Report

Of

Six Week Industrial Training

On

**NETWORK CONFIGURATION WITH OSPF**

at

NIIT

**Submitted By**

ABHISHEK KUMAR

Branch (CE)

Semester : 5th Sem

Roll No : 11501172



**Department of Computer Engineering**

**Punjabi University, Patiala,2017**

***PREFACE***

There is a famous saying “The theory without practical is lame and practical without theory is blind.”

This project has been composed with the aim of covering a part of B-TECH (Computer Science Engineering) syllabus as prescribed by Punjabi University, Patiala. A lot of effort has been made to make this project report interesting and a learning experience for the leader. The report has been explained with the help of diagrams and figures. The running project has presented through a CD representation. The subject matter has been compiled in a simple, illustrative and lucid manner.

My Project is on “NETWORK CONFIGURATION WITH OSPF” which is based on COMPUTER NETWORKING and its connectivity with MYSQL server to store Data bases.

Through this project I have describe so many skills and techniques about Computer Network & how to use them. I have also describe more concepts of NETWORK DEVICES and how we could use it in CONFIGURATION OF NETWORK and other applications.

***Acknowledgement***

**I hereby declare that the project work entire “NETWORK CONFIGURATION WITH OSPF” is an authentic record**

**of my own work carried out at NIIT, PATIALA as requirements of six weeks project (Computer Science department),**

**ENGINEERING WING, PUNJABI UNIVERSITY, PATIALA, under the guidance of MR. PRABHJOT SINGH**

**BAL during 1 June to 20 July, 2017.**

**Signature of Student**

**ABHISHEK KUMAR(11501172)**

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| SR. No. | DESCRIPTION | PAGE NO. |
| 01. | PREFACE | i |
| 02. | ACKNOWLEDGEMENT | ii |
| 03. | CERTIFICATE | iii |
| 04. | COMPANY'S PROFILE (Not more than 2 Pages) | 1-2 |
| 05. | INTRODUCTION TO TECHNOLOGY USED IN PROJECT | 3-5 |
| 06. | PROJECT | 6-37 |
| 07. | SCREENSHOTS | 38-42 |
| 08. | BIBLIOGRAPHY/ REFRENCES | 43 |

**COMPANY’S PROFILES**

Overview

Established in 1981, NIIT Limited, a global leader in Skills and Talent Development, offers multi-disciplinary learning management and training delivery solutions to corporations, institutions, and individuals in over 40 countries. The company ranks among the world’s leading training companies owing to its vast, yet comprehensive array of talent development programs.

With a strong focus on assuming leadership role in the Digital Learning World and to further accelerate NIIT's growth and profitability, the company has charted a focused business strategy to address the Digital Transformation needs for individuals and corporate customers by offering training and consulting to help them re-invent themselves & their organisations.

The [Training.com](https://www.training.com/) learning platform, is a pioneering initiative for advanced career programs, which are delivered live by industry experts in an immersive and interactive online mode, combining instructor-led classrooms with the convenience of accessing the training sessions from anywhere. The programs are targeted at working professionals who want to take their careers to the next level by enhancing their knowledge of the latest concepts through programs offered from premier institutes like IIM Calcutta, DMI Ireland and edX.

Other key offerings include [StackRoute](http://www.stackroute.in/) which focuses on creating Digital Innovators by building an elite breed of Full-stack programmers; [DigiNXT](http://www.niitdiginxt.com/) which addresses the urgent need to help India's IT Services industry source fresh staff as well as retrain 4 million of their existing staff into Digital Developers; and finally [NIIT.tv](http://www.niit.tv/) that aims to create Digital Workers and Digital Citizens by bringing skilling from NIIT classrooms to every digitally connected Indian, for free, at any time and place of their choice to train the masses to evolve their skills and participate productively in the future digital world.

As a company, NIIT has three main lines of businesses namely – Corporate Learning Group, Skills and Careers Group, and MindChampion Learning Systems Limited – which will lead the transition of the organisation into the Digital Learning World.

NIIT's Corporate Learning Group (CLG) offers comprehensive suite of Managed Training Services that includes custom Curriculum Design and Content Development, Learning Administration, Learning Delivery, Strategic Sourcing, Learning Technology, and Advisory Services to leading companies in North America, Europe, Asia, and Oceania.

