10.1.210.1
Vl221        0     100 P Standby 10.1.220.2     local          10.1.220.1
Vl231        0     100 P Standby 10.1.230.2     local          10.1.230.1
Vl241        0     100 P Standby 10.1.240.2     local          10.1.240.1
```

In case of failure of active router the standby router will take over and will stay active until a router with higher priority will take over.

Print-out bellow describes HSRP status of Agency # 1 VLAN number 241. In first case, the output describes standby router status.

*_SW_RA01_C_02_*

```
_SW_RA01_C_02_#sh standby Vlan241
Vlan241 - Group 0
  State is Standby
    5 state changes, last state change 00:00:11
  Virtual IP address is 10.1.240.1
```

```
   Active virtual MAC address is 0000.0c07.ac00
     Local virtual MAC address is 0000.0c07.ac00 (v1 default)
   Hello time 1 sec, hold time 3 sec
     Next hello sent in 0.064 secs
   Preemption enabled
   Active router is 10.1.240.2, priority 110 (expires in 1.652 sec)
   Standby router is local
   Priority 100 (default 100)
   Group name is "hsrp-Vl241-0" (default)
```

Second case describes active router status.

_SW_RA01_C_01_

```
_SW_RA01_C_01_#sh standby Vlan241
Vlan241 - Group 0
  State is Active
  Virtual IP address is 10.1.240.1
  Active virtual MAC address is 0000.0c07.ac00
    Local virtual MAC address is 0000.0c07.ac00 (v1 default)
  Hello time 1 sec, hold time 3 sec
    Next hello sent in 0.684 secs
  Preemption enabled
  Active router is local
  Standby router is 10.1.240.3, priority 100 (expires in 1.840 sec)
  Priority 110 (configured 110)
  Group name is "hsrp-Vl241-0" (default)
```

7.1.4.2 Port-Channel

As part of link redundancy is used Etherchannel protocol which combines a number of physical links into one logical link. In case of failure of one link, the channel stays intact and the flow is redirected only to the functional link. The Etherchannel is used to increase physical speed, because throughput of all members of the channel is added together. Bellow is detail of one port-channel interface which is connection between two core switches.

_SW_A_C_01_

```
_SW_A_C_01_#sh etherchannel 1 detail
Group state = L2
Ports: 2   Maxports = 8
Port-channels: 1 Max Port-channels = 1
              Ports in the group:
              -------------------
Port: Fa1/1
------------

Port state    = Up Mstr In-Bndl
Channel group = 1              Mode = On/FEC     Gcchange = 0
Port-channel  = Po1            GC   = 0x00010001    Pseudo port-channel = Po1
Port index    = 0
Age of the port in the current state: 00d:00h:24m:15s
Port: Fa1/2
------------

Port state    = Up Mstr In-Bndl
Channel group = 1              Mode = On/FEC     Gcchange = 0
Port-channel  = Po1            GC   = 0x00010001    Pseudo port-channel = Po1
```

```
Port index     = 1
Age of the port in the current state: 00d:00h:24m:10s
                Port-channels in the group:
                ----------------------

Port-channel: Po1
------------

Age of the Port-channel   = 00d:00h:24m:34s
Logical slot/port   = 8/0            Number of ports = 2
GC                  = 0x00010001      HotStandBy port = null
Port state          = Port-channel Ag-Inuse

Ports in the Port-channel:

Index   Port    EC state
------+------+-------------
  0     Fa1/1     on
  1     Fa1/2     on

Time since last port bundled:    00d:00h:24m:10s    Fa1/2
```

Port-Channel can be set for load balancing too, but this configuration is not used in virtual lab.

7.1.5   WAN

WAN network, which is connecting Main site and both Agencies, is simulated by virtual frame-relay switch. Each Agency is connected to the Main site by two PVC circuits as redundant connection to server farm resources. The connection is used also as internet connectivity for Agency # 2.

Because OSPF areas are configured and WAN network representing area number 1; areas configured at Agencies can not be connected to backbone area 0. Therefore on all ABR WAN routes have been configured virtual links. For details please refer to configuration of the Main site WAN router which includes frame-relay interface setting, OSPF configuration and virtual links.

_RT_A_WAN_01_.cfg

```
~
interface Serial2/1
 no ip address
 encapsulation frame-relay
 serial restart-delay 0
!
interface Serial2/1.1 point-to-point
 ip address 192.168.100.1 255.255.255.252
 ip ospf network point-to-multipoint
 ip ospf 1234 area 1
 frame-relay interface-dlci 101
~
router ospf 1234
 router-id 10.255.1.30
 log-adjacency-changes
 area 1 virtual-link 10.253.1.30
 area 1 virtual-link 10.253.1.31
 area 1 virtual-link 10.254.1.30
 area 1 virtual-link 10.254.1.31
```

```
 redistribute connected
 redistribute static
 network 10.255.1.30 255.255.255.255 area 0
 network 172.16.0.5 0.0.0.3 area 0
 network 192.168.100.1 0.0.0.3 area 1
 network 192.168.100.5 0.0.0.3 area 1
 network 192.168.100.9 0.0.0.3 area 1
 network 192.168.100.13 0.0.0.3 area 1
~
```

Next output shows details of running PVC circuit between Main site and Agency # 2.

*_RT_RA01_WAN_01_*

```
_RT_RA01_WAN_01_#sh frame-relay pvc

PVC Statistics for interface Serial2/1 (Frame Relay DTE)

               Active        Inactive       Deleted        Static
 Local           2              0              0              0
 Switched        0              0              0              0
 Unused          0              0              0              0

