

KYMENLAAKSO UNIVERSITY OF APPLIED SCIENCES

Master of Engineering Degree Programme in Technology Administration

Vesa Kankare

IMPLEMENTATION OF A SERVICE PROVIDER NETWORKS STUDY UNIT
BASED ON VIRTUAL NETWORKING ENVIRONMENT

Master's Thesis 2015

ABSTRACT

KYMENLAAKSO UNIVERSITY OF APPLIED SCIENCES

Master of Engineering Degree Programme in Technology Administration

KANKARE, VESA	Implementation of a service provider networks study unit based on virtual networking environment
Master's Thesis	47 pages + 26 pages of appendices
Supervisor	Principal Lecturer Martti Kettunen
Commissioned by	Kymenlaakso University of Applied Sciences
May 2015	
Keywords	LCCE, Internet, Service Provider Networks, Cyber security

The goal of this thesis work is to improve the current service provider study unit into more realistic and practical learning experience. During the project a redesign of the content of the course is made to match the requirements of the current service providers. A new large-scale virtual laboratory environment is created to better support the hands on exercises. The topics covered in the lessons and the practical exercises come from a local service provider and represent the current technologies used in production networks.

Service provider networks are usually large and complex systems, which are not possible or economically viable to model in laboratory using real hardware. A major part of this work in addition to course design, is also a development of a supporting laboratory environment where all the studied technologies can be implemented in practice. The developed model will support exercises requiring multiple operators and eventually a very large Internet case study. There will also be cyber security point of view in design and the resulting system can be used to demonstrate and study various cyber threats related to service provider networks.

The environment created as a result of this thesis is multifunctional concept that can be expanded to model other Internet scale systems such as name server hierarchy. Virtualization of the laboratory network opens possibilities also for online courses and gamification.

TIIVISTELMÄ

KYMENLAAKSON AMMATTIKORKEAKOULU

Teknologiaosaamisen Johtaminen

KANKARE, VESA	Implementation of a service provider networks study unit based on virtual networking environment
Opinnäytetyö	47 sivua + 26 liitesivua
Valvoja	Yliopettaja Martti Kettunen
Toimeksiantaja	Kymenlaakson Ammattikorkeakoulu
Toukokuu 2015	
Avainsanat	LCCE, Internet, Operaattoriverkot, Kyberturvallisuus

Tämän työn tavoitteena on parantaa tämän hetkistä operaattoriverkkojen opintojaksoa realistisemmaksi ja työelämälähtöisemmäksi. Projektin aikana opintojakson sisältöä päivitettiin vastaamaan paremmin tämän päivän palveluntarjoajien vaatimuksia. Työssäni loin myös laajojen verkkojen laboratorioympäristön, mikä tukee paremmin opintojaksolla tehtäviä käytännön harjoitteita. Opintojakson aiheet tulevat paikalliselta palveluntarjoajalta ja edustaa heidän tuotantoverkoissaan käyttämiään tekniikoita.

Operaattorien verkot ovat tyypillisesti laajoja ja monimutkaisia järjestelmiä, joita ei ole mahdollista tai ainakaan taloudellista toteuttaa laboratoriossa käyttäen laitteistopohjaisia ratkaisuja. Iso osa tätä työtä opintojakson uudistamisen lisäksi on kehittää laboratorioympäristö, missä operaattoriverkkojen teknologioita voidaan toteuttaa käytännössä. Kehittämäni malli tukee operaattorien väliseen liikenteenvaihtoon liittyviä harjoituksia ja lopulta erittäin laajaa Internet reititysharjoitusta. Työssä on myös otettu huomioon kyberturvallisuuskulma ja tuloksena tehdyllä ympäristöllä voidaan tutustua ja harjoitella operaattoriverkkoihin kohdistuvia kyberuhkia.

Lopputuloksena syntynyt laboratorioympäristö on monikäyttöinen konsepti, jota voidaan laajentaa koskemaan muitakin Internet -kokoluokan järjestelmiä, kuten nimipalvelinhierarkiaa. Virtualisointi avaa myös mahdollisuuksia verkko-opiskeluun ja pelillistämiseen.

TABLE OF CONTENTS

ABSTRACT

TIIVISTELMÄ

1 INTRODUCTION	7
1.1 Significance of the competence in Internet routing technologies	9
1.2 KyUAS Information Technology.....	10
1.3 Similar projects and related products	11
2 PROJECT GOALS	12
2.1 Competence based learning.....	12
2.2 Platform supporting modern approaches to learning	12
2.3 Support and integration to other study units	13
2.4 Linkage to the cyber security	13
2.5 Laboratory network supporting modern MPLS network technologies....	13
3 OVERVIEW OF THE TECHNICAL DESIGN	14
3.1 Hardware and virtualization options	14
3.2 High level design of the environment	15
4 VIRTUAL OPERATOR NETWORK.....	16
4.1 System level design.....	17
4.2 Desktop computer requirements and limitations	18
4.3 Host operating system	19
4.4 Student network design	19
4.5 Other considerations.....	20

5 INTERNET SIMULATION PLATFORM.....	20
5.1 Internet technology and operation.....	21
5.2 Design of Internet simulation.....	23
5.3 Software	23
5.4 Routing Design	24
5.5 Use of BGP Communities.....	26
5.4 IXP	28
5.5 Web service providers.....	29
6 IMPLEMENTATION OF THE LABORATORY.....	29
6.1 Common Implementation Notes	29
6.1.1 KVM Host operating system.....	29
6.1.2 Network startup	30
6.1.3 Other common notes	30
6.2 Student Network specific implementation notes.....	30
6.3 Internet simulation specific implementation notes	31
7 SERVICE PROVIDER NETWORKS STUDY UNIT IMPLEMENTATION	32
7.1 Study unit overview	32
7.2 Lessons and their contents	32
7.2.1 Role of the IGP	32
7.2.2 MPLS and LDP	33
7.2.3 Any Transport over MPLS.....	33
7.2.4 Virtual Private LAN service.....	34
7.2.5 Layer 3 VPN Service	34
7.2.6 Advanced L3 VPN Services	35
7.2.7 Internet Routing	36
7.2.8 Case Study.....	36
7.2.9 Skill Exam.....	36

8 CONCLUSIONS.....	37
8.1 Results.....	37
8.2 Challenges experienced.....	38
8.3 Experiences as a teacher.....	39
8.4 Summary of feedback from the students.....	40
8.5 Ideas for future use.....	41
8.5.1 DNS Hierarchy.....	41
8.5.2 Provider services	41
8.5.3 Advanced Service Provider Networks	42
8.5.4 The Big Picture of Internet Project	42
8.5.4 Offensive Cyber Security Labs	43
REFERENCES	44

APPENDICES

Appendix 1: Service Provider Networks Lab Guide

Appendix 2: Feedback summary

1 INTRODUCTION

Internet has become a very important network in modern society. It is widely used for many vital functions and it is also basis for many areas of economy. Lots of services like banking, entertainment and logistics are relying on the Internet. Internet has been based on BGP (Border Gateway Protocol) for decades. The BGP protocol itself has been extended throughout its life to meet evolving needs of ever growing use of the Internet. Another protocol driving the Internet has been IPv4 (Internet Protocol version 4), which has reached its limits and is being replaced by IPv6 (Internet Protocol version 6). This technological evolution causes new security threats. But it is still BGP, which makes the Internet work whether it uses IPv4 or IPv6. Independent service providers who are interconnected together run the Internet by making agreements together without any centralized management.

Throughout its history Internet has faced some events, where it is completely been paralyzed or its service degraded severely because of problems or vulnerabilities in routing infrastructure. One of the events that gained a lot of attention was Pakistani telecommunications authority's order to filter YouTube from Pakistani Internet users. Government owned Pakistani Telecom managed to cut YouTube from the whole Internet by hijacking their prefix where YouTube DNS (Domain Name Service) servers were (McCullagh, 2008). The problem was caused by a flaw in the way BGP works and how networks were poorly configured throughout the Internet. The event would have been avoided if every network connected to the Internet had followed common guidelines and configured their networks accordingly. It was only the high level of expertise in YouTube network operations that enabled quick response and partial restoration of the services in less than two hours (Ripe.Net, 2008)

A threat to Internet routing can also be caused not by malicious or intentional activity, but also its huge scale. One of the events of this type is so called "512k event", where Internet routing table exceeded a 512 thousand-prefix milestone due to large operator Verizon splitting its aggregated prefixes in many smaller ones. What followed this change resulted some of the older Internet routers to exceed their memory capacity and fail. This caused outage to those networks, including one

Finnish operator, which served almost 70000 IP addresses. (Aben and Hogewoning, 2014)

Internet connects enormous amounts of computers and people together. In April 2015 there were over 50000 AS numbers (comparable to the amount of service providers and large enterprises) advertised in the Internet (Huston, 2015).

InternetLiveStats.com is estimating there is over 3.1 billion users in the Internet worldwide. (Internetlivestats.com, 2015) Internet is based on agreements between operators and there is no central administration of Internet. A popular Finnish science writer Esko Valtaoja referred Internet as an example of pure anarchist society, which works because co-operation is beneficial, and there is basically no limit of growth. (Valtaoja, 2004: 48) Internet is not owned by anyone and no single party can control it.

Internet routing is very complicated system and therefore it is very important that network operators have good understanding on how Internet works, both technology and policy point of view. In the same way a computer security is managed by the IT operators, networks have to be secured by network administrators. This model I study here, enables a possibility to simulate various Internet threats and policies and use that in part of cyber security teaching and research. This in turn gives students better understanding on the internal functions of the Internet and how they should take the cyber threats into account when they enter into real world jobs including Internet routing. In addition students will have real virtual router environment at their hand, so they will have very realistic hands on training on the topic. The work in this thesis is linked to a service provider course and is part of the study unit design also, which is in the scope of this work too.

Cyber security is also part of Finnish National Security Strategy and it highlights the importance of competence in such areas of expertise. (Valtioneuvosto, 2010) The importance of Internet routing in cyber security is also mentioned in Cyber Strategy of the United States of America as securing the critical Internet infrastructure including IP, DNS as well as BGP routing. (US-Cert, 2003: 30)

1.1 Significance of the competence in Internet routing technologies

Computer and network systems are becoming larger and larger part of everyday life and business. It is easy to look around and see how much of the services we use are depending on networks. More and more of critical information is stored on these systems and data is crossing over government borders and is handled by global companies.

A good example of an important service that is relying on Internet is banking services. In Finland more and more daily banking operations like paying bills or transferring money is handled through web services offered by banks. Nowadays banks does not have enough desk services to serve its customers in the case networks would be unavailable for sustained period of time. Even in the case they would have, probably some of their internal services might rely on the same physical networks and a well-targeted attack could affect also private services offered by service providers, thus rendering the desk services also unavailable. These services and systems handle all the money traffic and it is a critical for the whole society to function. It is thus very clear that cyber security is of high importance for finance.

Internet has also enabled business models and enterprises whose business model is completely depending on Internet. A concrete example of this kind of business is web commerce. The business of those companies will halt completely if Internet or the access to their web servers is not available.

In smaller scale similar effect might be very devastating to small business that uses a card payment service to take payments from customers. In countries like Finland card payments are very common and people rarely carries sufficient amount of money to pay for the goods. Continued loss of Internet availability may well mean days of lost sales for small shop if Internet is unavailable.

These examples are everywhere, entertainment, business interaction, email, etc. But also many traditional looking services like logistics are also heavily depending on networks, companies have online interfaces such as ordering and work order management systems which are connected through Internet. Even facility management systems, security and traffic control systems rely on networks. Internet

of Things is predicted to be the next major leap in the use of Internet and it will reveal a lot of new threats as the numbers and variety of devices will be connected to the network. (Nedeltchev, 2014: 6-7)

This change is rapid and it is becoming more and more recognized how important cyber security and networks actually are. Not only because reliability of these systems but also because of the confidentiality of the data transferred over networks. Increasing use and importance of digitalized world has led to more and more of a concern about security. And preparing for even more digitalized future and ever growing dependency on networks and computer systems is becoming essential. This requires more education and spreading of knowledge amongst the people designing and operating these systems as well as in the management level.

To be able to participate in such a special community as the Internet, service providers need to agree on certain parameters between each other. It requires technical knowledge but also understanding of how the ecosystem works. Both parties must be competent to configure their networks according to the agreement and take security threats into account by them selves. For example a mitigation of DDoS (Distributed Denial of Service) attack requires both technical knowledge and good co-operation between service providers. One of the ways for defending from such malicious traffic to restore services is to parameterize BGP routing in such way upstream operators will blackhole this malicious traffic closer to its source. Network World author Sean Leach lists lack of core competence as one of the key problems relying on service providers for DDoS attack mitigation. (Leach, 2013)

1.2 KyUAS Information Technology

Information Technology studies in KyUAS is based on four key competences: Data Networks, Cyber Security, Game Programming and Data Center Technology. Data Networks and programming (later Game programming) has been long in the offering, Data centers and Cyber Security are very current and important topics and including them as part of the Information Technology studies is an important development.

KyUAS is continuously doing pedagogical development. In 2009 a concept called LCCE (Learning and Competence Creating Ecosystem) was introduced as an ecosystem model for learning. The model aims for closer co-operation between business and university to achieve more rapid response to learning new skills required by employers. (Tulkki, 2009) This meant finding new ways to learn and has lead to interesting pedagogical experiments such as The Big Picture of Internet project, which has been a major source of ideas to this project also. (Kettunen, 2014)

Students beginning their bachelor's studies today will graduate four years from now. Internet-era devices, networks and services will evolve significantly during that time and the complete Internet ecosystem might be totally different then. This is completely unique field of technology and gives quite a challenge to the design of the study plan.

1.3 Similar projects and related products

JYVSECTEC is a program coordinated by JAMK University of Applied Sciences. Their RGCE (Realistic Global Cybersecurity Environment) is a large Internet simulation platform. It is very advanced system including background traffic, DNS system, security certificates as well as routing infrastructure. It also has an ability to connect to real hardware world. JAMK uses it as a teaching platform in their studies. However it is quite an extensive project and fixed in its location to serve as a research and development platform with JYVSECTEC's co-operation network. (jyvsectec.fi, 2014)

GNS3 is an open source network simulation platform. It includes a graphical user interface to build various model networks. It can interact with outside world, so it can also be used as part of the learning environment. (gns3.com, 2015)

Cisco VIRL is a Virtual Internet Routing Lab, a commercial product of Cisco Systems. It consists on several different virtualized router operating systems inside a KVM virtualization host. It also includes firewalls and lower end router software images. It is very interesting product and could serve as part of the environment described in this project. It includes an graphical user interface where user can build their own networks. (virl.cisco.com, n.d.)

Cisco VIRL and GNS3 both offer a very flexible practice platform for students where they can design their network from scratch, however, neither of them is well suited for the future ideas with gamification and online learning environments. Also they cannot be used to build a large-scale network as the Internet simulation.

2 PROJECT GOALS

2.1 Competence based learning

One of the big pedagogical topics in KyUAS is LCCE (Learning and Competence Creating Ecosystem), which highlights the importance of competence in education as well as close connection to local businesses. Creating competence is to learn by doing in addition to traditional theoretical approach. LCCE also focuses on co-operating with local companies and creates projects and study environments which are close to real life working environments.