NIIT's Skills and Careers Group (SNC) delivers a diverse range of learning and talent development programs to millions of individual and corporate learners in areas including Banking, Finance & Insurance, Retail Sales Enablement, Management Education, Multi-Sectoral Vocational Skills, Digital Media Marketing, and programs in digital transformation technologies

As NIIT's wholly owned subsidiary for its K-12 school learning initiative - [MindChampionLearning Systems Limited (MLSL)](http://www.niitnguru.com/), is providing technology based learning to around 2,000 private schools across India, reaching out to more than a million students. The futuristic NIIT nGuru range of learning solutions for schools comprises Interactive Classrooms with digital content, technology-driven Math Lab, IT Wizard programs and Quick School - an Education Resource Planning software.

Recent Awards and Acknowledgments

• NIIT has been recognized as ‘India’s Most Trusted Training Brand’ 2017 by Trust Research Advisory (TRA) for the 5th consecutive year

• NIIT has also been featured as the 'Most Respected Education Company’ – 2016 by leading financial magazine, Business World

• NIIT bagged the 'Best Innovation Brand award’ 2016 in the Education sector at ASSOCHAM National Brand Summit

• [NIIT.tv](http://www.niit.tv/) - a disruptive innovation by NIIT Limited has been awarded the ‘Best online education platform’ at the Indian Education Awards 2016 organized by Franchise India, India’s leading Franchising publication.

• [NIIT.tv](http://www.niit.tv/) has been acknowledged for Education Technology (Institutions) by Indo-American Education Summit 2016

• NIIT Limited won the ‘Innovation and Technology’ award under the Special category at the Franchise Awards & Star Retailer Awards 2016 by Franchise India

• [NIIT Imperia](http://www.niitimperia.com/) won the ‘Best training to Working Professionals’ category at the BBC Knowledge Education Leadership Awards 2016

• [Training.com](https://www.training.com/) won ‘eEducation Services of the Year – Online educational services award 2017’ by Franchise India

• NIIT USA has been awarded ‘CLO LearningElite Gold Award 2016’

• NIIT USA received ‘8 Brandon Hall Excellence in Learning Awards 2016’ jointly with customers

• NIIT USA has been ranked among the ‘Top 20 Training Outsourcing Companies 2017’ by TrainingIndustry.com for the 10th consecutive year

• NIIT UK has been awarded the status of ‘Accredited Learning Provider’ by Learning and Performance Institute (LPI), UK

• NIIT USA has been ranked among the ‘Top 20 Companies in Content Development 2017’ by TrainingIndustry.com for the seventh consecutive year

• NIIT USA has been ranked among the ‘Top 20 Companies in Gamification 2016’ by TrainingIndustry.com for the third consecutive year.

**TECHNOLOGY USED IN PROJECT**

Software Requirements

• CISCO PACKET TRACER

• Windows 7,8,10

• GNS3

Hardware Requirements

* **FOR PACKET TRACER**

**• Hard Disk – 1GB.**

**• RAM – 2GB.**

**• Processor – Dual Core Minimum.**

**• Mouse.**

**• Keyboard.**

**• Monitor**

**• Printer.**

**PACKET TRACER**

Packet Tracer is a [cross-platform](https://en.wikipedia.org/wiki/Cross-platform) visual [simulation](https://en.wikipedia.org/wiki/Simulation) tool designed by [Cisco Systems](https://en.wikipedia.org/wiki/Cisco_Systems) that allows users to create [network topologies](https://en.wikipedia.org/wiki/Network_topologies) and imitate modern [computernetworks](https://en.wikipedia.org/wiki/Computer_networks). The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface. Packet Tracer makes use of a [drag and drop](https://en.wikipedia.org/wiki/Drag_and_drop) user interface, allowing users to add and remove simulated network devices as they see fit. The software is mainly focused towards Certified Cisco Network Associate Academy students as an educational tool for helping them learn fundamental CCNA concepts. Previously students they had enrolled in a CCNA Academy program could freely download and use the tool free of charge for educational use.[[1]](https://en.wikipedia.org/wiki/Packet_Tracer#cite_note-jar-1) Since August 2017 with version 7.1 is free to everyone.[[2]](https://en.wikipedia.org/wiki/Packet_Tracer#cite_note-2)