DLCI = 202, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE =
Serial2/1.1

 input pkts 92          output pkts 86         in bytes 13787
 out bytes 12114        dropped pkts 0         in pkts dropped 0
 out pkts dropped 0          out bytes dropped 0
 in FECN pkts 0         in BECN pkts 0         out FECN pkts 0
 out BECN pkts 0        in DE pkts 0           out DE pkts 0
 out bcast pkts 37      out bcast bytes 6866
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
 pvc create time 00:13:25, last time pvc status changed 00:10:46
```

7.1.6   Security

The security measures have to be taken also on each layer; as the redundancy. The first concern which has to be considered is physical security. It means network devices and their interfaces have to be protected against unauthorized users. This part of security is usually handled by storing active network equipments in secure room with limited access and only access ports are available to network users.

Chapter *Security Issues within the Campus* described basic security measures what should be taken implemented during campus design. Following chapters are describing exact security configurations issued in virtual lab.

7.1.6.1 Firewalls

Third layer security is simulated by virtual Cisco PIX firewall running under PEMU program and enabled IOS firewall on Agency # 1.

The function of the PIX firewall in Main site is to secure and divide specific subnets (*Figure 23*).
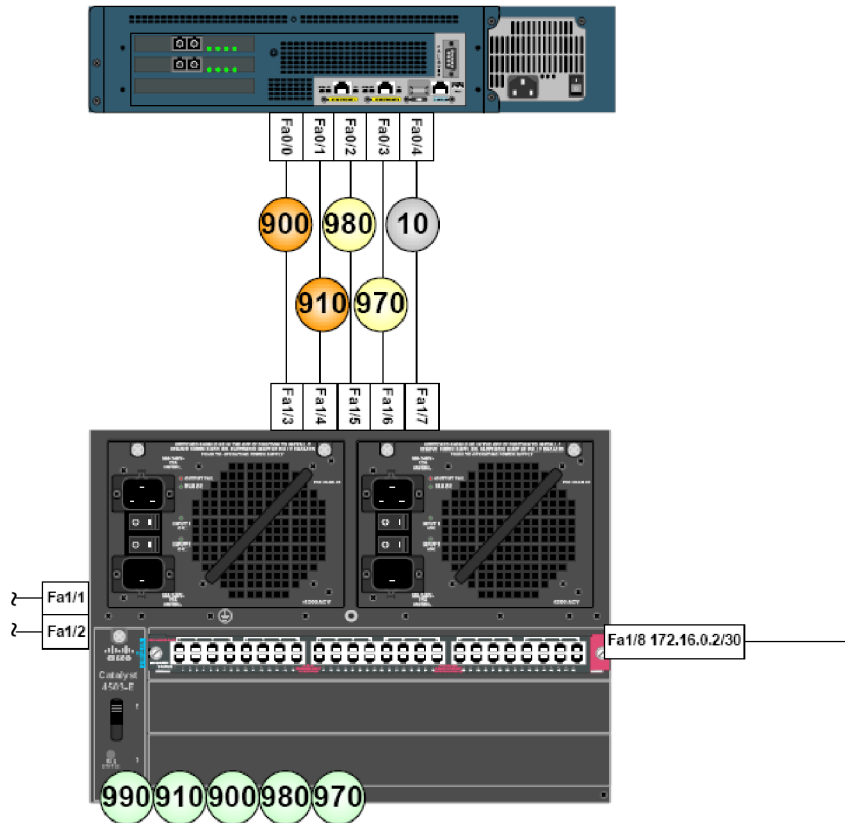
Figure 23   *PIX firewall, VTP layout*

VLAN number 900 (configured name of the VLAN is DMZ-INTERNET) could be used for placing a proxy server for internet connection. In this case the flow could enter the distribution switch from any part of the virtual network because the subnet is propagated into OSPF by DMZ switch. From switch the flow would be routed to the proxy and then to proxy's gateway. The gateway is represented by PIX firewall. On PIX interface VLAN 900 (FastEthernet 0/0) is the flow inspected by configured access-lists. Then, according to static routing table of the firewall, it is routed through interface DMZ-INTERNET-NAT and NATed into public IP address.

Bellow is dump of main points of the PIX configuration including setting of an interface, group definition, access-list, NAT and static routing.

_FW_B_DMZ_01_.cfg

```
~
interface Ethernet2
 speed 100
 duplex full
 nameif DMZ-SRV-MANAGEMENT
 security-level 0
 ip address 10.0.253.1 255.255.255.0
~
object-group network NET-DMZ-INTERNET
 description Internet subnet
 network-object 10.0.255.0 255.255.255.0
~
access-list acl_DMZ-INTERNET extended permit ip 10.0.0.0 255.0.0.0 any log
```

```
access-list acl_DMZ-INTERNET extended deny ip any any log
~
access-list NO_NAT remark no NAT for NET-DMZ-SRV-MANAGEMENT
access-list NO_NAT extended permit ip object-group NET-DMZ-SRV-MANAGEMENT
10.0.0.0 255.0.0.0
~
nat (DMZ-SRV-MANAGEMENT) 0 access-list NO_NATT
~
static (DMZ-INTERNET,DMZ-INTERNET-NAT) 10.0.255.0 192.0.2.0 netmask
255.255.255.0
~
access-group acl_DMZ-INTERNET in interface DMZ-INTERNET
access-group acl_DMZ-SRV-MANAGEMENT in interface DMZ-SRV-MANAGEMENT
~
route DMZ-INTERNET-NAT 0.0.0.0 0.0.0.0 172.16.0.1 1
route NET-INTERCONNECT 10.0.0.0 255.0.0.0 10.0.1.12 1
~
```

7.1.6.2 Other Security Measures

All devices within the virtual network contain basic security settings:

- First security recommendation is that all services which are not needed suppose to be disabled. This setting has to be carefully planed considering what services are used. In the virtual lab has been disabled for example services *ip bootp server* and *ip source-route*.

- Native VLAN has been set to bogus VLAN.
- Only SSH protocol is allowed to access devices for remote management.
- VTP domain is using password authorization.
- An access-list is applied on every IP interface; allowing only proper management subnet to enter a device, specifying IP subnets for VLAN which can enter the VLAN IP interface.
- Device logs are locally stored and sent to Syslog server.
- Unused interfaces are in shutdown state.
- Switch ports connecting end-user devices are configured as *spanning-tree portfast*.

The configuration is following recommendations of SNAC (System and Network Attack Center) [6, 7].

7.2   Example of Switch Configuration

The configured privilege and user password are not shown in the configuration files because password-encryption service is enabled. Use following passwords to access devices:

user / password : sdmsdm / sdmsdm.

The configuration has been snippet and only one device configuration is presented due to limited number of pages of MT. Attached DVD contains configurations of all simulated devices.

_SW_A_C_02_.cfg