Current lab network cannot support this approach. To be able to create real competence on service provider technologies a different approach has to be taken. This project aims for as realistic operator network operations experience as possible. Also this project is connected to the service provider industry through my previous job where I worked as a responsible manager of a small service provider MPLS network. All the ideas and topics of the lessons are real life examples how modern services are implemented in service providers network.

2.2 Platform supporting modern approaches to learning

One of the prominent uses of virtualization could be web-based learning and gamification, which could not be possible with current hardware based laboratory. The outcome of this project is intended to be very flexible platform for integration into web based learning environments and gamification ideas. Gamification is a fun way to motivate students to learn and it is proven to be an excellent tool in networking studies also as the Big Picture of Internet has shown us.

Also the environment should also support teamwork and project based studies, so virtualization should not be a limiting factor either. This sets a requirement for interconnecting virtual labs into each other and to hardware laboratory.

2.3 Support and integration to other study units

The virtualization model should also be supporting other study units, such as basic routing, cyber security and data center networks. This is natural outcome from virtualization, but it should be taken into account the model should be as flexible as possible and well documented so other study units can easily replicate the environment for their needs.

2.4 Linkage to the cyber security

One of the goals KyUAS set for the project was linkage to the cyber security. The Internet model should be supporting cyber threat simulation. Cyber security will be one of the key competences in information technology studies and its importance should be taken into related data networks studies also. Bringing Internet scale network models and programmable virtualization technology into the toolbox, gives endless opportunities to test and study cyber threats networks and network users may face. This thesis work only focuses on proofing the concept to certain level of modeling the Internet and some of the threats. If the pilot of the system is successful, more effort can then be placed into the further development.

2.5 Laboratory network supporting modern MPLS network technologies

A technical goal of this project is to create a working solution to the problems above and in a way that it supports modern MPLS network technologies. Major part of this work in addition to study unit development is to implement the technologies needed in the laboratory environment. It requires learning new technologies to be able to implement the required level of features.

3 OVERVIEW OF THE TECHNICAL DESIGN

The objective of the service provider study unit is to learn various technologies used in service provider networks. This includes basic MPLS technology, services run on top of MPLS as well as Internet routing. KyUAS ICTLAB has quite a nice selection of hardware routers, but they lack in numbers and features to efficiently teach technologies needed in large networks. They are primarily designed to be used in enterprise edge and LAN routing. One of the major goals of this thesis is to create a complete new lab environment to support modern service provider technologies.

3.1 Hardware and virtualization options

Modeling Internet routing and architecture with physical equipment is a demanding task. Many of the study cases require tens of routers to simulate real life scenarios. This kind of environment is expensive to purchase, difficult to manage and consumes lots of energy and space. Most of the lower end equipment does not have features needed for complex operator networks.

Using real Internet as study platform is either expensive or for many reasons impossible. It is unethical to use real production networks to test for example security issues related to Internet routing. Also some of the Internet technologies, such as anycast is practically impossible to implement in real internet.

Virtualization enables a possibility to simulate rather large networks, which can also be controlled and reconfigured by the host computer almost any imaginable way. This reconfiguration can be scripted and automated for any need. Properly established virtual platform can also be extended to connect into physical equipment, which gives an opportunity to practice with large networks using real world routers. This way both the real and virtual network benefits can be utilized. Physical connection can also be used to connect several virtualization platforms running in desktop computers together. That way students can also co-operate and do team work.

Using light virtualization techniques like containers in modern powerful computer a simulation of hundreds of routers can be run inside a single computer. Virtualization

also makes it very easy to create a dynamic environment where various scenarios can be run using scripts. Even gamification of exercises is possible, which gives a whole new dimension to laboratory work. Virtualized, software based network is also very easy to duplicate, or even run inside a virtual machine, thus making it possible to do personal case studies without having to share the environment with others.

Recently virtualized routers have become available. These are of particular interest because they run full routing software inside a virtualization platform. Using real router operating system enables possibility to teach operator level technologies as if they were real routers. Combined with lightweight systems, real world hardware and multiple computers this opens a wealth of possibilities to build very complex and large networks.

3.2 High level design of the environment

The design in this work consists of three different levels of virtualization and hardware.

- Physical hardware used as CPE devices and interconnection points
- Fully virtualized real router software used as realistic operator network running in student desktop computer
- Model Internet platform operated by teacher to simulate Internet scale network

All three of these can be interconnected together as a large case study of Internet routing. Figure 1 illustrates the high level design

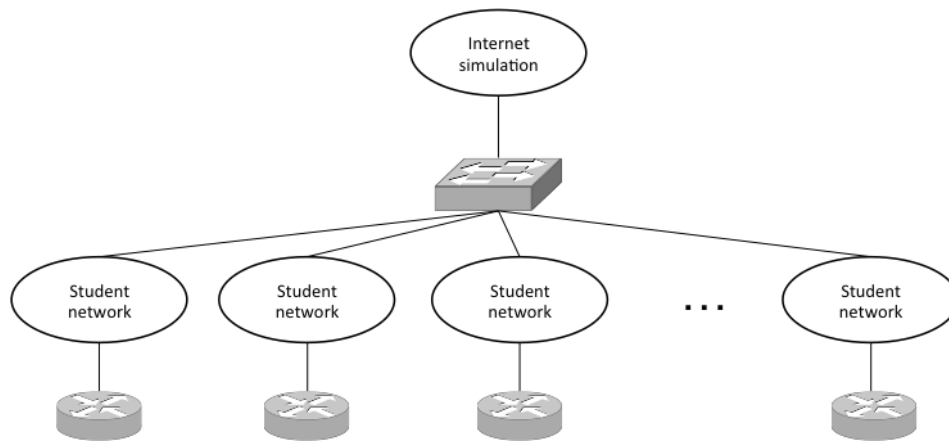


Figure 1: High Level Design

One of the laboratory switches is used as an interconnection point between each of the student networks and the Internet simulation. Rest of the routers and multilayer switches are then available to use as a customer endpoint devices.

The model is not limited to use as an Internet case study, student networks can also be connected together directly to enable studying of MPLS network interconnection models, such as Inter-AS MPLS VPN.

4 VIRTUAL OPERATOR NETWORK

Today's service provider networks are mostly based on MPLS technology and ran using high-end routers. Most of the operator network technologies are not available on enterprise level hardware currently used in ICTLAB. Some of the vendors offer virtualized versions of their high-end router software and IOS-XRv provided by Cisco Systems is used in this system. (Cisco.com, n.d.)

IOS-XRv is a complete router operating system used in the most powerful routers Cisco Systems offer in their product line. It has all the control plane features as the real world counterpart, lacking only some of the hardware-assisted functions in layer 2 VPN services. However that limitation doesn't prevent from creating those services, only real traffic is not available to be tested. Layer 3 functionality is available completely. For that reason it is completely applicable for Internet case studies and a perfect tool for learning latest innovations in MPLS technology. The version 5.3.0 supports even segment routing, a future technology, which may be the next big thing in MPLS networks. Segment Routing is a technology that simplifies

network and enables possibility of SDN (Software Defined Networks) in large-scale operator networks. (Filsfils and Marting, 2013)

4.1 System level design

There are few requirements of the student platform that needs to be addressed:

- Easy deployment and upgrade of the system
- Readymade network configuration
- Flexible outside network connectivity

Ease of the deployment is achieved using hypervisor nesting. Hypervisor nesting is a technology where hypervisor is run on top of another hypervisor. Student desktop computers have VMware Workstation software installed. The student network is then run inside a virtual machine, where Linux based KVM virtualization is used to run the actual virtual routers. That way the image can be built in advance and distributed as a single virtual machine to the student desktops.

Virtual machine image can then be built to include all the required network connections and basic configuration of the routers if needed. Teacher can also create scenarios for skill exams and distribute an image before an exam. The flexibility of outside connections is achieved by creating a virtual network adapter for each of the terminating router inside a KVM host. Students can then connect the routers to outside network or to another virtual machine. The virtualization layers is described in figure 2.

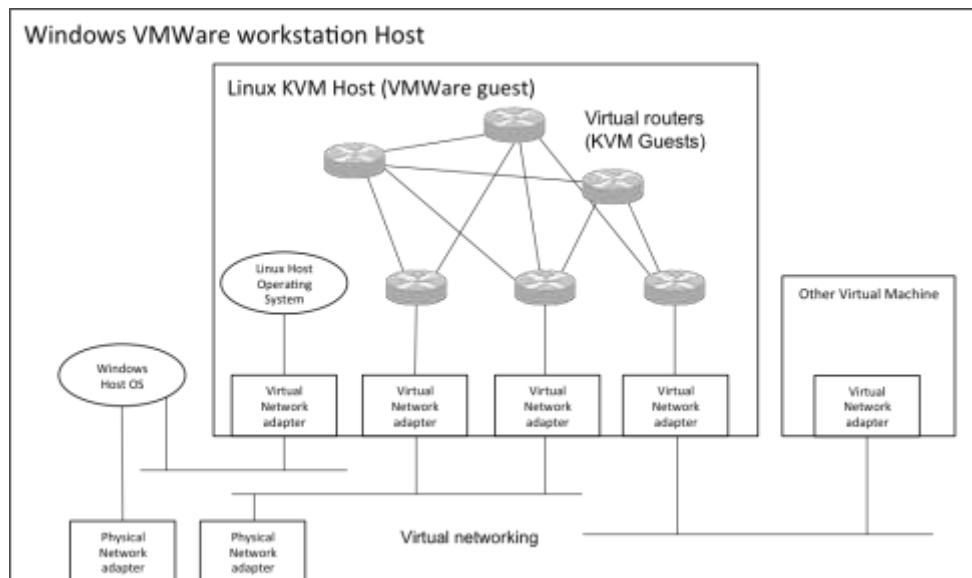


Figure 2: Student Platform virtualization layers

As seen in the figure, a VMware guest virtual machine holds a KVM virtualization system with router guests and router interconnects. Students have control over the desktop virtualization and can reconfigure the network inside VMware workstation for their needs.

4.2 Desktop computer requirements and limitations

Running a real router operating system is a resource-demanding task. Each of the IOS-XRv routers used in student network requires 3GB of RAM per specifications. Although powerful computers, the desktops in current laboratory have only 16GB of RAM equipped. However testing the system proved the routers can run with only 1.6GB to 2GB allocated memory depending on their function in the network. That enables possibility to run six routers in virtual machine that has 12GB memory allocated for the KVM host. Six routers is absolute minimum to create interesting exercises and was therefore selected for the final setup. ICTLAB is building a new computer class and due to this limitation a requirement for larger memory was given. New computer class desktops will also be equipped with more external physical interfaces to give more opportunities for outside connectivity.

MTU (Maximum Transmission Unit) is a limitation of how large frames can be transported across an interface or a bridge. The limiting factor is the maximum MTU of the system. VMware workstation does not support bridging frames over 1514

bytes, so adding an IEEE 802.1q VLAN tag or MPLS labels into packets transiting the VMware virtual networks limits the packet size from the standard 1500 bytes in IP layer. This limitation needs to be taken in account while designing exercises.

4.3 Host operating system

The host operating system and hypervisor running the routers was chosen to be Linux and KVM. Linux is a free operating system and it has plenty of possibilities through scripting. It is also very light operating system itself on resources due to no need for graphical interface. Linux also has a very simple virtual networking through bridging which makes it relatively easy to build the required connection between routers. KVM is also supported as hypervisor for IOS-XRv

Linux host was built to start the network automatically when the virtual machine is started. Several scripts were built for the purpose of booting the router guests and building the bridging between the routers and from the routers to the outside world. From the VMware host four virtual network interfaces were allocated for outside connectivity. One of the interfaces was reserved for management of the virtual routers. Each of the router guests was allocated a telnet port to which a virtual router console port is connected. Students can then access the consoles from their desktops of the routers using telnet to this port. Each router was assigned a number and a corresponding port number was described in lab guide (Appendix 1).

4.4 Student network design

Main purpose of student network is to teach MPLS technologies. To be able to see all the required MPLS forwarding plane cases a minimum of two P routers should be on a path from PE to PE. The network was designed to build upon three P routers and three PE routers in par with the limitations described in chapter 4.1. All the routers were redundantly connected to give possibilities to alter the topology by shutting down interfaces. Designed topology is described in figure 3.

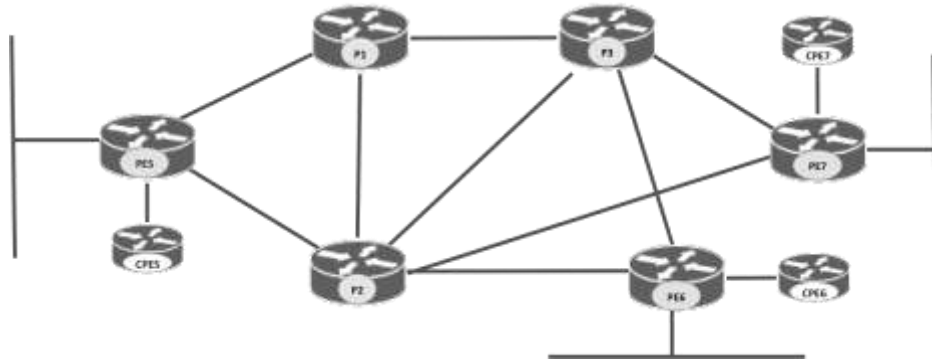


Figure 3: Student network topology

Each of the PE routers has an interface connected to KVM host interface, which can be then used in VMware virtual networking to connect the routers either to the outside world or to another virtual machine running on VMware host. Also lightweight LXC containers were connected to each of the PE routers to act as customer devices.

4.5 Other considerations

Distributing a single copy of complete virtualization system has also some factors that need to be taken into account. To be able to connect two devices together using an Ethernet connection, a unique MAC address is needed to communicate. Because the routers are cloned the KVM virtualization image, all of the student networks would then have same MAC addresses and duplicate addresses would prevent them from communicating with each other. To overcome this problem, the network startup scripts were programmed to randomize part of the MAC addresses to avoid collisions.

5 INTERNET SIMULATION PLATFORM

To be able to fully experiment with Internet routing topics, a simulation of large Internetwork was built in another virtual machine. As it is not used for teaching router configurations but just to simulate very large network, a lightweight virtualization using containers was used. Linux is able to virtualize at operating system level to conserve resources. Containers are not running full operating system on top of hardware virtualization but a virtual instance of its host's operating system

instead. The difference is illustrated in Figure 4. Container technology gives an opportunity to run tens or even hundreds of virtual instances in basic desktop system. For that reason container technology and Linux routing was selected for the Internet simulation.

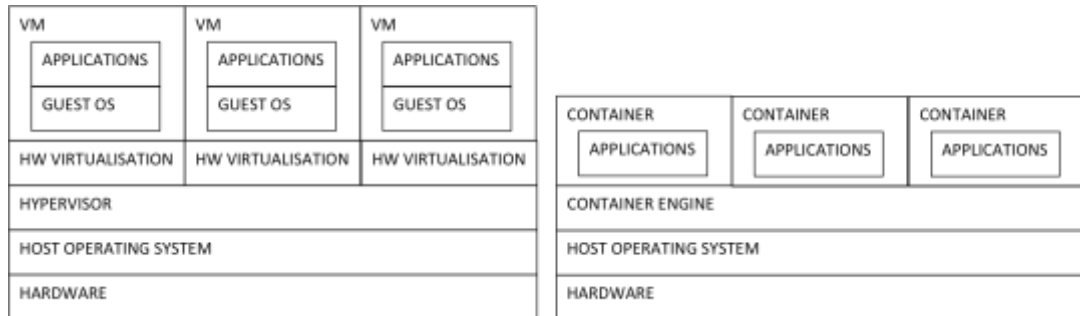


Figure 4: Containers vs. Hypervisors

Teaching Internet routing and routing security was the main goals of this project. For that reason in the following chapters a terms and technology behind Internet is described.