Overview[[edit](https://en.wikipedia.org/w/index.php?title=Packet_Tracer&action=edit&section=1)]

Packet Tracer can be run on iOS, Linux and Microsoft Windows. A similar Android app is also available. Packet Tracer allows users to create simulated network topologies by dragging and dropping routers, [Application Layerprotocols](https://en.wikipedia.org/wiki/Application_Layer), as well as basic routing with [RIP](https://en.wikipedia.org/wiki/Routing_Information_Protocol), [OSPF](https://en.wikipedia.org/wiki/OSPF), [EIGRP](https://en.wikipedia.org/wiki/EIGRP), [BDP](https://en.wikipedia.org/wiki/Bandwidth-delay_product), to the extents required by the current [CCNA](https://en.wikipedia.org/wiki/CCNA) curriculum. As of version 5.3, Packet Tracer also supports the [Border Gateway Protocol](https://en.wikipedia.org/wiki/Border_Gateway_Protocol).[[3]](https://en.wikipedia.org/wiki/Packet_Tracer#cite_note-BGP-3)

In addition to simulating certain aspects of [computernetworks](https://en.wikipedia.org/wiki/Computer_networks), Packet Tracer can also be used for collaboration. As of Packet Tracer 5.0, Packet Tracer supports a multi-user system that enables multiple users to connect multiple topologies together over a [computer network](https://en.wikipedia.org/wiki/Computer_network).[[4]](https://en.wikipedia.org/wiki/Packet_Tracer#cite_note-Development_of_a_simulated_Internet_for_education-4) Packet Tracer also allows instructors to create activities that students have to complete.[[1]](https://en.wikipedia.org/wiki/Packet_Tracer#cite_note-jar-1) Packet Tracer is often used in educational settings as a learning aid.[[5]](https://en.wikipedia.org/wiki/Packet_Tracer#cite_note-designPatterns-5)[[6]](https://en.wikipedia.org/wiki/Packet_Tracer#cite_note-teaching-6) Cisco Systems claims that Packet Tracer is useful for network experimentation.[[7]](https://en.wikipedia.org/wiki/Packet_Tracer#cite_note-datasheet-7)

Role in Education[[edit](https://en.wikipedia.org/w/index.php?title=Packet_Tracer&action=edit&section=2)]

Packet Tracer, which is often not feasible with physical hardware, due to costs.[[5]](https://en.wikipedia.org/wiki/Packet_Tracer#cite_note-designPatterns-5) Packet Tracer is commonly used by CCNA Academy students, since it is available to them for free.[[1]](https://en.wikipedia.org/wiki/Packet_Tracer#cite_note-jar-1) However, due to functional limitations, it is intended by CISCO to be used only as a learning aid, not a replacement for Cisco [routers](https://en.wikipedia.org/wiki/Router_(computing)) and [switches](https://en.wikipedia.org/wiki/Network_switch).[[7]](https://en.wikipedia.org/wiki/Packet_Tracer#cite_note-datasheet-7) The application itself only has a small number of features found within the actual hardware running a current [Cisco IOS](https://en.wikipedia.org/wiki/Cisco_IOS) version. Thus, Packet Tracer is unsuitable for modelling production networks. It has a limited command set, meaning it is not possible to practice all of the IOS commands that might be required.[[8]](https://en.wikipedia.org/wiki/Packet_Tracer#cite_note-visual-8)

# Packet Tracer can be useful for understanding [abstract](https://en.wikipedia.org/wiki/Abstraction)[networkingconcepts](https://en.wikipedia.org/w/index.php?title=Networking_concepts&action=edit&redlink=1), such as the [Enhanced Interior Gateway Routing Protocol](https://en.wikipedia.org/wiki/EIGRP) by animating these elements in a [visual form](https://en.wikipedia.org/wiki/Information_visualization).[[5]](https://en.wikipedia.org/wiki/Packet_Tracer#cite_note-designPatterns-5)[[8]](https://en.wikipedia.org/wiki/Packet_Tracer#cite_note-visual-8) Packet Tracer is also useful in education by providing additional components, including an authoring system, network protocol simulation .