```
!
version 12.4
service timestamps debug datetime
service timestamps log datetime
service password-encryption
!
hostname _SW_A_C_02_
!
boot-start-marker
boot-end-marker
!
logging buffered 16384 informational
enable secret 5 $1$IKCE$JC5sNlP9GlSWDR/2lTnfi/
!
no aaa new-model
memory-size iomem 5
clock timezone GMT+1 1
clock summer-time GMT+1 recurring
no ip source-route
ip cef
!
!
!
!
no ip bootp server
no ip domain lookup
ip domain name cisco-lab.com
!
multilink bundle-name authenticated
!
!
!
!
crypto pki trustpoint TP-self-signed-998521732
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-998521732
 revocation-check none
 rsakeypair TP-self-signed-998521732
!
!
crypto pki certificate chain TP-self-signed-998521732
 certificate self-signed 01 nvram:IOS-Self-Sig#1.cer
!
!
!
spanning-tree vlan 10 priority 8192
vtp file nvram:vlan.dat
username sdmsdm privilege 15 secret 5 $1$LJ9t$LiHr/DK73t0xOld.HUO9k1
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
!
!
ip ssh time-out 60
```

```
ip ssh authentication-retries 2
!
!
!
interface Loopback0
 description _SW_A_C_02_OSPF
 ip address 10.255.1.2 255.255.255.255
!
interface Port-channel1
 switchport mode trunk
!
~
!
interface FastEthernet1/1
 description _SW_A_C_01_f1/1
 switchport trunk native vlan 33
 switchport mode trunk
 channel-group 1 mode on
!
interface FastEthernet1/2
 description _SW_A_C_01_f1/2
 switchport trunk native vlan 33
 switchport mode trunk
 channel-group 1 mode on
!
~
!
interface Vlan10
 description NET-INTERCONNECT
 ip address 10.0.1.2 255.255.255.0 secondary
 ip address 10.0.1.129 255.255.255.0
 ip access-group 10 in
 no ip redirects
 ip ospf cost 10
 ip ospf hello-interval 2
 standby 0 ip 10.0.1.128
 standby 0 timers 1 3
 standby 0 priority 110
 standby 0 preempt
!
router ospf 1234
 router-id 10.255.1.2
 log-adjacency-changes
 redistribute connected
 redistribute static
 network 10.0.1.0 0.0.0.255 area 0
!
!
!
ip http server
ip http authentication local
ip http secure-server
ip http timeout-policy idle 600 life 86400 requests 10000
!
logging history informational
access-list 10 permit 10.0.0.0 0.255.255.255 log
access-list 10 deny    any log
access-list 10 remark VLAN10_IN
access-list 23 permit 10.0.40.0 0.0.0.255 log
access-list 23 permit 10.0.1.0 0.0.0.255 log
access-list 23 permit 10.1.1.0 0.0.0.255 log
```

```
access-list 23 permit 10.2.1.0 0.0.0.255 log
access-list 23 deny    any log
access-list 23 remark LINE_IN
access-list 90 permit 10.0.254.0 0.0.0.255 log
access-list 90 deny    any log
access-list 90 remark VLAN990_IN
access-list 99 permit 10.0.40.0 0.0.0.255 log
access-list 99 permit 192.168.204.0 0.0.0.255 log
access-list 99 deny    any log
access-list 99 remark SNMP_IN
snmp-server community c1sc0l4b RW 99
snmp-server enable traps snmp authentication linkdown linkup coldstart
warmstart
~
snmp-server enable traps rf
snmp-server host 10.0.40.10 c1sc0l4b
!
!
!
!
control-plane
!
banner motd □#####################
#                     #
#     Cisco Lab      #
#                     #
#####################□
!
line con 0
 login local
line aux 0
line vty 0 4
 access-class 23 in
 privilege level 15
 login local
 transport input ssh
!

!
webvpn cef
!
end
```

7.3   GNS3 Configuration

GNS3 is used mainly for topology drawing, because building Dynagen lab file is simpler with GNS3. In case of the designed virtual lab, the configuration file is almost 400 lines long. GNS3 is also used for running limited number of virtual devices on one computer.

The final lab configuration (*Figure 24*) contains 29 routers (switches are simulated only by EtherSwitch module), one virtual frame-relay switch and PIX firewall.
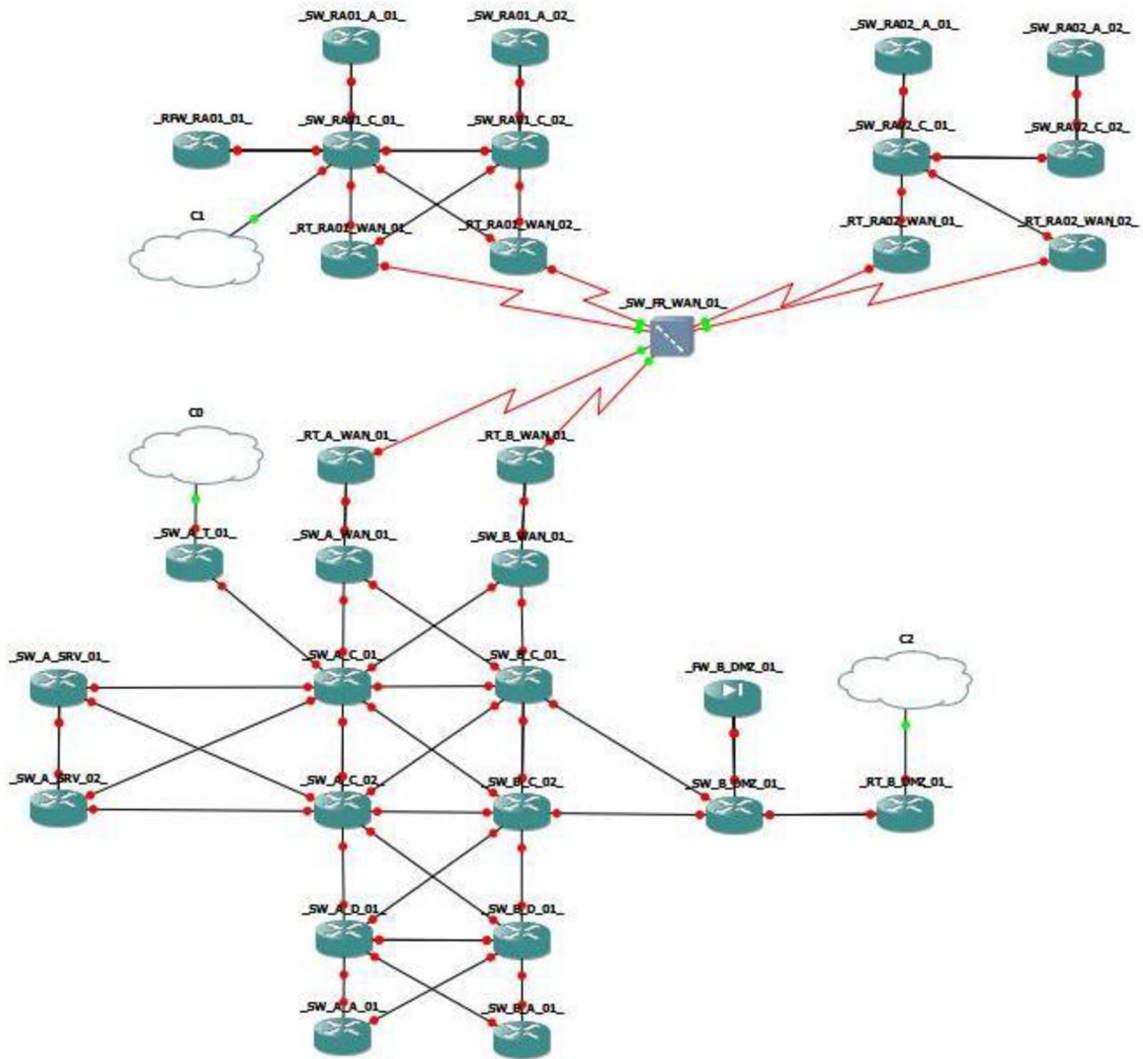
Figure 24   GNS3 virtual lab overview

GNS3 lab configuration file contains specification for each equipment including its position at lab overview. Bellow are listed specifics for PIX firewall and two switches.

MMST_v1.0_GNS3.net