5.1 Internet technology and operation

Internet consists of several individually managed networks, called Autonomous Systems or AS for short. In practice an AS is a large network under single management usually operated by Service Provide or large Enterprise. Every AS holds at least one IP address block, called a prefix. This prefix along with an AS number is assigned by regional Internet registries like RIPE or ARIN. Regional registries are working under IANA, which is a top level Internet number authority. AS numbers as well as IP addresses and prefixes has to be globally unique to be able to work in Internet. AS number was originally a 16-bit number but later it is expected to be insufficient and a 32-bit AS number was standardized. (Vohra and Chen, 2007) This enables the growth of the Internet in future. Portion of the 16-bit AS number space (64512-65534) is reserved for private use. These Private AS numbers are not allowed in the Internet routing. (Mitchell, 2013)

Internet operators are classified to different levels called tiers. The classification is based on the way operator gets its traffic. Basically there are two ways to get traffic:

- Transit: Operator purchases traffic from another, usually larger operator. Traffic is usually paid per volume to an agreed minimum amount.
- Peering: Operators can exchange traffic with mutual agreement. No money is transferred. This is usually between operators in similar size

Small operators usually have to purchase all their traffic from transit operators. These are called Tier 3 operators. Usually for redundancy, transit is bought from two or more different higher tier operators. In addition to Tier 3 operators, large enterprises having their own AS usually work this way too. However very large enterprises that hold interesting enough traffic can attract higher-level operators into peering. Netflix and its movie streaming service is a good example of such an enterprise. Sandvine does regular interesting study about Internet phenomena and they found that Netflix has accounted for 34,9% of North American peak hours Internet traffic during second half of 2014. (Global Internet Phenomena Report, 2015)

Tier 2 operators are large enough to be able to get peering agreements and get a sufficient amount of their traffic via peering. They still need to purchase traffic from higher-level operators, but are interesting enough to be able to offer transit services to Tier 3 operators also. Largest national operators in Finland can be classified as Tier 2 operators.

Some of the largest (Tier 1) operators in the Internet are big enough to get all their traffic with peering agreements from another Tier 1 operators. (Winther, 2006) At first it sounds as a wonderful position in the market, but it is very difficult to hold your position at this level. Their customers (Tier 2 operators) are constantly trying to find a way to divert traffic past the Tier 1 operators and they constantly faces a threat to be de-peered, which means ending a peering agreement if the ratio of the size of the networks changes too much for the favor of the smaller one. (Berg, 2008: 4)

Internet Exchange Points or IXP's for short are organizations that operate a service where Internet operators can bring their network and starts peering with each other.

IXP's are usually an Ethernet switch or a VPLS service over MPLS and all the connected operators use addresses assigned by the IXP. IXP's are usually redundant and requires their members to connect to both IXP sites.

5.2 Design of Internet simulation

The project name for the simulation platform was chosen to be "Simternet". The name was coined to be in par with the other network simulation in ICTLAB, Simunet, which is a model implementation of small service provider MPLS network. From now on whenever Simternet is mentioned, it means the simulated Internet network inside the computer.

The Simternet was designed to operate much the similar way as the student platform. It runs as a VMware virtual machine running Linux as a guest operating system. But instead of having fully virtualized routers, the routers inside the simulation are built on top of Linux containers to save resources. Linux bridging is used to connect the containers together. Containers are also very easy to clone and their configuration can be altered directly from the host operating system. That way a large network can be built using scripting which eliminates the need for configuring large amounts of routers one by one. One thing that should be taken into account is the container backend storage. Cloning virtual machines without snapshot support from the file system grows the size of the simulation image significantly and can cause disk space problems and affect the movability of the image. A btrfs file system for example can support container snapshotting while very common ext4 cannot.

5.3 Software

Software used to run the simulation was chosen to be open source. Reasoning behind this is low (or zero) cost and good enough support for routing features.

Virtualization was done using Linux Containers or LXC for short. LXC containers are very light to run compared to hypervisor virtualization and offer more scalable solution. (linuxcontainers.org, n.d.) The downside is that every container has to run the same operating system as the host computer. However it is not a limiting factor for this project, since the simulation is to be run under Linux based routers and thus

using same operating system in all containers is fine. Use of LXC also enables relatively easy scripting of the container creation and configuration, which is a key requirement to this project. Handling tens of virtual routers by hand without automation would be too time consuming.

The containers need to run routing software to be able to simulate the Internet. There are many routing software packages available for Linux. Quagga is one of the most popular routing software and due to the fact it is recognized as good option widely, it was selected. Quagga supports BGP, OSPF and IS-IS and their extensions. Also it has a Cisco IOS like user interface, which is used in KyUAS other laboratory equipment. Most importantly is Quagga has support for Internet traffic management features like BGP communities and routing policies. (nongnu.org, 2013)

For different test and example cases, it is important to have real services also in the Simternet. Easy way to make this is to install lightweight www server into the containers. Lighttpd is a very small memory footprint www-server that is well suited for the task. (lighttpd.net, n.d.)

For scripting purposes Bash and Perl scripting was used to generate routers and their configurations.

5.4 Routing Design

The design goal was to create as realistic environment as possible to enable scenarios for as many Internet wide exercises as possible. The design needs to support exercises on traffic management and to be able to demonstrate Internet security threats and their mitigation. The topology of the design is described in figure 5.

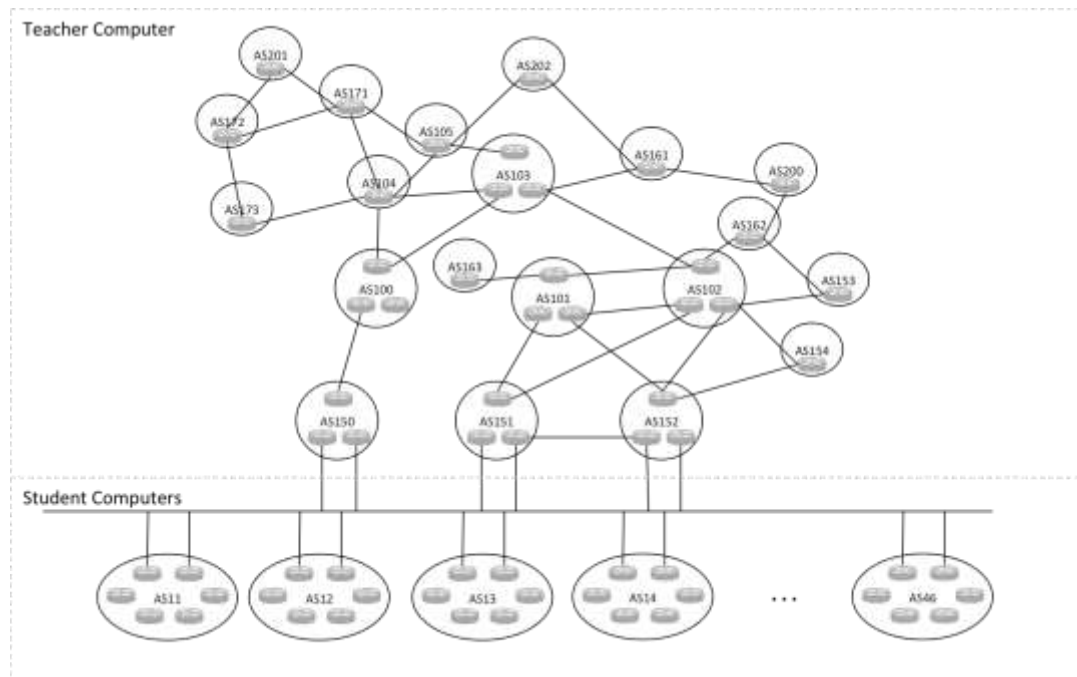


Figure 5: Simternet Topology

Simternet and the student networks consist mainly from Tier 2 (inside Simternet) and Tier 3 (Student Networks). Five Tier 1 operators form the core of the Simternet, which peer with each other and exchange full routing table. Tier 2 operators connect to the Tier 1 operators through several bridges inside the simulation. Tier 2 operators are thought to purchase traffic from the Tier 1 operators and their routing policy will be designed this idea in mind. They will also peer with each other into some degree. In Simternet there will be two kinds of Tier 2 operators. A well maintained networks with all the recommended filtering in place and ill maintained ones who have poorly designed filtering policy. The purpose of these differences is to demonstrate the importance of good network maintenance and well-designed policy in Internet security and how Internet is as weak as its weakest link. All Simternet routers are also accessible from student networks to enable students to see their point of view in routing infrastructure.

There are also various www-servers throughout the network. These are connected to operators with their own AS and BGP, like real world large web service providers. These www-servers will then be used to demonstrate security threats or can be made to mimic an operator policy web page. Www-servers can also be used to demonstrate Anycast in the network.

5.5 Use of BGP Communities

Simternet operators use BGP community attributes to signal additional information about their prefixes, as in real Internet. Communities can be utilized in traffic management and even signal blackholing to mitigate DDoS attacks closer to their sources. Traffic route manipulation is an effective tool if you need to avoid parts of the network due to congestion or other problems. The reason can also be purely economical. You might want to force majority of traffic to one operator offering lower quality, but more reasonable pricing and certain services to other, just for quality reasons even the cost is higher. Community attribute is in form ASN:nnnn, where ASN is an autonomous system of the operator. Many public community lists from several operators have been used as example in designing the communities for Simternet. (elisaip.net, n.d.) (Tele2, 2013) (Globenet, 2014)

Source of prefix is indicated using communities 1000 to 1999. This community is inserted into prefix attributes when prefix enters an operator network. It can indicate a way the prefix is inserted, IXP or particular router/location. Several communities can be added to single prefix. Following table describes prefix source communities:

1000	Customer or operators own network
1001	Peering
1002	Transit
1021	Router R1
1022	Router R2
1023	Router R3

For example community 100:1001 100:1021 would tell that router R1 in AS100 received the route from peering partner. Customer then can make local routing decisions based on this information.

The customer of operator can affect how upstream operator handles downstream traffic using communities designed to alter Local Preference attribute. Local Preference is a value which upstream operator will add to the route when it is received from customer. Higher local preference wins the selection when upstream operator routes the packet. This can be used to force downstream traffic to particular

link. Communities used for setting Local Preference is described in the following table:

2090	Set Local Preference 90
2100	Set Local Preference 100 (default)
2110	Set Local Preference 110

For example if customer of AS150 has dual links to his provider and they want to force traffic to primary link and leave the secondary link idle. They then set their own Local Preference to 110 for upstream traffic in primary link and advertise community 150:2110 to upstream provider to force downstream traffic to the primary link.

One common way of controlling prefix advertisements is to affect how the upstream operator advertises the prefix further. One very common way is to affect to the AS path length by prepending advertising AS to the AS path thus making it longer. The path selection is primarily based on AS path length and this way customers can control their prefix visibility and path selection in the Internet very effectively. The communities used to control advertisements are:

x = 0	Advertise as is
x = 1	Prepend one time
x = 2	Prepend two times
x = 9	Don't advertise
300x	All customers
310x	All peers
320x	All transits

For example looking from a AS104 point of view (in the Figure 5 topology) the path to AS12 is through AS100 and AS103 and seen as (100 150 12) from AS100 and (103 102 151 12) from the other side. Traffic will flow via AS100 due to shorter AS path. If AS12 for some reason wants the traffic flow through AS103 path and controls this by sending community 150:3202 to its upstream provider AS150. After this advertisement is fully converged in Simternet, AS104 sees the path (100 150

150 150 12) from AS100 and now selects AS103 as a better option due to shorter AS path.

Blackholing is a way to mitigate Denial Of Service attacks. Especially distributed attacks, which are usually very hard to mitigate. Suppose a customer has a very important service like online banking and it is bombarded with DDoS from Internet. The banking service fails and customer starts mitigating the problem. This service is used only domestically. DDoS is directed to single serving IP address. The option how they can now try to mitigate the issue is to signal their upstream operator to blackhole traffic to this host in the transit edges, but leaving national traffic intact. This will work in most cases since most of the DDoS sources are usually foreign addresses and national ones are easily managed with local authorities. This might ease the situation by allowing national customers access the service and thus leading almost complete service restoration, especially those addresses outside the affected one inside the same prefix. This uses community attributes together with AS Path control attributes. The community attributes are 9000-9999 in this case.

9000	Blackhole from all customers
9100	All peers
9200	All transits

For example, AS46 has DDoS targeted into 46.10.10.5. Inside the prefix where the address belongs there is also several other important services down because of the attack. Customer notices that all the malicious traffic is coming from other continent and starts mitigating the problem by advertising prefix 46.10.10.5/32 along with community 152:9200 to its upstream provider AS152.

5.4 IXP

To be able to connect student networks into the Simternet a simulated IXP is created. Due to limitations of the VMware workstations MTU there will not be real representation of different IXP's to the students. Instead a single VLAN switch is used to represent to IXP switches and only IP addressing is used to divide the IXP in two simulated IXP switches. This is brought outside the Simternet host operating system and connected to a laboratory switch where students can connect their

networks. Even there is a single physical connection, in network layer the network will function as if there were two different IXP points present. The prefixes used by these IXP points are 1.1.1.0/24 and 1.2.1.0/24 respectively. Students and simulated operators will use their AS number as the last nibble of the IP address to connect to the IXP. All Tier 2 level operators will have ready-made peers waiting for the student networks to connect.

5.5 Web service providers

To give a real feel of Internet use, some of the operators are designed to be operating a web service. These are used as practice targets for traffic control or security issue demonstrations.

6 IMPLEMENTATION OF THE LABORATORY

Due to the focus of this work, which is mainly the design and implementation of virtual environment to aid teaching and give more exciting exercises, only highlights of the actual implementation is presented here. More details will be in the technical documentation of the individual system.

6.1 Common Implementation Notes

6.1.1 KVM Host operating system

Both the student network and the Simternet were implemented on Ubuntu 12.04 LTS Linux virtual machine. Using minimal install the operating system footprint was very low to start with, which reserved resources for the actual Network virtualization. Both of the systems need LXC containers, which was installed into the operating system. To be able to provide needed services also VLAN support was added to the operating system. Most of the other required packages were there already from the beginning.

By default Linux operating system does some filtering of the traffic due to security issues. To make the network operate correctly ICMP redirecting and Reverse Path Filtering must be taken off.

6.1.2 Network startup

Both systems have startup scripts which purpose is to build the network inside the KVM host. These scripts are run on startup from */etc/rc.local*, so no other action is needed from the student who operates the network.

Outside network access virtual network interfaces was created using VMware workstation. Inside the KVM Host operating system these networks were connected to bridges used for internal communication. These connections were created using Bash scripts which will be run during the startup of the KVM host after the virtual routers have booted up.