# PROJECT

# **General Networking:**

A network is simply a group of two or more Personal Computers linked together. Many types of networks exist, but the most common types of networks are Local-Area Networks (LANs), and Wide-Area Networks (WANs).

In a LAN, computers are connected together within a "local" area (for example, an office or home). In a WAN, computers are further apart and are connected via telephone/communication lines, radio waves or other means of connection.

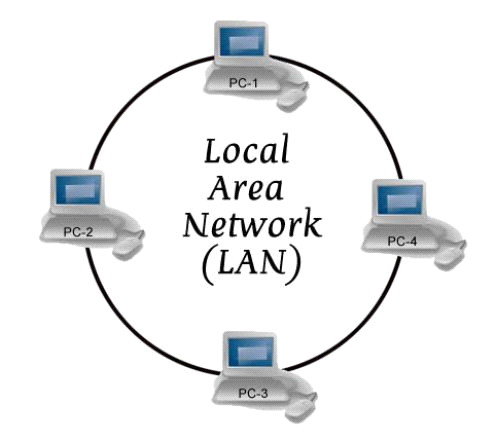
**Benefits of Networking:**

1. **File Sharing**
2. **Printer / Peripheral sharing**
3. **Internet connection sharing**
4. **Multi-player Games**
5. **Internet telephone service.**

**Types of Networks** :

1. **LAN - Local Area Network**

LAN connects networking devices with in short spam of area, i.e. small offices, home, internet cafes etc. LAN uses TCP/IP network protocol for communication between computers. It is often but not always implemented as a single IP subnet. Since LAN is operated in short area so It can be control and administrate by single person or organization.

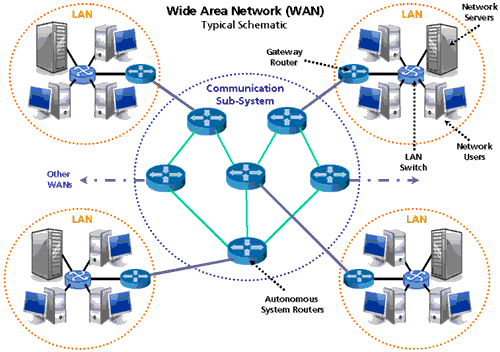


1. **MAN - Metropolitan Area Network**

This kind of network is not mostly used but it has its own importance for some government bodies and organizations on larger scale. MAN, metropolitan area network falls in middle of LAN and WAN, It covers large span of physical area than LAN but smaller than WAN, such as a city.

1. **WAN - Wide Area Network**

As “word” Wide implies, WAN, wide area network cover large distance for communication between computers. The Internet itself is the biggest example of Wide area network, WAN, which is covering the entire earth. WAN is distributed collection of geographically LANs. A network connecting device router connects LANs to WANs. WAN used network protocols like ATM, X.25, and Frame Relay for long distance connectivity.



**Networking devices**:

**Hubs &Repeaters**:Hubs and repeaters are basically the same, so we will be using the term "Hub" to keep things simple. Hubs are common today in every network. They are the cheapest way to connect two or more computers together. Hubs are also known as *Repeaters* and work on the first layer of the [OSI model](http://www.firewall.cx/networking-topics/the-osi-model.html). They are said to work on the first layer because of the function they perform. They don't read the data frames at all (like switches and routers do), they only make sure the frame is repeated out on each port and that's about it.



**SWITCH**:

It is an advanced version over a Hub. The main benefit of switch is Unicast. Data packets are transmitted only to the target computer instead of all. Switch maintains a table called MIT (Mac Information Table.) which is generated as soon as we turn on the switch, which acts like an index table and easy the process of finding the networked system. MIT contains the port no, IP address and MAC address.



**MAC(Media Access Control):**

It is an address burnt in the NIC by themanufacturer. MAC address is of 48 bits in the farm of Hexadecimal.Every NIC has its own unique MAC address. MAC address determines the physical location of a system.

**ROUTER**:

Routers are very common today in every network area, this is mainly because every network these days connect to some other network, whether it's the Internet or some other remote site. Routers get their name from what they do.... which is route data from one network to another.