```
autostart = False
[pemu localhost]
    workingdir = C:\CISCO_LAB
    [[525]]
        image = C:\CISCO_LAB\pix722.image
        serial = 0x00000000
        key = 0x00000000,0x00000000,0x00000000,0x00000000
    [[FW _FW_B_DMZ_01_]]
        e0 = _SW_B_DMZ_01_ f1/3
        e1 = _SW_B_DMZ_01_ f1/4
        e2 = _SW_B_DMZ_01_ f1/5
        e3 = _SW_B_DMZ_01_ f1/6
        e4 = _SW_B_DMZ_01_ f1/7
        x = -231.0
        y = 247.0
[localhost:7201]
```

```
     workingdir = C:\CISCO_LAB
     udp = 10100
     [[3745]]
         image = C:\CISCO_LAB\c3745-advsecurityk9-mz.124-15.T.image
         idlepc = 0x618ba000
         ghostios = True
         sparsemem = True
     [[ROUTER _SW_RA01_A_02_]]
         model = 3745
         console = 2030
         cnfg = C:\CISCO_LAB\_SW_RA01_A_02_.cfg
         slot1 = NM-16ESW
         f1/1 = _SW_RA01_C_02_ f1/3
         f1/2 = _SW_RA01_C_02_ f1/4
         x = -475.585786438
         y = -496.828427125
~
```

IOS image used on all devices is from advance security feature set; in T train. It supports all required services used in the virtual lab. By the means of Dynagen function *ghostios* and *sparsemem,* using only one image consumes less PC memory.

The attached *DVD* contains complete GNS3 preference file and lab configuration.

7.4   Dynamips and Dynagen Configuration

Dynagen configuration is almost identical to GSN3 just information about equipment's position is missing.

The first step to run Dynagen is to configure two .ini files. Bellow is content of *dynagen.ini* and *dynagenidledb.ini*.

dynagen.ini
```
idledb = C:\CISCO_LAB\dynagenidledb.ini
# Idle pc database. Contains values generated per IOS image.
telnet = start C:\progra~1\PuTTY\putty.exe -telnet %h %p
# Telnet configuration, in this case PuTTY will be used for console access.
```

dynagenidledb.ini
```
c3745-advsecurityk9-mz.124-15.T.image = 0x618ba000
```

Final Dynagen lab configuration is set to run distributed virtual lab simulation. For detailed description of the virtual lab design please refer to physical simulation layout (*File Layouts_-_Low_levels_-_Physical_Simulation_View_v1.0.pdf*). Next print-out is illustration of the Dynagen lab setting.

MMST_v1.0_Dynamips.net
```
autostart = False
ghostios = True
sparsemem = True
[PC_01:7201]
     workingdir = C:\CISCO_LAB
     udp = 10100
     [[3745]]
         image = C:\CISCO_LAB\c3745-advsecurityk9-mz.124-15.T.image
         ram = 256
         rom = 4
```

```
        nvram = 128
        disk0 = 64
        confreg = 0x2102
        idlepc = 0x618ba000
    [[ROUTER _SW_A_T_01_]]
        model = 3745
        console = 2025
        cnfg = C:\CISCO_LAB\_SW_A_T_01_.cfg
        slot1 = NM-16ESW
        f1/1 = _SW_A_C_01_ f1/5
        f1/15 = nio_gen_eth:\device\npf_{bf4895c4-0489-436c-b480-
8396205579b9}
~
```

The attached *DVD* contains complete Dynagen preference file and distributed lab configuration.

7.5   PEMU

As Cisco PIX firewall simulator is used program PEMU. Basic overview of the PEMU has been described in chapter *PEMU*, with step-by-step procedure for launching virtual PIX firewall. Following lines show issued PEMU and Pemuwraper configuration (Pemuwraper is used for integrating PEMU instance into Dynagen)

pemu.ini
```
serial=000000000
image=C:\CISCO_LAB\pix722.image
key=0x00000000,0x00000000,0x00000000,0x00000000
bios1=mybios_d8000
bios2=bios.bin
bios_checksum=1
```

pemuwrapper-start.cmd
```
@echo off
rem Launch pemuwrapper
set pemuwrapper=%CD%\pemuwrapper.exe
start /B /wait "Pemuwrapper" "%pemuwrapper%"
pause
```

7.6   SDM

Switches and routers which are part of the virtual lab are all configured for management by Cisco SDM. Cisco SDM program has been already described in chapter *Cisco Security Device Manager*.

Due to the fact that the SDM is available only to CCO users, its installation is not part of the attached DVD content. For demonstration of the SDM running within the virtual lab please refer to screenshots in SDM document (*File MMST_-_SDM.pdf*).

7.7   Nagios

Whole virtual lab is monitored by program Nagios. Nagios is installed in Debian VMWare machine and is connected to virtual lab as PC_01 (overview of the virtual lab shows physical simulation layout (*File Layouts_-_Low_levels_-_Physical_Simulation_View_v1.0.pdf*)).

To access the VMWare server and Nagios web interface use following passwords:

Debian standard user account:
user / password : user / user

Debian root account:
user / password : root / root

Nagios admin account:
user / password : nagiosadmin / nagios

All virtual devices are monitored by ping and SNMP. SNMP protocol is the most widely used monitoring tool (either by open-source or commercial projects). SNMP monitoring is really simplified in the virtual lab and it is used only for discovering device's uptime.

Nagios main configuration file contains links to hosts (groups) definitions and services definitions.

/usr/local/nagios/etc/nagios.cfg