One of the interfaces was reserved for management purposes. This interface is connected into a host only network in VMware workstation to enable access to the virtual network from the desktop. All console ports, management interfaces and the KVM host are connected to this network. On both systems 192.168.91.0/24 was selected to the management network and their addressing has been designed to be compatible with each other's, so they can run also in the same computer if needed.

6.1.3 Other common notes

Both systems were also documented briefly on */etc/issue* -file. This file contains a message, which is shown in the login screen of the operating system. It was used to give information about the version of the image, access credentials and addresses to the network components and other notes that might be useful for the students.

6.2 Student Network specific implementation notes

Student network used both the hypervisor virtualization and lightweight container virtualization. The IOS-XRv routers were installed into the KVM host using the installation guide provided by Cisco Systems. (Cisco.com, n.d.)

At first the network was indented to be with eight routers to make interesting exercises, but later it was found that low memory resources made it unstable and the

number of routers was reduced to six, which was possible to run using 12GB reserved memory for the KVM Host. Each of the routers was allocated a console port serial connection from host operating system and after the router has started, console shows the router booting.

Each of the P-core routers was allocated five interfaces for the interconnection of the core and PE routers. PE routers was allocated four interfaces; two for the uplinks, one outside connection and one for the internal CPE.

Internal CPE's was created using LXC containers. Each of the PE routers has a CPE each and these can be accessed using SSH from the host computer. These CPE's run on low resources and can be used to practice MPLS L3 VPN services.

6.3 Internet simulation specific implementation notes

Perl scripting was used to create the Internet simulation. Building large amounts of routers would be exhausting task to do by hand, so a programmatic approach was chosen. As a source for the scripts a simple text file "ASTABLE" and "PEERTABLE" was defined. These files define the virtual operators and their connections inside the simulation. The script reads the tables and creates all the required LXC containers, pushes the router and www service configurations into the container and starts the simulation.

Configuration of the routers is done through templates. These templates use several keywords indicated being between percentage marks (%). Script will then replace these keywords with the specific parameters for the particular router.

The functional part of the simulation is the IXP and the ability to students to connect to the simulation. The tables mentioned before includes also a special AS number "S", which indicates a macro for every possible student network. So whenever there is peering with "S", it will generate peers for all 24 desktops running student network platforms. That way all the required configuration is in place and it is just needed to start up the simulation and connect it to the switch together with the student networks.

7 SERVICE PROVIDER NETWORKS STUDY UNIT IMPLEMENTATION

7.1 Study unit overview

The service provider networks study unit goal is to learn technologies operators are using to provide services to their customers. These technologies include MPLS transport layer technologies such as IS-IS and LDP, MPLS services like Metro Ethernet and L3 MPLS VPN and Internet routing. Throughout the course students will learn how to build an operator network starting from transport layer and progressing into services. Every lesson includes a theory lecture and a lab exercise. The environment created during this project will be used in the lab exercises. Every lesson a new feature is added and the network is built incrementally. In the beginning students will operate their own network and as the course progresses they will start to connect the networks together, implementing MPLS interconnections and customer equipment connections to the services. Finally when all the services are built to support Internet routing, all the student networks are connected to the Internet simulation to make an Internet case study. During these sessions students will get the benefits from this project to learn how traffic is managed in the Internet and what security implications Internet routing has. Finally the course is graded based on a skill exam where students are acting as a member of an imaginary MPLS network operations team and given tasks to troubleshoot problem cases and implement new routers and services to the network.

7.2 Lessons and their contents

Following chapters describe the course content per lesson to highlight how the system is used in teaching and how the study unit is implemented. Students were given a lab guide (Appendix 1), which explains the exercises and how to implement them. The guide is designed to give only partial instructions, so the students need to figure out the complete solution to the problem from the hints given in the guide. Some of the exercises are challenge labs, where only the desired outcome is described without any instructions how to implement it.

7.2.1 Role of the IGP

Theory part of this lesson focuses on importance of IGP protocol to the service provider network. The main goal is to stress the importance of good practices on how IS-IS or OSPF should be configured and what the importance of the IGP is in the MPLS networks. Students will learn about maintaining IGP, using prefix-suppression to minimize routing tables and various ways to secure the MPLS network. Also, a brief introduction to IOS-XR operating system and service provider networks in general is given.

In the exercises the students will implement an IS-IS routing in the virtual student network lab. They will also learn the practical operational tasks related to IS-IS network and how for example prefix suppression affects the reachability of the Intra-AS links. They will implement adjustments on IS-IS metrics and secure the IS-IS neighborships.

7.2.2 MPLS and LDP

The second lesson focuses primarily on MPLS transport layer. MPLS transport layer is the most important part of MPLS network providing edge to the edge transport to the services. The students are presented MPLS network architecture and how MPLS transport and service layers are related together. MPLS packet forwarding and LDP (Label Distribution Protocol) as a label exchange protocol are described in detail.

Exercises will focus on building working MPLS infrastructure in student lab. They will implement LDP in their networks and use LDP features to secure LDP neighborships. After successful completion of the MPLS transport layer, MPLS OAM (Operation and Maintenance) features are used to study how MPLS forwarding plane works between PE (Provider Edge) routers.

7.2.3 Any Transport over MPLS

During this lesson students are learning about their first service; Any Transport over MPLS. Any Transport over MPLS or AToM for short is a technology service providers use to provide point-to-point services to the customers. AToM will appear as a virtual wire called pseudowire to the customer. The lesson will focus on EoMPLS (Ethernet over MPLS), which is one of the key technologies to provide

Metro Ethernet Services in MPLS network. A service label distribution mechanisms are described and how service labels and transport labels are related together. Students are also constantly reminded the MPLS architecture to point out the importance of MPLS transport layer studied in the first two classes. Several use cases for the AToM service will also be introduced to link the theory in real life applications, such as mobile backhauling.

During the exercise part of the lesson, students will implement EoMPLS pseudowire service into their network and explore various ways to connect towards customer using Cisco EFP (Ethernet Flow Point) infrastructure. Virtual lab created in this project lacks support of Ethernet services data plane so students will only be able to see only the control plane and OAM functionality, not the actual traffic passing through the pseudowire. However using the OAM features students will be able to observe transport layer importance via an exercise where LDP and IGP is intentionally made out of sync and caused a blackholing of traffic. Students then will implement features to overcome issues caused IGP and LDP being out of synchronization.

7.2.4 Virtual Private LAN service

Virtual Private LAN service or VPLS for short is a multipoint Ethernet service in MPLS network. Customer sees VPLS service as if it were an Ethernet switch reaching all the customer endpoints. Students will learn how VPLS works, how MAC addresses are learnt, what the loop avoidance mechanisms are and how to implement a VPLS service into an MPLS network. VPLS also has some scalability concerns, which will be addressed using hierarchical VPLS (H-VPLS). The principles of H-VPLS and its redundancy mechanisms are also covered during the lesson. Lab exercise of the lesson will include creating a VPLS service as well as H-VPLS service. The same limitation on data plane functionality is present in this exercise as in previous lesson.

7.2.5 Layer 3 VPN Service

Starting from this lesson, the rest of the course will focus on Layer 3 services on the MPLS network and virtual lab environment is gradually brought up into a full use.

In the similar way VPLS is used to create virtual switching environment into MPLS network, Layer 3 VPN creates a virtual routing environment. Using layer 3 functionality gives a lot more control on how traffic can be handled and it can scale up to routing Internet traffic over VPN. During this lesson students will learn how layer 3 VPN's are built from virtualizing a routing table to signaling routing information over the MPLS network using BGP and VPNv4 address-family. Concepts including VRF's (Virtual Routing and Forwarding), Route Distinguishers, Route Targets and label distribution are explained in detail. Also security concepts on hiding the infrastructure from customers are described.

In the lab exercise students will implement a layer 3 VPN between the CPE devices in their virtual lab environment. The goal of the exercise is to make fully working connections between the subnets CPE's are connected to. Students will see the effects of TTL propagation and will implement features to overcome the issue. After completing the guided exercises students are presented tasks they can use to experiment with their network and deepen the learned topics and create more customer to the network.

7.2.6 Advanced L3 VPN Services

Building upon previous lessons topics this lesson focuses on some more advanced topics in layer 3 VPN's. These topics include more complex topologies, passing customer network routing information to MPLS VPN using static or BGP routing, IPv6 enabled VPN's and Inter-AS VPN models. A revisit to basics of the layer 3 VPN's is also made to strengthen the basic understanding of the foundational technology.

Lab exercises will focus on enabling the newly learnt technologies into the student networks. During the Inter-AS MPLS VPN exercise students will work as pairs. As if they were two real operators, they will agree on connecting their networks together using Inter-AS VPN Model A and enable customer traffic across their network to network interconnection.

7.2.7 Internet Routing

This lesson will focus mainly on the technologies used in Internet Routing. The full use of the environment created in this thesis is taken into use. Students will learn about Internet routing, Core Hiding and routing policies. Some of the Internet routing security issues and technologies are also described.

In the lab exercise students will connect into the Internet simulation through an IXP switch and start to acquire capacity from the virtual operator inside the simulation. They also can start making peering agreements together and gradually create a very large network in the lab.

7.2.8 Case Study

Internet routing case study continues with traffic handling policies and security issue demonstrations. A prefix hijacking and DDoS attacks are demonstrated. Students are also given practice lab opportunities for the skill exam. Also a future technology lesson about Segment Routing is given and an opportunity to implement it in practice. The topic and the atmosphere in this class is intended to motivate experimenting with the simulated Internet and peering with colleagues.

7.2.9 Skill Exam

The assessment of the study unit is based in a skill exam. Skill exams purpose is to demonstrate student's ability to implement and operate MPLS networks and services. The exam is divided into two sections and is written as a scenario. It represents an MPLS network operators typical day at work, where he faces two trouble tickets and some implementation tasks.

First section of the exam is a troubleshooting test, where students are required to solve two trouble tickets they have received. Time given to this task is 20 minutes and every minute saved in this phase is earned in next phase. If student is not able to resolve the issues in time, the solutions will be revealed and student can continue to the implementation phase.

The second phase of the exam is to test the skills of implementing MPLS PE and MPLS services. Students are given a fresh new PE, which they need to bring up as a part of the MPLS infrastructure and services. Students are also required to implement services on to the network. Tasks will be gradually more difficult and the exam progresses in steps. After completion of each step, a student must get an approval from the instructor to continue with the exam. These checkpoints are then used to grade the exam and students will know exactly at which grade they are in as they progress in the exam.

This method of evaluation has been used in various information technology study units, however the use of troubleshooting together with implementation test is new.

8 CONCLUSIONS

8.1 Results

Virtualized laboratory environment is very flexible tool for teaching practical exercises. Especially in higher-level study units, where connecting the cables and building the basic configuration is no longer giving new insights to the topic. Also for study units like this service provider networks, features and technologies are only available in very expensive and power hungry routers. Virtualization gives access to these technologies, thanks to recent availability of virtualized routers.

Also much larger networks and experiments can be built. Only limiting factor is the computer capacity, which is constantly increasing. The new computer class room which is available in next implementation of the service provider study unit will be an ideal environment for virtualized network.

Internet simulation was also considered to be very interesting and it showed its potential already. Students were eager to try out policies and especially prefix hijacking techniques. Due to its complexity to build, all of the desired features were not implemented yet (like the blackholing of the DDoS traffic), but as a proof of concept it proved to be very useful tool for teaching and hopefully it will serve other study units also.

All in all this concept is opening new possibilities and it can definitely serve the competence based learning through more realistic exercises. I would say the project was success and definitely worth of taking into daily use in laboratory.

8.2 Challenges experienced

As this was the first time this kind of system was used in teaching especially at the beginning of the course several issues were faced with the virtual labs. As soon as the virtual lab was taken into use, resource issues caused the lab system to fail. The original image had eight routers and it seemed to be too resource intensive for the desktops currently in use in the ICTLAB. After reducing the number of routers to six the problem was resolved and students were able to continue using the virtual lab.

The virtualization images also tend to grow quite large, which may limit how often the image can be upgraded or transferred through the network. Especially the Internet simulation was growing very large, due to large amount of virtual machines. However later was found that choosing correct file system like BTRFS will solve the problem and compact the images.

Another major issue was the lack of proper support of layer 2 services data plane functions. This was found during the lab exercises and caused a bit of confusion during the exercises, but still the results were acceptable. Compared to the physical hardware lacking even the control plane support, students got an opportunity to implement the layer 2 services and observe the signaling and forwarding plane setup, even the traffic wasn't there.

There was also an unexpected blockage in one of the skill exam implementation tasks, which took a long time from the students to figure out. The solution was quite easy, but it was something the students hadn't faced before. That caused quite a large part of the students to fail the test or get a grade representing their skills. During a retake a method of "buying" off a blocking task with negative points will be introduced.

8.3 Experiences as a teacher

From teachers point of view it was good for the students they had to operate their network by themselves. Teamwork is an important part of studies but it can also lead into situations where members of the team are not able to see the whole picture in exercises. Members of the teams will also learn in different paces. This environment is giving more room to the individual to be able to work in his own pace and learn the technologies in full understanding. However the method described here does also support teamwork in form on Inter-AS VPN's and Internet peering. And teams are not constrained to the equipment they are using. That enables the possibility to find individuals working at same pace to continue doing the exercises together.

Virtualized environment also gave a better ability to distribute exercises and especially the skill exam. There is a similar skill exam using hardware routers in other study unit, and it is very big task to put all together and verify they are operational. Virtualization gives a possibility to build a skill exam image and test it out as an individual unit, then replicate it to the student computers and be sure everyone has the same starting point.

The goals of this project were met very well. The virtual laboratory environment was technically a success, although it had some issues at the beginning. As the virtualization image matured during the course, the more successful tool it became. We were able to go through even such an interesting new technology as Segment Routing. The students were able to do an interesting lab exercise on segment routing and probably were amongst the first to do that in practice. That was also a great learning experience to myself also. Also the Internet simulation was of great success, students networked themselves quite well and were able to implement policies and even did prefix hijacking exercises. We were able to also proof the concept of simulated DDoS attack, however the lack of controls in simulation did not give a possibility to defend against the attack. It is definitely something that needs to be implemented in next study unit implementation spring 2016.

Overall this showed to be a very effective way of teaching network technologies and is something that should be evaluated in other studies and projects also. Especially

the Cyberlab project might be beneficial of some of the technical ideas presented here.

8.4 Summary of feedback from the students

Feedback was collected using Moodle e-learning platform. The summary of the feedback received is in appendix 2. The feedback collected included overall questions to improve the content of the study unit and also feedback about the virtual laboratory. 6 out of 16 active students answered the questions.

Overall students were satisfied to the virtual lab, especially the Internet simulation was considered to aid in learning Internet routing. 83% of the responders were either agreeing or strongly agreeing to the argument. However having the network completely under control divided the responders almost completely in half the average being slightly above the neutral. This fact is something that needs to be taken into account in following implementations. One idea would be to implement a possibility to co-operate the same network using two computers and students could work in pairs.

Open questions about virtual lab were very encouraging. Here are few quotes from the responses translated into English:

“It was quite an interesting environment. Labs were handy and there was no need to play with the cabling”

“In my opinion similar system could be taken into use in other study units also”

“It would have been better to my learning if the simulations could have been able to be accessed from either my own computer (Which doesn't have enough memory) or outside the lectures (class room was often occupied and environment doesn't run in a server which could be accessed remotely)”.