```
~
cfg_file=/usr/local/nagios/etc/objects/switch.cfg
~
```

The file where are defined monitoring groups and assigned services is listed below. Nagios does not support management of configuration files thought the web interface, therefore all configurations and changes has to be manually issued in mentioned files.

/usr/local/nagios/etc/objects/switch.cfg

```
~
define host{
        use             generic-switch
        host_name       _SW_A_T_01_
# The name given to this switch
        alias           _SW_A_T_01_
# A longer name associated with the switch
        address         10.0.1.22
# IP address of the switch
        hostgroups      switches
# Host groups this switch is associated with
        }
~
define hostgroup{
        hostgroup_name  switches
# The name of the hostgroup
        alias           Network Switches
```

```
# Long name of the group
        }
~
~
define service{
        use                     generic-service
#       host_name               _SW_A_T_01_
# The name of the host the service is associated with
        hostgroup_name          switches
        service_description     PING
# The service description
        check_command           check_ping!200.0,20%!600.0,60%
# The command used to monitor the service
        normal_check_interval   5
# Check the service every 5 minutes under normal conditions
        retry_check_interval    1
# Re-check the service every minute until its final/hard state is
determined
        }
~
define service{
        use                     generic-service
# Inherit values from a template
#       host_name               _SW_A_T_01_
        hostgroup_name          switches
        service_description     Uptime
        check_command           check_snmp!-C c1sc0l4b -o sysUpTime.0
        }
~
```

In order to verify configuration, run Nagios with the -v command line option:
/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

The easiest way to start/stop/reload the Nagios daemon is by using the init script:
/etc/rc.d/init.d/nagios start
/etc/rc.d/init.d/nagios reload
/etc/rc.d/init.d/nagios stop

The Nagios daemon can be manually started with the -d command line option:
/usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg

Example of running Nagios and monitoring status of one core switch in Main site illustrates next figure (*Figure 25*).
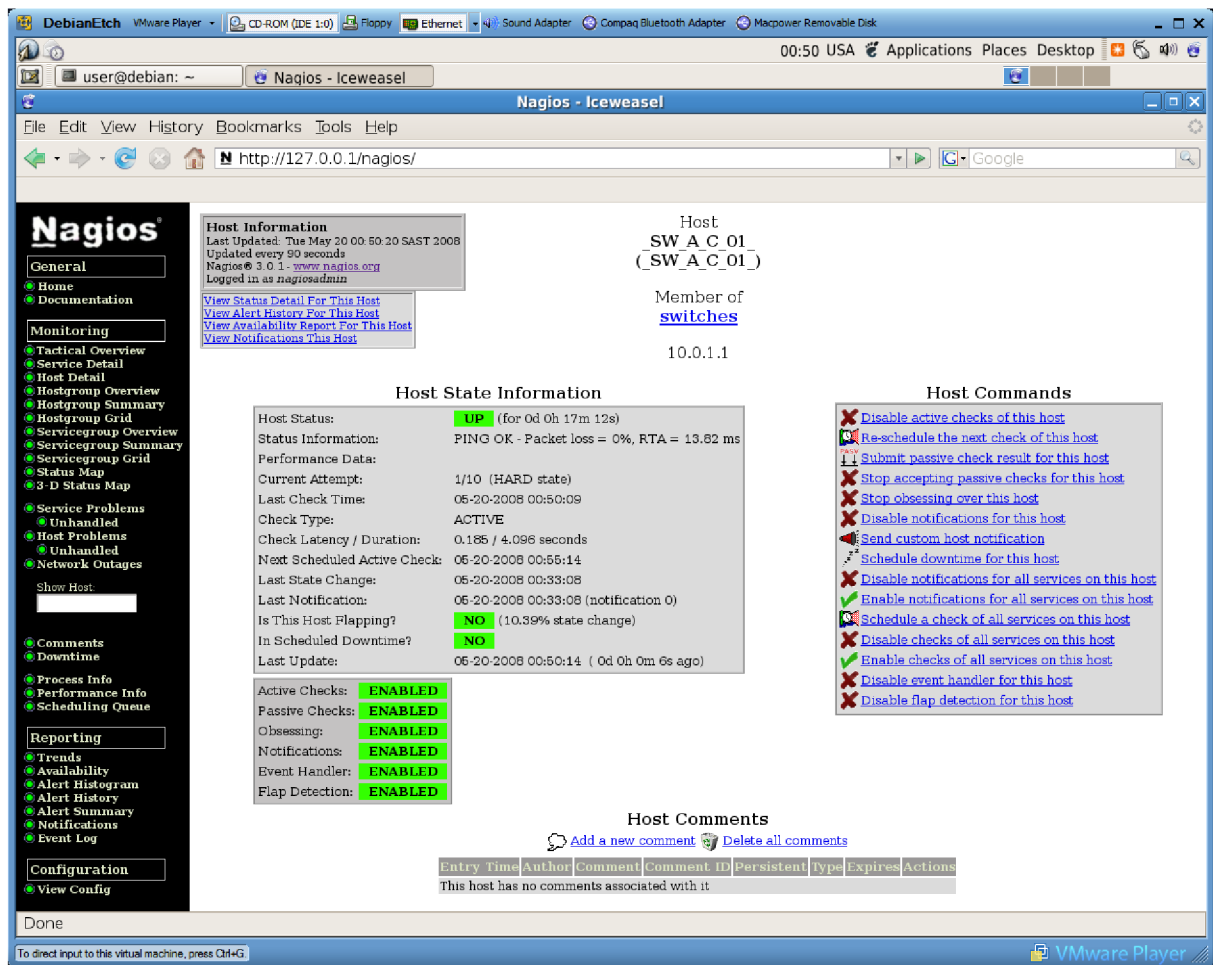
Figure 25   Nagios web interface

The attached *DVD* contains the VMWare Debian image with configured Nagios. For installation, configuration and management of the Nagios program please refer to [12].

7.8   PC Configuration

IP configuration of a PC, hosts file and IP routing are the only requirements to access the Dynamips simulation as real network. The IP routing on Windows machine can be little tricky, due to many active network interfaces (physical and loopbacks). It is necessary to manually configure IP routing table on each Windows PC, because Windows is creating default routes with the same metric for each active interface in the routing table.

Next print-outs show basic IP and hosts file configuration.

ipconfig

```
PS C:\> ipconfig

Windows IP Configuration

Ethernet adapter VMware Network Adapter VMnet8:
```

```
        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . : 192.168.204.1
        Subnet Mask . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . :

Ethernet adapter LAN_TOOLS:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . : 10.0.40.10
        Subnet Mask . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . : 10.0.40.1
~
```

hosts

```
127.0.0.1               localhost
127.0.0.1               PC_01
192.168.204.128         PC_02
192.168.205.3           PC_03
192.168.205.4           PC_04
192.168.205.5           PC_05
192.168.205.6           PC_06
```

Workstation IP configuration is illustrated by physical simulation layout (*File Layouts_-_Low_levels_-_Physical_Simulation_View_v1.0.pdf*).

8   Conclusion

General impression of this Master's Thesis could be that is brief with lots of references to resources and attached DVD with configurations and layouts. Reason for that is the MT and its required content are limited by length. The topics covered by the MT are so complex and just documentation published by Cisco concerning only network designs contains tens of thousands pages. Therefore content of the MT has been snippet and the main focus is paid to creation of network layouts and configuration of the whole virtual lab environment.

Theoretical part of the MT covers basic description of the network hierarchical design, primary campus network services and brief description of security.

Sixth chapter contains overview of monitoring, management and simulation tools which are used for realization of the virtual lab. There are also mentioned procedures to run these tools.

For demonstration of network designs, and main focus of the MT, concept of an enterprise network has been realized. Attached DVD contains detailed network layouts. Layouts describe hierarchical network architecture with focus on physical, logical, VTP and STP design.

Physical layouts are drawings of cable connections for the lab environment. Logical layouts focus on LAN IP management and also present the description of proposed application flows. IP routing protocol used in the lab is OSPF and as network protocol IPv4 is used. Other layouts describe VTP and STP designs of the virtual lab.

Layouts are not printed as attachments of the MT, because of their complexity and therefore are just saved on attached DVD. Printing layouts is usually not allowed in production environment also. The production practice is to store layouts in secure databases.

Virtual lab is running under Dynamips program with text-based Dynagen or graphical GNS3 front end. For Cisco PIX firewall simulation is used PEMU program. Because of CPU and RAM requirements, the lab is configured as distributed to run on five computers (plus virtual computer running Nagios). The simulation follows designed layouts exactly.

The lab is monitored by Nagios software by ICMP and SNMP protocols and as management tool is used Cisco SDM. Devices are accessible by SSH from management VLAN or through Dynagen by virtual serial connections.

Virtual lab is fully functional enterprise network with standard configurations and basic security measures. The lab can not replace real equipment for test, but is the cost-effective solution for educational purposes or tests that can not be performed in real production environment.

9 References

[1] Teare, D., Paquet, C. Building Scalable Cisco Internetworks (BSCI): Authorized Self-Study Guide. 3rd Edition. Cisco Press, 2006. 864 s. ISBN 1-58705-223-7

[2] Froom, R., Sivasubramanian, B., Frahim, E. Building Cisco Multilayer Switched Networks (BCMSN): Authorized Self-Study Guide. 4th Edition. Cisco Press, 2007. 984 s. ISBN 1-58705-273-3

[3] Ranjbar, A. S., CCNP ONT Official Exam Certification Guide. Cisco Press, 2007. ISBN 1-58720-176-3

[4] Morgan, B., Lovering, N., CCNP ISCW Official Exam Certification Guide. Cisco Press, 2007. ISBN 1-58720-150-x

[5] Teare, D. Designing for Cisco Internetwork Solutions (DESGN): Authorized CCDA Self-Study Guide (Exam 640-863). Second Edition. Cisco Press, 2007. 960 s. ISBN 1-58705-272-5

[6] Borza, A., Duesterhaus D., Switch Security Guidance Activity of the SNAC (Systems and Network Attack Center). Report Number: I33-010R-2004

[7] Antoine V., Bongiorni R., Router Security Guidance Activity of the SNAC (Systems and Network Attack Center). Report Number: C4-040R-02

[8] Cisco Validated Design Program, Last revision unknown, [quoted 25.5.2008], <http://cisco.com/go/designzone>

[9] Cisco Documentation, Last revision unknown, [quoted 25.5.2008], <http://cisco.com/univercd/>

[10] Computer Emergency Response Team, Last revision unknown, [quoted 25.5.2008], <http://cert.org/netsa/>

[11] Cisco Security Device Manager, Last revision unknown, [quoted 25.5.2008], <http://cisco.com/go/sdm>

[12] Nagios, Last revision 19.05.2008, [quoted 25.5.2008], <http://nagios.org/>

[13] Dynamips, Last revision unknown, [quoted 25.5.2008], <http://ipflow.utc.fr/index.php/Cisco_7200_Simulator>

[14] GNS3, Last revision unknown, [quoted 25.5.2008], <http://gns3.net/>

[15] PEMU, Last revision unknown, [quoted 25.5.2008], <http://pemu.net.cn/>

10 Appendix

10.1 DVD Content

```
MMST_-_MASTER'S_THESIS.pdf                          2 074 024  25.05.2008 01:58  -a--
MMST_-_POPISNY_SOUBOR_ZAVERECNE_PRACE.pdf             205 404  25.05.2008 02:01  -a--
MMST_-_SDM.pdf                                        439 039  20.05.2008 01:41  -a--
2 654 k in 3 files