“For once it was nice to be able to handle the complete system independently”

All in all these feedbacks really confirm that virtualized environment has truly a good potential and deserves to be developed further.

8.5 Ideas for future use

This environment was primarily designed to support the Service Provider Networks study unit. However similar systems can be built on other topics too. Here a few of the top ideas are presented for the consideration.

8.5.1 DNS Hierarchy

DNS plays a significant role in the Internet. Its main purpose is to convert Fully Qualified Domain Names (FQDN) into IP addresses for Internet routing. For people, it is easier to remember a domain name such as `www.facebook.com` than an IP address (`31.13.64.1` in this case for example). Creating a resolving DNS server is pretty straightforward, but it doesn't really give a picture how the system actually works. The simulated Internet model created in this project is also possible to incorporate a full DNS hierarchy with root servers including anycast nodes, used in Internet. This opens new opportunities to study security issues related to Internet DNS system.

8.5.2 Provider services

Service providers do much more than basic interconnection services. Usually they have DNS services, access networks, e-mail, web hosting etc. In the same way a student network environment was created during this project a simple ISP datacenter could be also build on top of a virtualization platform. Modern vendors offer their devices in virtualized versions also, so a full ISP server farm could be built using virtual firewalls and load balancers as well as workload servers. This kind of course aligned with the service provider course would open a possibility to run even more massive virtual system where almost real life like laboratory Internet could be built. The new planned computer class has powerful enough computers to run virtual

service provider network lab and an ISP system at the same time. Combined with the previous idea of DNS hierarchy this would lead into a complete picture of Internet. This could be an opportunity to create a one-of-a-kind huge lab exercise.

8.5.3 Advanced Service Provider Networks

Some of the modern service provider network technologies such as Seamless MPLS require a large amount of routers to do in practice. Seamless MPLS based on existing protocols and its purpose is to provide more scalability, better integration between aggregation, core and access and end-to-end resiliency.

Another interesting topic would be more deep insight on segment routing. Although the study unit included a brief introduction to segment routing as LDP replacement on transport layer, it didn't go deeper in the topic from traffic engineering or software defined networks point of view. Segment routing is an interesting technology, where you can encode routing instructions into the headers of the packet. This set of instructions is inserted by the source originating the traffic and no state information is needed in the MPLS network. (Bhamre, 2014)

8.5.4 The Big Picture of Internet Project

The successful BPI (Big Picture of Internet) project could be extended to even larger co-operative project based learning by adding an additional dimension from Service Provider Networks course outcome and others. BPI could be using Service Provider Networks virtual laboratory as service provider part of the environment and spare real hardware to more complex enterprise-level networks. Service Providers could operate their networks in separate computer classroom and provide services to the enterprises running their networks in hardware laboratory. It could be even extended to incorporate some of the ideas from optical networking and Data center study units. The result would be almost complete technical and operational representation of the Internet from customer perspective to service providers and their operations teams.

8.5.4 Offensive Cyber Security Labs

The virtual laboratory could also be used to constrain a network of computers, firewalls, servers and attack tools inside a single virtual platform. This way the exercises could be distributed as one file and also constrained strictly inside a hypervisor. It could also hide the targets completely inside the virtual machine to make the exercise more interesting while the student would not know what he is facing inside the exercise.

REFERENCES

Aben, E. and Marco, H. (2014). 512K-mageddon? — RIPE Labs. [online] Ripe.net. Available at: <https://labs.ripe.net/Members/emileaben/512k-mageddon> [Accessed 1 Oct. 2014].

Tele2, (2013). BGP Customer communities. [online] Available at: <http://as1257.tele2.net/network/communities.php> [Accessed 26 Apr. 2015].

Berg, R. (2008). How the 'Net works: an introduction to peering and transit. [online] Ars Technica. Available at: <http://arstechnica.com/features/2008/09/02/peering-and-transit/> [Accessed 3 May 2015].

Bhamre, K. (2014). Is Segment Routing the Answer to Carrier-Grade SDN? [online] Blogs.ixiacom.com. Available at: <http://blogs.ixiacom.com/ixia-blog/is-segment-routing-the-answer-to-carrier-grade-sdn/> [Accessed 26 Apr. 2014].

Cisco.com, (n.d.). Cisco IOS XRv Router Installation and Configuration Guide - Cisco IOS XRv Router Overview. [online] Available at: http://www.cisco.com/en/US/docs/ios_xr_sw/ios_xrv/install_config/b_xrvr_432_chapter_01.html [Accessed 24 Apr. 2015].

Cisco.com, (n.d.). Cisco IOS XRv Router Installation and Configuration Guide - Deploying the Cisco IOS XRv Router. [online] Available at: http://www.cisco.com/en/US/docs/ios_xr_sw/ios_xrv/install_config/b_xrvr_432_chapter_0100.html [Accessed 26 Apr. 2015].

Eunetip.net, (n.d.). Communities Used by ElisaIP. [online] Available at: <http://www.eunetip.net/communities.shtml> [Accessed 26 Apr. 2015].

Filsfils, C. and Marting, C. (2013). Segment Routing. [PowerPoint Slides] Presented at RIPE 66. Available at: https://ripe66.ripe.net/presentations/232-SR_RIPE_v2.pdf [Accessed 26 Apr. 2015].

Global Internet Phenomena Report. (2015). 1st ed. Waterloo, Ontario Canada: Sandvine, Inc ULC, p.6.

Globenet, (2014). BGP Communities. [online] Available at: <http://globenet.net/network/bgp-communities/> [Accessed 26 Apr. 2015].

Gns3.com, (2015). GNS3. [online] Available at: <http://www.gns3.com/index.php> [Accessed 26 Apr. 2015].

Huston, G. (2015). 32-bit Autonomous System Number Report. [online] Potaroo.net. Available at: <http://www.potaroo.net/tools/asn32/> [Accessed 24 Apr. 2015].

Internetlivestats.com, (2015). Internet Live Stats - Internet Usage & Social Media Statistics. [online] Available at: <http://www.internetlivestats.com/> [Accessed 24 Apr. 2015].

Jyvsectec.fi, (2014). RGCE. [online] Available at: <http://jyvsectec.fi/en/rgce/> [Accessed 26 Apr. 2015].

Kettunen, M. (2014). The Big Picture of Internet. In: Kiri, O., Huovi, T. and Malvela, P. eds. Learning Garden - Pedagogisia kukintoja LCCE mallin reunamilla. Kouvola: Kymenlaakson Ammattikorkeakoulu. Pp. 90-96.

Leach, S. (2013). Four ways to defend against DDoS attacks. [online] Network World. Available at: <http://www.networkworld.com/article/2170051/tech-primers/tech-primers-four-ways-to-defend-against-ddos-attacks.html> [Accessed 24 Apr. 2015].

Lighttpd.net, (n.d.). Lighttpd - fly light. [online] Available at: <http://www.lighttpd.net/> [Accessed 26 Apr. 2015].

Linuxcontainers.org, (n.d.). Linux Containers. [online] Available at: <https://linuxcontainers.org/> [Accessed 26 Apr. 2015].

McCullagh, D. (2008). How Pakistan knocked YouTube offline (and how to make sure it never happens again) - CNET. [online] CNET. Available at: <http://www.cnet.com/news/how-pakistan-knocked-youtube-offline-and-how-to-make-sure-it-never-happens-again/> [Accessed 1 Oct. 2014].

Mitchell, J. (2013). [online] RFC Editor. Available at: <http://www.rfc-editor.org/rfc/rfc6996.txt> [Accessed 24 Apr. 2015].

Nedelchev, P. (2014). The Internet of Everything is the New Economy. [online] Cisco. Available at: http://www.cisco.com/c/en/us/solutions/collateral/enterprise/cisco-on-cisco/Cisco_IT_Trends_IoE_Is_the_New_Economy.pdf [Accessed 3 May 2015].

Nongnu.org, (2013). Quagga Software Routing Suite. [online] Available at: <http://www.nongnu.org/quagga/> [Accessed 26 Apr 2015].

Ripe.net. (2008). YouTube Hijacking: A RIPE NCC RIS case study — RIPE Network Coordination Centre. [online] Available at: <http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study> [Accessed 1 Oct. 2014].

Tulkki, P. (2009). Oppimisen ja Työn Yhteys. In: Ruohonen, S. and Mäkelä-Marttinen, L. eds. Kohti osaamisen ja oppimisen ekosysteemiä. Kouvola: Kymenlaakson Ammattikorkeakoulu, pp.34-37.

US-CERT.gov, (2003). The National Strategy to Secure Cyberspace. [online] Available at: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf [Accessed 1 Oct. 2014].

Valtaoja, E. (2004). Avoin tie. Helsinki: Ursa.

Valtioneuvosto (2010). Yhteiskunnan Turvallisuusstrategia: Tiivistelmä. [online] Yhteiskunnanturvallisuus.fi. Available at: http://www.yhteiskunnanturvallisuus.fi/fi/materiaalit/doc_download/16-yhteiskunnan-turvallisuusstrategia-tiivistelmae [Accessed 1 Oct. 2014].

virl.cisco.com, (n.d.). VIRL - Virtual Internet Routing Lab. [online] Available at: <http://virl.cisco.com> [Accessed 26 Apr. 2015].

Vohra, Q. and Chen, E. (2007). RFC 4893 - BGP Support for Four-octet AS Number Space. [online] RFC Editor. Available at: <http://www.rfc-editor.org/rfc/rfc4893.txt> [Accessed 24 Apr. 2015].

Winther, M. (2006). Tier 1 ISPs: What They Are and Why They Are Important. 1st ed. Framingham, MA: IDC.

Service Provider Networks Lab Guide v0.9b

Kyminlaakso University of Applied Sciences, Vesa Kankare 2.4.2015. Applies to SPNET LAB Beta 8

Introduction

This guide will be a walkthrough instruction how to implement the exercises in the lessons using IOS-XRv virtual Service Provider Lab. Virtual lab is a single Ubuntu virtual machine which uses nested virtualization to deliver whole lab in single package. Inside Ubuntu is KVM based virtualization, which runs each of the IOS-XRv routers as guest. Lab needs at least 12GB allocated memory to run properly.

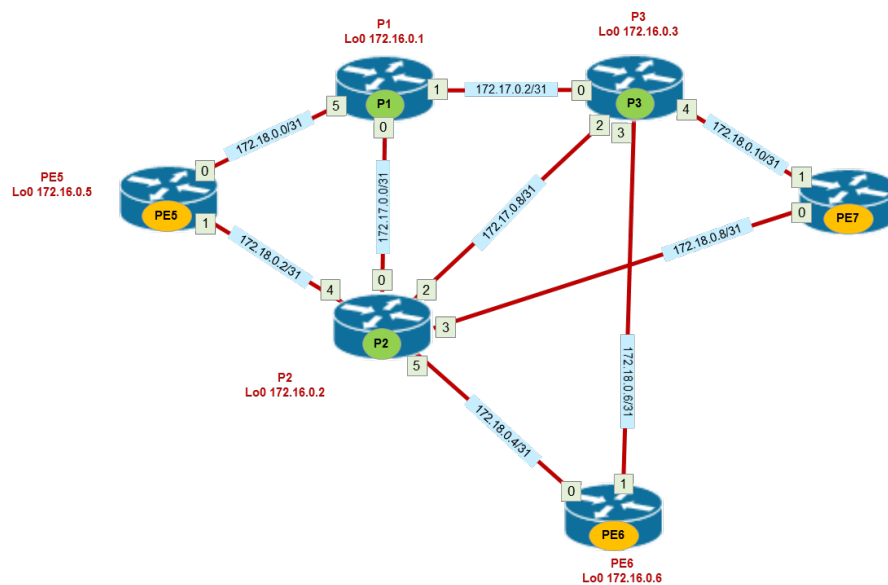


Diagram 1: Virtual Lab Topology

Routers are interconnected according to the diagram 1 and basic IP addressing and management interfaces are already configured. Management interfaces are connected into single Linux Bridge together with eth0, which is accessible from VMWare host-only network. The management network is 192.168.91.0/24 which may be needed to be configured to the VMWare workstation by the laboratory engineer (Requires administrative privileges).

Each of the PE routers has GigabitEthernet0/0/0/2 connected to the KVM host operating system interfaces for outside connections. These can be used to connect a lightweight Linux virtual machine as a CPE, or to connect to outside world using one of the VMWare host physical interfaces. Interfaces are eth1-3 for PE5-7 respectively.

Each router has an assigned number (P1, P2, PE5 etc), which is used in Loopback addressing and in management interfaces.

Loopbacks: 172.16.0.x

Management (COM): telnet 192.168.91.10:910x

Management (SSH): 192.168.91.20x

Where X is the router number. Note the network has to be fully operational, before SSH management is possible. It will take several minutes to boot the network in fully operational state. Username and password for the routers are *user/user*.

The state of the virtual machine can be saved as a snapshot. Service Provider lab will be incremental so each exercise will build upon the previous ones. Be sure to shut down the lab before taking the snapshot. Writing 12GB worth of memory wastes disk space and takes significant amount of time.

Desktop numbers

Some of the exercises need interconnection with other student lab networks. This requires unique numbering on some of the parameters (like IP addressing or AS numbers) Find your number using following table. Numbers start incrementing from right to left and from front to back, looking from students perspective

	TEACHER			
...	14	13	12	11
	...	23	22	21
		...	32	31
			...	41
				...

Table 1: Desktop numbers

CPE devices

The lab contains three CPE devices CPE5, CPE6 and CPE7 whose eth1 interfaces are connected to PE routers Gi0/0/0/3 interfaces respectively. You can access the CPE devices with ssh using IP address 192.168.21x where x is CPE number. Login as root and use *salasana* as password.

CPE's are run in Linux Containers and they have basic troubleshooting tools like ping, traceroute and tcpdump.

Setting CPE IP address

```
ifconfig eth1 10.10.5.10 netmask 255.255.255.0
```

```
ifconfig eth1 inet6 add 2001:DB8:10:5::10/64
```

Setting CPE default GW

```
route add default gw 10.10.5.1
```

```
route -A inet6 add default gw 2001:DB8:10:5::10
```

Showing routing table

```
route -n
```

```
route -n -A inet6
```

Tracerouting

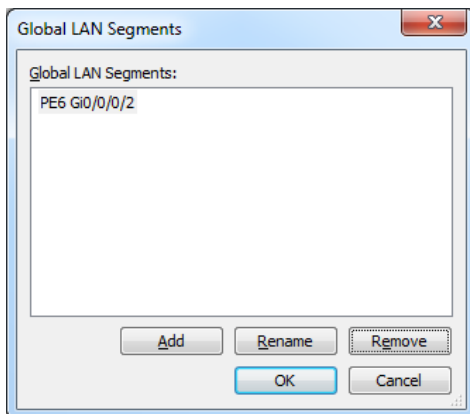
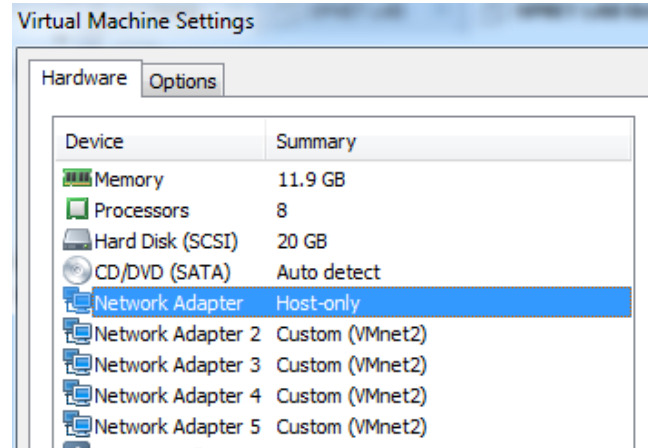
```
traceroute -n 10.10.6.10
```

```
traceroute6 -n 2001:DB8:10:6::10
```

If you accidentally misconfigure CPE and lose connection, reboot the CPE from the container console. Container console can be accessed from KVM host using `lxc-console -n CPE5`

External connections

External connections can be bridged to the outside world. Adapters 2-4 represents the Gi0/0/0/2 of each PE respectively. VLAN's or IP addressing can be used to separate traffic between PE's in outside connections. Note that using VLAN's will limit the MTU, since VMware workstation does not support Ethernet frames over 1518.



External connections can be linked to other virtual machines also, like a windows workstation. For that purpose, create a LAN segment into VMWare workstation and attach one of the PE interfaces and the virtual machine to that LAN Segment.

Lesson 1: IOS-XR basics and role of the IGP

Exercise 1.1: IOS-XR configuration mode

Familiarize yourself with IOS-XR configuration management

Step 1: Enter the configuration mode and add a description to CPE interfaces in PE routers

PE5# configure terminal

```
interface GigabitEthernet0/0/0/2
description TO CPE
!
```

Note: In this phase the configuration is not active yet

Step 2: Commit/discard changes

Exit the configuration mode either using `exit` command, or CTRL-Z. Changes can also be committed using `commit` command. Explore various ways to commit, cancel or discard changes.

Exercise 1.2: Configuration rollback

Cancel your previous changes using configuration rollback feature of IOS-XR

Step 1: Find out the commit you want to rollback to

```
show configuration commit list
```

Memorize the SNo of the configuration you want to roll back to. (or copy it to clipboard)

Step 2: Rollback to the selected configuration

Use the selected SNo from previous step.

```
rollback configuration to 10000000nn
```

Step 3: Verify the rollback was successful

```
show running-config
```

Step 4: Reconfigure back the rollbacked changes

Exercise 1.3: Configure IS-IS routing

Configure IS-IS routing between the routers. IGP has a major role on running an MPLS network. Each of the routers loopback address has to be reachable. IGP should also be kept clean from unnecessary routes.

Step 1: Enable IS-IS routing process and set the Network Entity

Replace x with router number in the following command.

```
router isis SPNET
  net 49.000.000.000x.00
!
```

Step 2: Include interfaces in IS-IS routing for ipv4

Only Loopbacks, P-P and P-PE interfaces should be added, not interfaces facing customers (Security!)

```
router isis SPNET
  interface Loopback0
    address-family ipv4 unicast
  !
  interface GigabitEthernet0/0/0/0
    address-family ipv4 unicast
  !
!
```

Step 3: Verify

Verify IS-IS neighborships are formed and IS-IS routes are appearing in routing table.

```
show isis neighbors
show isis database
show route
```

Exercise 1.4: Configure prefix suppression

Link subnets are not needed in MPLS network operation and should not be included in routing database. Configure IS-IS for prefix suppression and point-to-point links

Step 1: Configure prefix suppression

```
router isis SPNET
 interface GigabitEthernet0/0/0/0
   suppressed
   point-to-point
!
```

Step 2: Verify operation

```
show route
show isis database
```

You shouldn't see any of the link subnets advertised by IS-IS (only connected ones)

Ping PE7 Loopback from PE5 (ping 172.16.0.7). Explain why it's not working.

Lesson 2: MPLS LDP

Exercise 2.1: Enable MPLS LDP

Enable MPLS LDP on all of the routers. Make sure the router-id used is fixed to Loopback0 address

Step 1: Enable MPLS LDP and set a router-id

```
mpls ldp
 router-id 172.16.0.1
!
```

Step 2: Verify configuration

```
show mpls ldp parameters
```

Exercise 2.2: Enable MPLS LDP

Add interfaces into MPLS LDP operation. All P-P and P-PE links should be added. No customer facing interfaces should be added (Security risk!)

Step 1: Enable LDP on interfaces

```
mpls ldp
 interface GigabitEthernet0/0/0/0
!
```

Step 2: Verify configuration

```
show mpls ldp interface
show mpls interfaces
```

Exercise 2.3: Configure MPLS LDP authentication

Enable LDP authentication for all of the peers. Note: It can also be enabled per neighbor basis

Step 1: Enable LDP authentication

```
mpls ldp
 neighbor password clear cisco
!
```

Step 2: Verify LDP sessions are back up

```
show mpls ldp interface
show mpls interfaces
```

Exercise 2.4: Troubleshoot LSP

Find out how packets are flowing from PE5 to PE7 using show commands. Disable PE7-P2 link to see P-P labels.

Step 1: Shutdown PE7-PE2 link. Verify correct path

```
show route
```

Step 2: Trace the labels from PE5 to PE7 through

```
show mpls forwarding
```

Describe what labels and exit interfaces are used in each of the hops

Exercise 2.5: Enable MPLS OAM tools

Enable MPLS OAM tools for all of the routers.

Step 1: Enable MPLS OAM tools

```
mpls oam
```

Step 2: Verify operation

```
traceroute mpls ipv4 172.16.0.7/32 source 172.16.0.5
```

Compare the results with previous exercise.

Why is it important to use source address in traceroute command above?

Lesson 3: AToM Services

Exercise 3.1: Port Mode EoMPLS

Build a port mode EoMPLS service between PE5 Gi0/0/0/2 and PE7 Gi0/0/0/2. **Note: IOS-XRv does not implement a L2VPN Forwarding plane**, so real traffic cannot be demonstrated. However control-plane features are still available.

Step 1: Enable pseudowire logging to see the changes in pseudowire statuses

```
l2vpn
```

```
logging
 pseudowire
!
```

Step 2: Create l2transport interfaces on PE5 and PE7

```
interface GigabitEthernet0/0/0/2
 l2transport
!
```

Step 3: Create a VPWS service between interfaces

```
l2vpn
 xconnect group BASIC
  p2p CUSTOMER1
    interface gigabitEthernet 0/0/0/2
      neighbor 172.16.0.5 pw-id 123456
    !
  !
!
```

Step 4: Use troubleshooting tools to find out information about VPWS tunnel

```
show l2vpn xconnect pw-id 123456
```

What are the VC labels used for the connection?

Does the pseudowire use control word?

What are the MTU values of termination points?

Step 5: Verify the tunnel is operational using MPLS OAM tools

```
ping pseudowire 172.16.0.7 123456
```

Use troubleshooting tools from last exercises to find the LSP from the forwarding information

Exercise 3.2: VLAN Mode EoMPLS and rewrite

Implement a VLAN mode EoMPLS service with flexible tag rewrite options

NOTE: IOS-XRv has issues with this exercise and the pseudowire reports following error message. So lab is not possible to do in virtual lab.

Error: ATOM Dynamic with mismatched AC config

Exercise 3.3: Configure Control-Word using PW Class

Enable Control-Word for the pseudowire.

Step 1: Create a pseudowire class SPNET

```
l2vpn
 pw-class SPNET
   encapsulation mpls
   control-word
 !
!
```

Step 2: Attach the pseudowire class into a VPWS service

```
l2vpn
xconnect group BASIC
  p2p CUSTOMER1
    neighbor 172.16.0.5 pw-id 123456
    pw-class SPNET
  !
!
!
!
```

Step 3: Verify the configuration was successful

```
show l2vpn xconnect pw-id 123456
```

What the frame headers will now be during the transit?

Exercise 3.4: Configure Backup Pseudowire

Configure a backup pseudowire so that if PE7 fails, tunnel will be redirected to PE6. Avoid flapping by waiting 60 seconds before returning to original state.

Step 1: Prepare PE6 to be able to receive the tunnel with same parameters as PE5.

Use examples from exercise 3.2 PE7 configuration

Step 2: Configure a backup tunnel from PE5 to PE6

```
l2vpn
xconnect group BASIC
  p2p CUSTOMER1
    neighbor 172.16.0.7 pw-id 123456
    backup neighbor 172.16.0.6 pw-id 123456
    pw-class SPNET
  !
!
!
```

Step 3: Verify configuration by shutting down PE7 Gi0/0/0/2

Shutdown Gi0/0/0/2 (make sure to commit!) and verify tunnel redirection

```
show l2vpn xconnect pw-id 123456
ping pseudowire 172.16.0.6 123456
```

Step 5: Verify backup disable by enabling PE7 Gi0/0/0/2

Issue no shutdown Gi0/0/0/2 (make sure to commit!) and verify tunnel redirection

```
show l2vpn xconnect pw-id 123456
ping pseudowire 172.16.0.7 123456
```

Exercise 3.5: Explore effects of broken transport LSP

EoMPLS needs to have working transport LSP for it to work completely. It might happen an LDP and IGP (ISIS in this case) is out of sync and a broken LSP is formed.

Step 1: Redirect the traffic into going route P1-P3 by shutting down P2 links on PE5 and PE7

Step 2: Make sure you have still operational tunnel by pinging the pseudowire

```
ping 172.16.0.7 source 172.16.0.5
ping pseudowire 172.16.0.7 123456
```

Step 3: Remove LDP from the P1-P3 link

```
mpls ldp
no interface...
!
```

Step 4: Observe what happens

```
ping 172.16.0.7 source 172.16.0.5
ping pseudowire 172.16.0.7 123456
```

Explain what happens. Leave it as is for the next exercise

Exercise 3.6: Implement IGP Synchronization

IGP sync verifies LDP is operational before using the metrics assigned to interface. Labeled traffic can then route around unsynchronized links.

Step 1: Enable IGP Sync

Enable IGP synchronization on all MPLS links

```
router isis SPNET
interface GigabitEthernet0/0/0/1
address-family ipv4 unicast
mpls ldp sync
!
```

Step2: Verify operation

Verify EoMPLS tunnel is working

```
ping 172.16.0.7 source 172.16.0.5
ping pseudowire 172.16.0.7 123456
```

Verify ISIS LDP sync is working

```
show isis interface
Verify packet are routed around the unsynced link
```

```
show route
```

Step 3: Restore everything back to normal (leave IGP sync)

Lesson 4: VPLS Service

Exercise 4.1: Configure basic VPLS service

Configure VPLS service between PE5, PE6 and PE7. Reuse Attachment Circuits from lesson 3 exercises and create a new one to PE 6.

Step 1: Remove EoMPLS configuration from previous exercises

Step 2: Create l2transport interfaces on PE5, PE6 and PE7

```
interface GigabitEthernet0/0/0/2
  l2transport
!
```

Step 3: Create a Bridge domain and attach an AC to it

```
l2vpn
  bridge group E-LAN
  bridge-domain CUSTOMER1
  interface GigabitEthernet0/0/0/2
```

Step 4: Add a VFI and create core pseudowires

Core pseudowires are for the mesh configuration and will obey the split-horizon rule

```
l2vpn
  bridge group E-LAN
  bridge-domain CUSTOMER1
  vfi CUSTOMER1
    neighbor 172.16.0.6 pw-id 123456
    neighbor 172.16.0.7 pw-id 123456
```

Step 5: Verify your solution

```
show l2vpn bridge-domain
```

Exercise 4.2: Configure VPLS service parameters

The amount of MAC addresses is affecting the scalability of the system. Configure MAC address limiting into 1000 MAC addresses and disable unicast flooding if the limit is exceeded

Step 1: Configure MAC address limit

```
l2vpn
  bridge group E-LAN
  bridge-domain CUSTOMER1
  mac
    limit
      maximum 1000
      action no-flood
```

Step 2: Verify your configuration

```
show l2vpn bridge-domain
```

Lesson 5: L3 VPN

Following customer topology will be used throughout these exercises

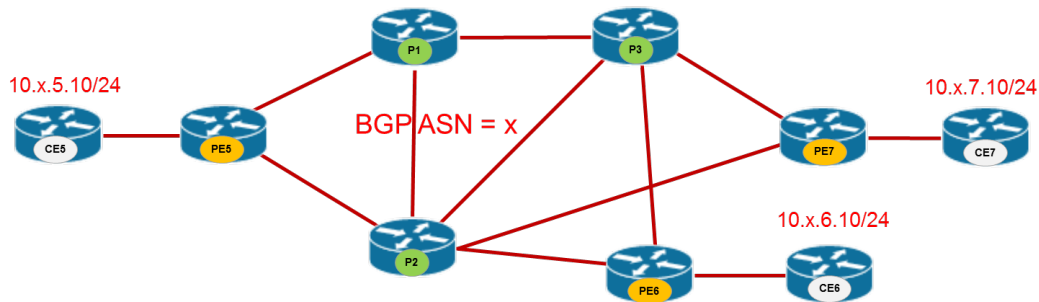


Diagram 5.1 Customer Topology

Exercise 5.1: Configure VRF for customer one

Setup a VRF for customer one. This will create a VRF instance where customer routes are stored. Route targets will be used later in BGP to pass routes between PE routers. Assigning CPE connections to VRF and verify connectivity inside VRF. Replace [POD] with your desktop number from the table 1.

Step 1: Create a VRF in each of the PE routers

This enables Virtual Routing and Forwarding instance for CUSTOMER1

```
vr f CUSTOMER1
 address-family ipv4 unicast
  import route-target
  [POD]:1
  !
  export route-target
  [POD]:1
  !
  !
```

Step 2: Assigning an interface to the VRF and set an IP address

Use your desktop number and PE number in IP address to make it unique in classroom

```
interface GigabitEthernet0/0/0/3
 vr f CUSTOMER1
 ipv4 address 10.[POD].[PE].1 255.255.255.0
 !
```

Step 4: Verify VRF routing table

```
show route vr f CUSTOMER1
```

Step 5: Configure CPE

Set a compatible IP address and default route to the CPE devices connected to the PE

```
ifconfig eth1 10.[POD].[PE].10 netmask 255.255.255.0
 route add default gw 10.[POD].[PE].1
```

Step 6: Verify configuration

From CPE:

```
route -n  
ping
```

From PE:

```
ping vrf CUSTOMER1
```

Exercise 5.2 Create a VPNv4 routing infrastructure

To connect the VRF's together a VPNv4 address-family needs to be routed between the PE routers. Create a full mesh of BGP VPNv4 neighborhoods between the PE routers.