[Configs]
0 k in 0 files

[Configs\Devices (IOS-PIX)]
_FW_B_DMZ_01_.cfg                                       5 005  19.05.2008 13:31  -a--
_RFW_RA01_01_.cfg                                       7 990  18.05.2008 02:31  -a--
_RT_A_WAN_01_.cfg                                       7 469  17.05.2008 17:06  -a--
_RT_B_DMZ_01_.cfg                                       6 840  18.05.2008 01:24  -a--
_RT_B_WAN_01_.cfg                                       7 476  17.05.2008 17:17  -a--
_RT_RA01_WAN_01_.cfg                                    7 637  17.05.2008 17:47  -a--
_RT_RA01_WAN_02_.cfg                                    7 624  17.05.2008 17:50  -a--
_RT_RA02_WAN_01_.cfg                                    7 253  17.05.2008 17:55  -a--
_RT_RA02_WAN_02_.cfg                                    7 222  17.05.2008 18:09  -a--
_SW_A_A_01_.cfg                                         6 628  17.05.2008 19:05  -a--
_SW_A_C_01_.cfg                                         7 641  17.05.2008 18:36  -a--
_SW_A_C_02_.cfg                                         7 256  17.05.2008 19:11  -a--
_SW_A_D_01_.cfg                                         8 540  17.05.2008 18:46  -a--
_SW_A_SRV_01_.cfg                                       8 045  17.05.2008 18:51  -a--
_SW_A_SRV_02_.cfg                                       8 056  17.05.2008 18:54  -a--
_SW_A_T_01_.cfg                                         6 370  17.05.2008 18:56  -a--
_SW_A_WAN_01_.cfg                                       7 283  17.05.2008 19:02  -a--
_SW_B_A_01_.cfg                                         6 653  17.05.2008 19:06  -a--
_SW_B_C_01_.cfg                                         7 496  17.05.2008 19:09  -a--
_SW_B_C_02_.cfg                                         7 153  17.05.2008 19:12  -a--
_SW_B_D_01_.cfg                                         8 533  17.05.2008 19:15  -a--
_SW_B_DMZ_01_.cfg                                       8 052  19.05.2008 13:33  -a--
_SW_B_WAN_01_.cfg                                       7 200  17.05.2008 19:19  -a--
_SW_RA01_A_01_.cfg                                      6 741  17.05.2008 19:23  -a--
_SW_RA01_A_02_.cfg                                      6 741  17.05.2008 19:25  -a--
_SW_RA01_C_01_.cfg                                     11 206  19.05.2008 13:32  -a--
_SW_RA01_C_02_.cfg                                     10 405  17.05.2008 20:22  -a--
_SW_RA02_A_01_.cfg                                      6 602  17.05.2008 22:00  -a--
_SW_RA02_A_02_.cfg                                      6 627  17.05.2008 22:02  -a--
_SW_RA02_C_01_.cfg                                     10 156  17.05.2008 22:08  -a--
_SW_RA02_C_02_.cfg                                      9 793  17.05.2008 22:11  -a--
232 k in 31 files

[Configs\Dynagen-Dynamips]
dynagen.ini                                               97  17.05.2008 22:29  -a--
dynagenidledb.ini                                        138  17.05.2008 22:28  -a--
0 k in 2 files

[Configs\GNS3]
gns3.ini                                                2 860  24.05.2008 02:20  -a--
2 k in 1 files

[Configs\PC]
hosts                                                     195  17.05.2008 22:36  -a--
0 k in 1 files

[Configs\Pemu-Pemuwrapper]
pemu.ini                                                 151  17.05.2008 22:30  -a--
pemuwrapper-start.cmd                                    126  04.03.2008 01:08  -a--
0 k in 2 files

[Configs\Simulation_Lab_Configs]
```

```
MMST_v1.0_Dynamips.net                                       11 075  18.05.2008 01:57  -a--
MMST_v1.0_GNS3.net                                           11 798  18.05.2008 02:38  -a--
22 k in 2 files


[Layouts]
Layouts_-_High_levels_v1.0.pdf                              352 872  25.05.2008 15:26  -a--
Layouts_-_Low_levels_-_Logical_v1.0.pdf                     182 282  25.05.2008 15:26  -a--
Layouts_-_Low_levels_-_Physical_Simulation_View_v1.0.pdf    234 721  25.05.2008 15:26  -a--
Layouts_-_Low_levels_-_Physical_v1.0.pdf                    368 488  25.05.2008 15:26  -a--
Layouts_-_Low_levels_-_Routing_v1.0.pdf                     312 074  25.05.2008 15:26  -a--
Layouts_-_Low_levels_-_SPT-VTP_v1.0.pdf                     377 616  25.05.2008 15:26  -a--
1 785 k in 6 files


[Programs - Monitoring & Management]
0 k in 0 files


[Programs - Monitoring & Management\Cisco Security Device Manager]
0 k in 0 files


[Programs - Monitoring & Management\Cisco Security Device Manager\Documentation]
Readme File for Cisco Router and Security Device Manager Version 2.4.1.doc
                                                            189 440  24.07.2007 23:54  -a--
SDMi21.pdf                                                1 005 756  21.11.2007 20:14  -a--
SDMr241.pdf                                                 373 101  24.07.2007 23:52  -a--
SDMv2.4-Readme.doc                                          147 968  21.11.2007 20:17  -a--
1 676 k in 4 files


[Programs - Monitoring & Management\Nagios]
0 k in 0 files


[Programs - Monitoring & Management\Nagios\Documentation]
nagios-3.pdf                                              1 896 035  28.04.2008 17:01  -a--
NDOUtils.pdf                                                298 917  28.04.2008 17:02  -a--
NRPE.pdf                                                    212 023  28.04.2008 17:02  -a--
PRE-RELEASE_The_Nagios_Book-05012006.pdf                   384 776  28.04.2008 16:14  -a--
2 726 k in 4 files


[Programs - Monitoring & Management\Nagios\Linux]
nagios-3.0.1.tar.gz                                       2 759 014  28.04.2008 17:03  -a--
nagiosmib-1.0.0.tar.gz                                        4 055  28.04.2008 17:04  -a--
nagios-plugins-1.4.11.tar.gz                              1 734 230  28.04.2008 17:04  -a--
4 391 k in 3 files