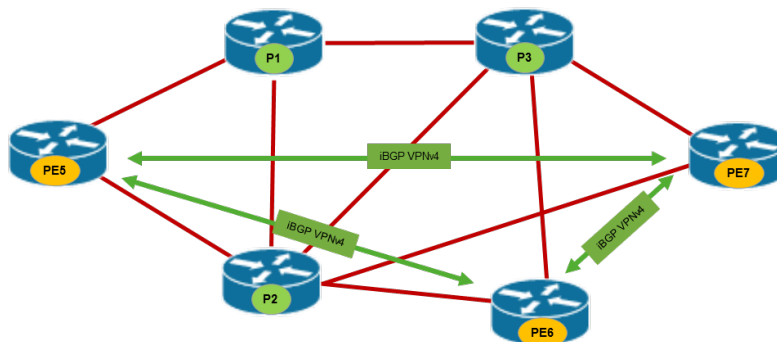


Diagram 5.2 BGP VPNv4 Peers

Step 1: Enable BGP and VPNv4 address-family

Use your desktop number as AS number. Enable Neighbor change logging and hardcode the router-id

```
router bgp [POD]
  bgp router-id 172.16.0.5
  bgp log neighbor changes detail
  address-family vpnv4 unicast
```

Step 2: Configure BGP peers

Peering sessions should use Loopback0 as source (and destination) address for redundancy. Enable VPNv4 address family for the peer for VPN route exchange. Using your own AS number as remote AS will create an iBGP session.

```
router bgp [POD]
  neighbor 172.16.0.6
  remote-as [POD]
  update-source Loopback0
  address-family vpnv4 unicast
```

Step 3: Verify your solution

Make sure all the peers are up and running and full mesh topology is established.

```
show bgp vpnv4 unicast summary
```

Exercise 5.3 Attach VRF to VPNv4 routing

VRF's are included into BGP routing under router bgp configuration mode. Redistribute connected routes to the VPNv4 routing.

Step 1: Add VRF to routing

Use IP address format for RD using PE Loopback0 IP address.

```
router bgp [POD]
  vrf CUSTOMER1
    rd 172.16.0.5:1
    address-family ipv4 unicast
    redistribute connected
```

Step 2: Verify your L3VPN solution

Inspect BGP and routing tables for BGP routes and traceroute from CPE to another. Inspect labels and forwarding tables how traffic is forwarded

From PE:

```
show bgp vpnv4 unicast (vrf CUSTOMER1)
show mpls forwarding
show route vrf CUSTOMER1
ping vrf CUSTOMER1
```

From CPE:

```
ping
traceroute -n
```

Explain why traceroute shows MPLS core addresses

Exercise 5.4 Traceroute optimization

It is not good practice to have core addresses visible to customers. Use IOS-XR features to disable visibility.

Step 1: Disable IP-TTL propagation

```
mpls ip-ttl-propagate disable
```

Step 2: Verify solution

Traceroute from CPE to another

```
traceroute -n
```

Explain why you still see one core address in traceroute

Step 3: Enable VRF address sourcing for ICMP

```
icmp ipv4 source vrf
```

Step 4: Verify solution

Traceroute from CPE to another

```
traceroute -n
```

Lesson 6: Advanced L3 VPN

Exercise 6.1: Configure Customer2 using Hub-and-Spoke topology

Setup a VRF for customer two. Use PE5 as a hub site. This is a challenge lab without any instructions. Use Lo100 for the customer interfaces. Make sure PE6 doesn't see customer routes from PE7 and vice versa. VRF name should be CUSTOMER2 not to cause confusion in later labs.

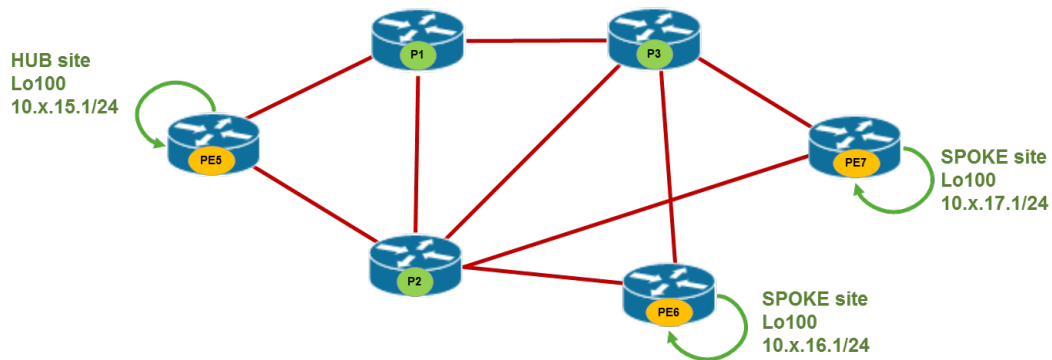


Diagram 6.1 Customer Topology

Exercise 6.2: Configure Customer1 for IPv6 routing

Add VPNv6 address-family to your Customer 1 and enable IPv6 on the interfaces

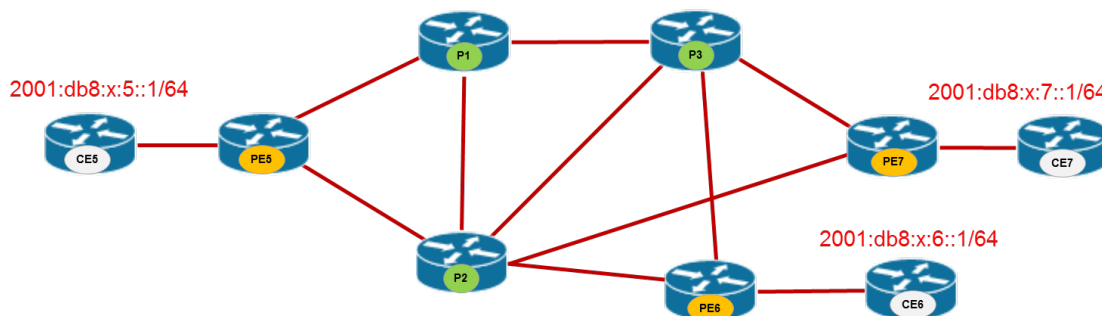


Diagram 6.2 Customer IPv6 Addressing

Step 1: Configure CPE for IPv6 using your POD and PE numbers

```
ifconfig eth1 inet6 add 2001:db8:[POD]:[PE]::10/64
route -A inet6 add default gw 2001:db8:[POD]:[PE]::1
```

Step 2: Configure router interfaces

```
interface GigabitEthernet0/0/0/3
 vrf CUSTOMER1
 ipv6 address 2001:db8:[POD]:[PE]::1/64
```

Step 3: Configure VPNv6 infrastructure

Configure VPNv6 AF for the BGP and its neighbors

```

router bgp [POD]
  address-family vpnv6 unicast
  neighbor 172.16.0.5
    address-family vpnv6 unicast

```

Step 4: configure VRF for IPv6

```

vrf CUSTOMER1
  address-family ipv6 unicast
    import route-target
      [POD]:1
    !
  export route-target
    [POD]:1
  !
!
router bgp [POD]
  vrf CUSTOMER1
    address-family ipv6 unicast
      redistribute connected

```

Step 5: Verify

From PE

```
show route vrf CUSTOMER1 ipv6
```

From CPE

```
ping6
```

```
tracert6 -n
```

Explain why it works even the core does not have IPv6 enabled.

Exercise 6.3: Add an external CPE for customer 1 using static routing

Connect a hardware router from the lab to the virtual lab. Use static routing to access a Lo100 network on CPE. Use network 10.[POD].10.0/24 for the Loopback 100 of the external router, and 10.[POD].11.0 as link addressing. The virtual lab will bridge all the interfaces together, so choose any of the PE routers as terminating point

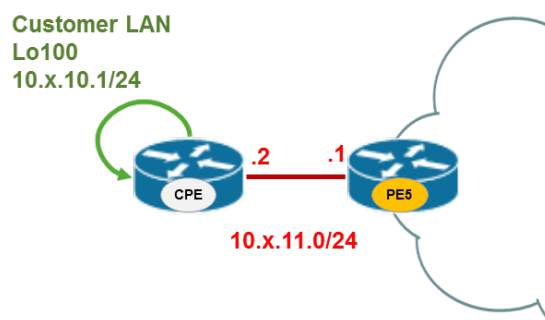


Diagram 6.3 CPE connection and addressing

Step 1: Configure and connect the external CPE (use routers from the lab)

Example configuration below, adjust if needed. Gi0/0/0/2 is the interface towards external interface. Make sure you have configured the workstation networking settings according to the Lab install guide.

```
hostname CPE10
interface Lo100
  ip address 10.[POD].10.1 255.255.255.0
!
interface FastEthernet 0/0
  ip address 10.[POD].11.2 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 10.[POD].11.1
```

Step 2: Configure PE for static routing inside VRF

```
router static
vrf CUSTOMER1
  address-family ipv4 unicast
    10.[POD].10.0/24 10.[POD].11.2
```

Step 3: Configure redistribution of static routes

Redistribute static routes into BGP routing from the PE

```
router bgp [POD]
vrf CUSTOMER1
  address-family ipv4 unicast
    redistribute static
```

Step 4: Verify

Ping from the external CPE to the customer network

Exercise 6.4: Convert external CPE for BGP routing

Enable dynamic routing between external CPE and your network. Use AS65000 for customer.

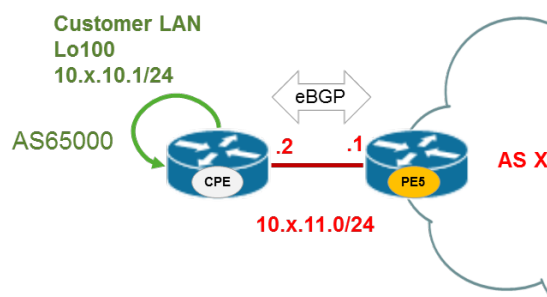


Diagram 6.4 eBGP PE-CE routing

Step 1: Remove all the static routing from both the CPE and the PE

Step 2: Configure BGP in CPE using private AS number

```
router bgp 65000
 neighbor 10.[POD].11.1 remote-as [POD]
 network 10.[POD].10.0 mask 255.255.255.0
```

!

Step 3: Configure Pass all route policy

```
route-policy PASS-ALL
 pass
end-policy
```

Step 4: Configure BGP in PE to peer with CPE

```
router bgp [POD]
 vrf CUSTOMER1
  neighbor 10.[POD].11.2
  remote-as 65000
  address-family ipv4 unicast
    route-policy PASS-ALL in
    route-policy PASS-ALL out
```

!

Step 5: Verify

Ping from the external CPE to the customer network

Exercise 6.5: Configure Inter-AS MPLS VPN

This lab requires two student networks. Find a partner who is in same pace with you and agree on Inter-AS VPN connection. Create Inter-AS connection between routers PE5

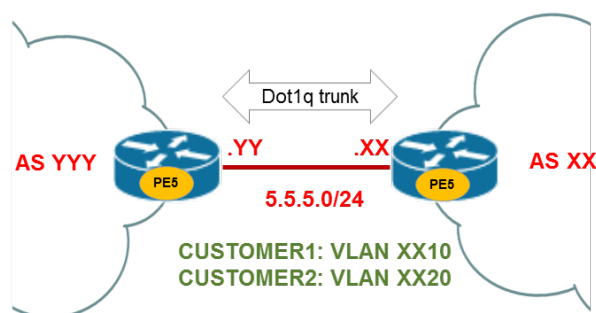


Diagram 6.5 Inter-AS VPN topology

Step 1: Remove the external CPE connection and all associated configuration

Step 2: Connect your networks together.

Remember to use the cross connection cable. Make sure the desired interfaces are bridged together.

Step 3: Configure subinterfaces for peering for both of the customer VRF's

Use 5.5.5.[POD]/24 as link network for every customer, and VLAN XX10 and XX20 for customers 1 and 2 respectively. Peer using PE5. XX in VLAN number can be either of the AS numbers. Agree with your peer which one will be used. Example using AS 23 -> VLAN2310 and VLAN2320.

```
interface GigabitEthernet0/0/0/2.XX10
  encapsulation dot1q XX10
  vrf CUSTOMER1
  ipv4 address 5.5.5.[POD]/24
!
interface GigabitEthernet0/0/0/2.XX20
  encapsulation dot1q XX20
  vrf CUSTOMER2
  ipv4 address 5.5.5.[POD]/24
!
```

Step 4: Configure peering inside the VRF

```
router bgp [POD]
  vrf CUSTOMER1
    neighbor 5.5.5.[neighbors POD]
    remote-as [Neighbors POD]
    address-family ipv4 unicast
  !
  vrf CUSTOMER2
    neighbor 5.5.5.[neighbors POD]
    remote-as [Neighbors POD]
    address-family ipv4 unicast
  !
```

Step 5: Verify you can reach your colleagues networks inside VRF's

```
show route vrf CUSTOMER1
show route vrf CUSTOMER2
```

```
ping
```

```
traceroute
```

Exercise 6.6: Enable IPv6 Inter-AS routing with Customer 1

This is a challenge lab. Figure out how you would connect CUSTOMER1 IPv6 networks together.

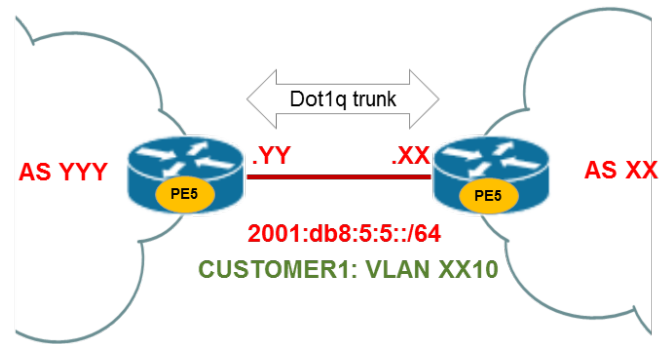


Diagram 6.5 Inter-AS topology for 6VPE

Lesson 7: BGP Policy and Internet Routing

In these exercises you will be connecting to the simulated model internet. These exercises use a network described in the diagram 7.1. Teacher will operate the Internet simulation.