[Programs - Other]
0 k in 0 files


[Programs - Other\Windows]
0 k in 0 files


[Programs - Other\Windows\PuTTY 0.60]
putty.exe                                                  454 656  09.06.2007 12:24  -a--
putty-0.60-installer.exe                                  1 759 261  09.06.2007 12:29  -a--
2 162 k in 2 files


[Programs - Other\Windows\WinPcap 4.0.2]
WinPcap_4_0_2.exe                                          550 560  28.04.2008 17:12  -a--
537 k in 1 files


[Programs - Other\WMWare]
0 k in 0 files
```

64

[Programs - Other\WMWare\Debian Etch (Debian 4.0), Full Gnome Desktop]
DebianEtch.vmdk   520 20.05.2008 00:42 -a--
DebianEtch.vmem   100 663 296 11.05.2008 01:23 -a--
DebianEtch.vmss   18 086 249 20.05.2008 00:57 -a--
DebianEtch.vmx   1 290 20.05.2008 00:24 -a--
DebianEtch.vmxf   265 30.04.2008 20:07 -a--
DebianEtch-s001.vmdk   371 982 336 20.05.2008 00:56 -a--
DebianEtch-s002.vmdk   421 724 160 20.05.2008 00:56 -a--
DebianEtch-s003.vmdk   286 785 536 20.05.2008 00:56 -a--
DebianEtch-s004.vmdk   1 348 861 952 20.05.2008 00:56 -a--
DebianEtch-s005.vmdk   851 968 20.05.2008 00:56 -a--
Desktop.ini   123 11.04.2007 09:54 rah-
InstallDoc.txt   6 663 19.04.2007 11:57 -a--
nvram   8 684 20.05.2008 00:57 -a--
Readme.txt   2 566 19.04.2007 12:01 -a--
sources.list   1 027 19.04.2007 11:56 -a--
vm_folder.ico   25 214 23.12.2005 16:42 rah-
vmware.log   51 699 20.05.2008 00:57 -a--
vmware-0.log   41 590 19.05.2008 14:57 -a--
vmware-1.log   45 462 19.05.2008 14:33 -a--
vmware-2.log   40 923 14.05.2008 21:37 -a--
vmware-debian-etch-40r0.zip   466 937 058 28.04.2008 22:37 -a--
VMwareToolsDialog.txt   9 553 19.04.2007 11:56 -a--
2 945 437 k in 22 files

[Programs - Other\WMWare\VMware Player 2.0.3]
VMware-player-2.0.3-80004.exe   182 479 472 28.04.2008 17:31 -a--
VMware-player-2.0.3-80004.i386.rpm   68 995 595 28.04.2008 17:27 -a--
VMware-player-2.0.3-80004.i386.tar.gz 68 494 110 28.04.2008 17:27 -a--
312 469 k in 3 files

[Programs - Other\WMWare\VMware Server 1.0.5]
VMware-mui-1.0.5-80187.tar.gz   36 052 483 28.04.2008 17:20 -a--
VMware-server-1.0.5-80187.i386.rpm   106 125 780 28.04.2008 17:28 -a--
VMware-server-1.0.5-80187.tar.gz   106 920 012 28.04.2008 17:28 -a--
VMware-server-installer-1.0.5-80187.exe 153 929 880 28.04.2008 17:29 -a--
VMware-server-linux-client-1.0.5-80187.zip 23 571 694 28.04.2008 17:18 -a--
416 601 k in 5 files

[Programs - Simulators]
0 k in 0 files

[Programs - Simulators\Cisco 7200 Simulator (Dynamips - Dynagen)]
0 k in 0 files

[Programs - Simulators\Cisco 7200 Simulator (Dynamips - Dynagen)\Documentation]
Cisco 7200 Simulator 1.11.7 - Tutorial.doc   890 368 28.04.2008 16:50 -a--
869 k in 1 files

[Programs - Simulators\Cisco 7200 Simulator (Dynamips - Dynagen)\Linux]
dynagen-0.11.0.tar.gz   1 418 846 28.04.2008 16:58 -a--
dynagen-0.11.0-1.fc9.src.rpm   1 421 963 28.04.2008 16:57 -a--
dynamips-0.2.8RC1-1.i386.rpm   305 943 28.04.2008 16:58 -a--
dynamips-0.2.8RC1-1.src.rpm   571 850 28.04.2008 16:58 -a--
dynamips-0.2.8RC2-1.i386.rpm   314 915 28.04.2008 16:58 -a--
dynamips-0.2.8RC2-1.src.rpm   581 736 28.04.2008 16:58 -a--
4 507 k in 6 files

[Programs - Simulators\Cisco 7200 Simulator (Dynamips - Dynagen)\Windows]
dynagen-0.10.1_dynamips-0.8.0-RC1_Win_XP_setup.exe 3 866 174 28.04.2008 17:01 -a--
dynagen-0.11.0_win_setup.exe   6 705 251 28.04.2008 16:52 -a--

65

10 323 k in 2 files

[Programs - Simulators\GNS3]
0 k in 0 files

[Programs - Simulators\GNS3\Documentation]
GNS3-0.4.1_documentation.pdf   1 639 206 28.04.2008 16:56 -a--
1 600 k in 1 files

[Programs - Simulators\GNS3\Linux]
GNS3-0.5-src.tar.bz2   2 373 575 28.04.2008 16:55 -a--
GNS3-0.5-src.tar.gz   3 487 309 28.04.2008 16:55 -a--
5 723 k in 2 files

[Programs - Simulators\GNS3\Windows]
GNS3-0.5-win32-all-in-one.exe   10 079 170 28.04.2008 16:54 -a--
9 842 k in 1 files

[Programs - Simulators\PEMU]
0 k in 0 files

[Programs - Simulators\PEMU\Documentation]
0 k in 0 files

[Programs - Simulators\PEMU\Linux]
pemu_2008-03-03_bin.tar.bz2   309 467 28.04.2008 17:10 -a--
pemu_2008-03-03_src.tar.bz2   322 386 28.04.2008 17:09 -a--
617 k in 2 files

[Programs - Simulators\PEMU\Windows]
pemu_2008-03-03_win.zip   245 199 28.04.2008 17:10 -a--
239 k in 1 files

66