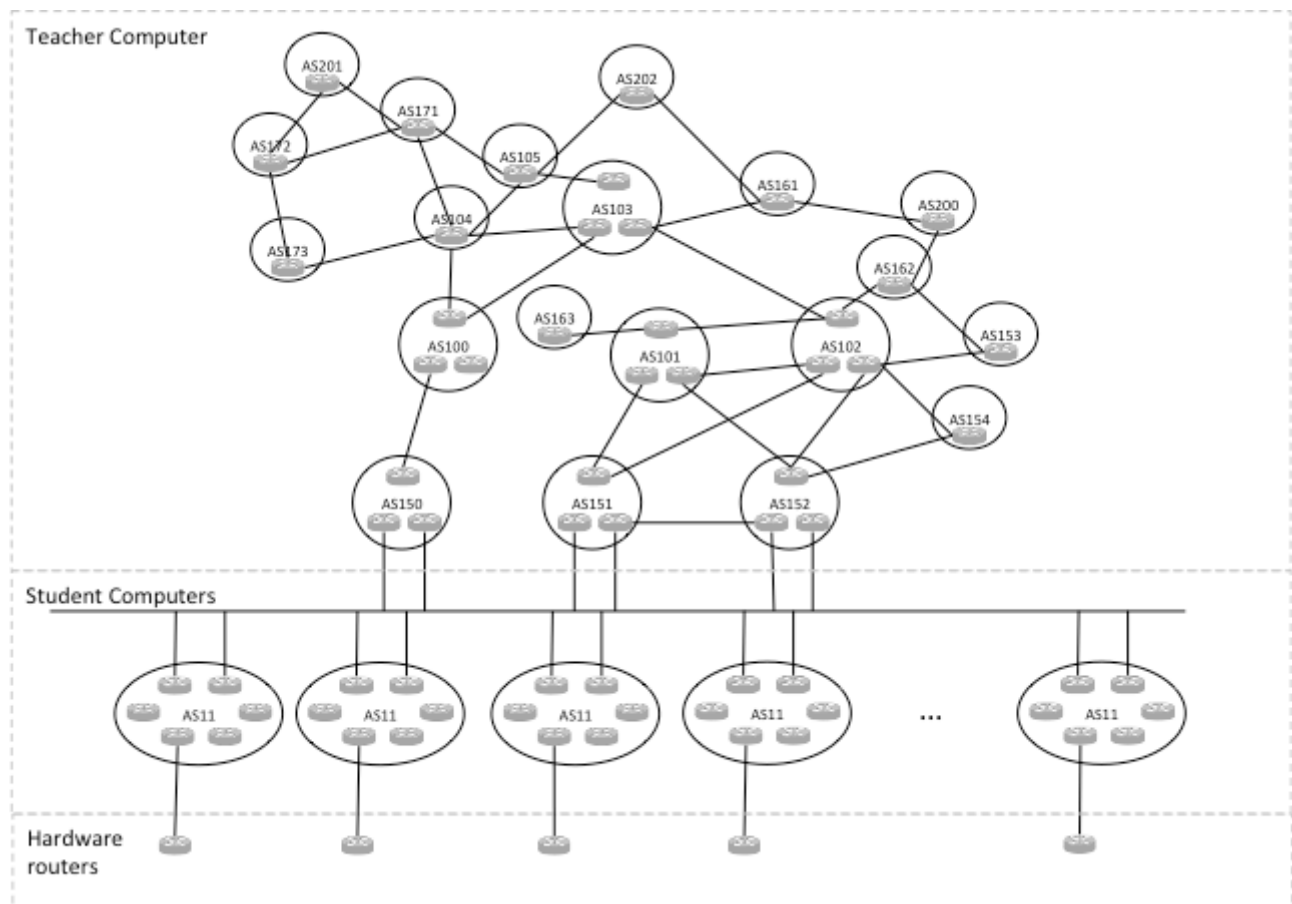


Diagram 7.1: Internet exercise network (Note: May not be an exact topology)

Internet simulation network has many policies implemented and each of the routers has a web page where the policy is described. These web pages can be accessed using ASN.0.0.RN, where ASN is the Autonomous system number, and RN the router number (1-3)

Exercise 7.1: Create MPLS VPN for Internet use

Use your prior knowledge to build an Internet VPN in your network. Set the VRF in big mode to support large Internet routing table.

Step 1: Create MPLS VPN between PE routers

Use examples from previous classes

Step 2: Set the VRF to big mode

```
vrf INTERNET
mode big
```

Step 3: Boot up an XP workstation and attach it to PE6 using LAN segment

Exercise 7.2: Connect to Internet

You have acquired an ASN, IP Prefix and a membership to IXP. Your ASN number is your Desktop number and IP Prefix X.0.0.0/8 (where X is your desktop number). You have made contracts with three service providers. Diagram 7.2 illustrates how the service providers are connected.

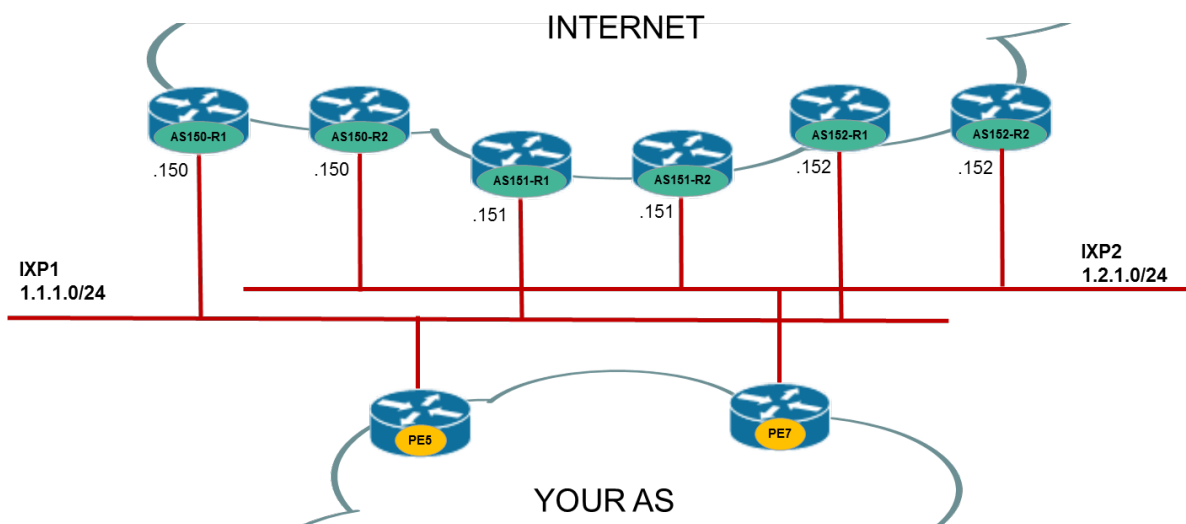


Diagram 7.2. Internet connection

Step 1: Connect your physical cable to assigned IXP switch

Step 2: Configure IP connectivity

Assign an IP address to PE5 and PE7 Gi0/0/0/2 interfaces. Connect PE5 to IXP1 (IP 1.1.1.X/24) and PE7 to IXP2 (1.2.1.X/24).

Step 3: Verify IP connectivity

From PE5

```
ping vrf INTERNET 1.1.1.150
```

From PE7

```
ping vrf INTERNET 1.2.1.150
```

Step 4: Create a basic route-policy

The purpose of the policy is to only allow locally originated routes to be advertised. For future preparation, create a separate route policy for each of the service providers. Accept all routes from the provider.

```
route-policy AS150-OUT
  if as-path is-local then
    pass
  else
    drop
  endif
end-policy
```

```
route-policy AS150-IN
  pass
end-policy
```

Step 5: Configure a static Null0 route for your prefix

Use methods learned in previous lessons how to create a static route inside a VRF

Step 6: Configure peering

Redistribute static routes. Set the BGP router-id to public address X.0.0.N, where X is your desktop number and N is the router number.

```
router bgp X
vrf INTERNET
  bgp router-id X.0.0.N
  address-family ipv4 unicast
    redistribute static
  neighbor 1.1.1.150
    remote-as 150
  address-family ipv4 unicast
    send-community ebgp
    route-policy AS150-IN in
    route-policy AS151-OUT out
```

Step 7: Configure access

Assign a prefix to PE6 and configure it to Gi0/0/0/2. The choice is yours inside your assigned /8. Configure a static IP address into XP workstation and make sure it can reach the PE6. Use PE6 as default gateway

Step 8: Verify

This is a large configuration task, but if you managed to pull it off, you should be able to browse to 200.10.0.10 with your XP workstation! If not, start troubleshooting.

Exercise 7.3: Make peering agreements with your colleagues over the IXP's

Make sure you won't be accepting other than routes originated from your peers. Test this behavior with your partner

Exercise 7.4: Create a routing policy

Create a routing policy with following guidelines. Progress one step at a time and try to figure out how to implement the policy. This is a challenge lab and no detailed instructions are provided.

1. Upstream traffic towards AS200 should always go through AS150
2. Downstream traffic should prefer AS151 (check from AS201 routers)
3. AS152 should not be used other than 152 originated routes. Use communities AS152 provides to establish this behavior.

Lesson 8: Segment Routing

In this exercise you will be exploring a future development to MPLS transport layer operation. IOS-XRv still lacks functions on implementing path control, but is still able to do basic segment routing. This lab should give you an idea how simple a MPLS core can be.

Step 1: Verify you have working MPLS service as baseline

```
show route vrf CUSTOMER1
```

```
ping vrf CUSTOMER1
```

Step 2: Remove all LDP configuration

```
no mpls ldp
```

You should see your baseline MPLS service break

Step 3: Remove all LDP configuration

Configure segment routing under IS-IS in each of the routers, use your router number as prefix-sid index

```
router isis SPNET
 address-family ipv4 unicast
   segment-routing mpls
 !
interface Loopback0
 address-family ipv4 unicast
   prefix-sid index [ROUTER]
 !
!
```

Step 4: Verify your baseline service is working again

```
show route vrf CUSTOMER1
```

```
ping vrf CUSTOMER1
```

Step 5: Inspect the MPLS forwarding plane

Look at the labels from starting 16000. These are the assigned prefix segment id's, or node segments. These labels can be used to forward traffic to particular node. And labels starting from 24000 are adjacency labels, which in turn can be used to force traffic through particular link. Adjacency labels are only locally significant.

```
show mpls forwarding
```

```
show isis database verbose
```




Step 6: Look how simple configuration is at P-routers

Simplicity means easy operations and high reliability. By using IS-IS for label distribution you already avoid LDP sync issues and have much more simpler approach. Admire your work!

Submitted answers: 6



Questions: 10

1. (1) I found the overall course interesting

- strongly disagree (1): 0
- disagree (2): 0
- neutral (3):  1 (16.67 %)
- agree (4):  2 (33.33 %)
- strongly agree (5):  3 (50.00 %)



Average: 4.33

2. (1) The virtual lab was reliable and worked well during the course

- strongly disagree (1): 0
- disagree (2): 0
- neutral (3):  2 (33.33 %)
- agree (4):  4 (66.67 %)
- strongly agree (5): 0


Average: 3.67

3. (1) The virtual lab was easy to use

- strongly disagree (1): 0
- disagree (2):  1 (16.67 %)
- neutral (3): 0
- agree (4):  5 (83.33 %)
- strongly agree (5): 0




Average: 3.67

4. (1) Having the whole network under my control aided my learning compared to teamwork with HW lab

- strongly disagree (1): 0
- disagree (2):  2 (33.33 %)
- neutral (3):  1 (16.67 %)
- agree (4):  1 (16.67 %)
- strongly agree (5):  2 (33.33 %)



Average: 3.50

5. (1) I gained good understanding about service provider networks

- strongly disagree (1): 0
- disagree (2):  1 (16.67 %)
- neutral (3):  2 (33.33 %)
- agree (4):  3 (50.00 %)
- strongly agree (5): 0




Average: 3.33

6. (1) Working with Internet simulation gave me deeper understanding about the Internet routing

- strongly disagree (1): 0
- disagree (2): 0
- neutral (3):  1 (16.67 %)
- agree (4):  3 (50.00 %)




Average: 4.17

7. (1) The course was too difficult for me

- strongly disagree (1):  1 (16.67 %)
- disagree (2): 0
- neutral (3):  2 (33.33 %)
- agree (4):  3 (50.00 %)
- strongly agree (5): 0

Average: 3.17

8. (1) The lecturer presentation skills were good

- strongly disagree (1): 0
- disagree (2):  1 (16.67 %)
- neutral (3): 0
- agree (4):  4 (66.67 %)
- strongly agree (5):  1 (16.67 %)

Average: 3.83

9. () Overall feedback of the course

- Opetus oli aika paljon suorannaista kerrontaa, eikä aina saanut kiinni missä mentiin. Onneksi sai tehdä paljon harjoituksia, joilla oppi paljon. Yleiskuva jäi hyväksi aiheesta.
- Omasta näkökulmasta omaan oppimiseen liittyen: Olin ehtinyt jo unohtamaan joitain reititysmenetelmiin liittyviä asioita ihan perustasolta, sillä opintokokonaisuudet kestävät pitkään ja välillä tuli oltua aivan liikaa pois oppitunneilta muiden vähäpätöisimpien menojen takia. Oma oppimistani heikensi hieman kurssin vieraskielisyys, koska jotkin termit olivat kylläkin tuntemustasolla hallussa mutta niiden syvällisempi merkitys jäi hämäräksi. Jonkin verran auttoi aiempi perehtyminen IPsec-protokollapinoon, jolloin kokonaisuustasolla oli helpompi omaksua MPLS:n liittyviä toimintoja.

Omasta näkökulmasta opetusmenetelmiin liittyen: Kerrankin oli hienoa päästä harjoittelemaan kokonaisuutta itsenäisesti. Vaikka kyseessä olikin vain kuuden virtuaalilaitteen kokonaisuus provider-verkossa + cpe:t, niin labroja tehdessä meni välillä pahasti sekaisin etenemisestä. Toisilta opiskelijoilta ei saanut apua kovinkaan paljoa koska jotkut olivat "pihalla" vaikka saivatkin tehtävät tehtyä tai eivät olleet edenneet samaa vauhtia. Ryhmätyöskentelyä tuli oikeastaan vasta myöhemmin ja ainoa asia, jota olisin kaivannut oli opettajan antama suora tuki. Vihjeitä kyllä sateli, mutta joissain kohdin iski turhautuminen kun vihjeistä huolimatta ongelmaa tai tehtävää ei saanut toteutettua kokonaan. Mielestäni kurssi tuki liikaa siihen, että opiskelijoilla olisi kaikista tekniikoista olemassa olevaa substanssiosaamista vaikka näin monen kohdalla ei ole.

Yleisellä tasolla kurssi oli mielestäni onnistunut vaikka opiskelijoiden henkilökohtaisella tasolla tavoitteita ei olisi saavutettukkaan. Kurssi tulee olemaan parhaimmistossa kunhan lisätään opettajan ohjausta käytännöntehtäviin liittyen ja opetusaineistoon linkitetään cison:n sivulta löytyviin materiaaleihin suoraan termeistä (linkki PDF:stä sivustolle, viite missä kappaleessa mikäli ei olemassa olevaa hyperlinkkiankkuria)

- Topic was interesting and hopefully useful in future.
- Muuten hyvä, mutta lähiopetus tuntien vähäinen määrä (alkoi vasta helmikuussa) vaikutti kokeessa erittäin negatiivisesti. Jonkun näköinen

kun asiaa tuli paljon.

- Kurssissa ei varsinaisesti mitään vikaa, mutta omaa opiskelumotivaatiota valitettavasti laski se, että kurssi oli englanniksi. Tämä ei tietenkään ole opettajan syy, mutta vaikutti tuloksiini.

10. () Feedback of the virtual environment and the Internet simulation

- Virtuaaliympäristö toimi hyvin alun vaikeuksien jälkeen, itselläni ei juuri ongelmia ollut. Simulaatiot toimivat omasta mielestäni erinomaisesti, mutta oman oppimisen kannalta olisi ollut hyvä jos virtuaaliympäristöön olisi päässyt käsiksi joko omalla koneella (jolla ei ole riittävästi muistia tämän pyörittämiseen) tai tuntien ulkopuolella (luokka usein varattu eikä ympäristö pyöri palvelimella, johon pääsisi kiinni etäyhteydellä).
- Yllättävän hyvin lähti toimimaan, vaikka alussa oli vaikeutta. Oli ihan mielenkiintoinen työympäristö. Labrat olivat käteviä ja ei tarvinnut leikkiä kaapeleiden kanssa. Tämä taas tarkoitti, että tarvitsee paremman hahmotuskyvyn asioista.
- Yleisesti erittäin hyvin järjestelty. Voisi omasta mielestä ottaa käyttöön muissakin kursseissa samankaltainen järjestely
- After the complications in the start, the virtual environment worked really well. It was pretty easy to use and it gave a wider picture of service provider networks.
- Virtuaaliympäristö toimi hyvin. Koneet alkoivat olla tosin hieman alimitoitettuja.
- Loppua kohden homma alkoi sujumaan paremmin, kun ympäristö tuli tutuksi.