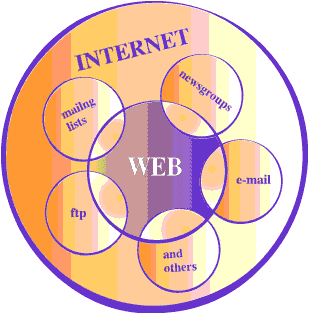
the other unecessary traffic is filtered (blocked), thus saving you valuable bandwidth and money.For example, if you had a company which had an office in Sydney and another one in Melbourne, then to connect the two you would use a leased line to which you would connect a router at each end. Any traffic which needs to travel from one site to another will be routed via the routers, while all



**CCNA**  
**(CISCO CERTIFIED NETWORK ASSOCIATE)**

**Protocols:**

1. Set of rules for exchanging messages between computers.
2. Without a protocol, two devices may be connected but not communicating.
3. A protocol defines what is communicated, how it is communicated and when it is communicated.
4. A commonly issued protocol known as TCP/IP which supports every kind of protocol.
5. Other protocols are:- HTTP,SMTP,FTP,PPP,POP3,NFS,TELNET,DHCP,DNS,RIS,RRAS,RIP,IGRP,EIGRP,OSPF,BGP,TFTP.



|  |
| --- |
| In the networking and communications area, a protocol is the formal specification that defines the procedures that must be followed when transmitting or receiving data. Protocols define the format, timing, sequence, and error checking used on the network. |
| In plain english, the above means that if you have 2 or more devices e.g computers which want to communicate, then they need a common "Protocol" which is a set of rules that guide the computers on how and when to talk to each other. |

**IP Addressing:**

Class Range N/w bits Host bits Subnet mask Total IP Valid IP

A 1 – 126 8 24 255.0.0.0 16777216 16777214

B 128 – 191 16 16 255.255.0.0 65536 65534

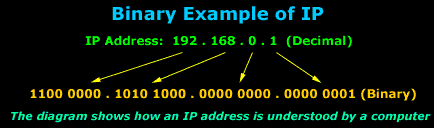
C 192 – 223 24 8 255.255.255.0 256 254

D 224 – 239 it is reserved for multicast.

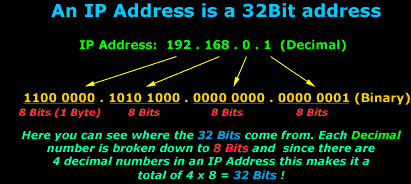
E 240 – 255 it is reserved for research/scientific use.

1. Identification of a device with in a network is called IP addressing.
2. IP address is a 32-bit address. It is divided into four octets. Each octet has 8 bits.
3. It has two parts one is network address and second is host address.
4. Subnet mask is also 32-bit address, which tell us how many bits are used for network and how many bits are used for host address.
5. In Subnet mask Network bits are always 1 and Host bits are always 0.

The picture below gives an example of how a computer understands an IP Address:



The above example shows an IP address in decimal notation, which we understand more easily, this IP Address - 192.168.0.1 is then converted to Binary, which is what the computer understands and you can see how big the number gets ! It's easier for us to remember 4 different numbers than 32 zeros or ones.



So to sum up all the above, we now know what Binary notation is, what a Bit, Byte and KByte is and how Binary relates to an IP Address which is usally represented in its Decimal notation.

**What is Subnetting :**

When we Subnet a network, we basically split it into smaller networks. For example, when a set of IP Addresses is given to a company, e.g 254 they might want to "break" (the correct term is "partition") that one network into smaller ones, one for each department. This way, their Technical department and Management department can each have a small network of their own. By subnetting the network we can partition it to as many smaller networks as we need and this also helps reduce traffic and hides the complexity of the network.

By default, all type of Classes (A, B and C) have a subnet mask, we call it the "Default Subnet mask". You need to have one because:

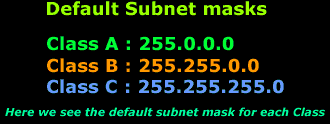
1) All computers need the subnet mask field filled when configuring IP

2) You need to set some logical boundaries in your network

3) You should at least enter the default subnet mask for the Class you're using

In the previous pages I spoke about IP Classes, Network IDs and Host IDs, the fact is that the Subnet mask is what determines the Network ID and Host ID portion of an IP Address.

The table below shows clearly the subnetmask that applies for each network Class.



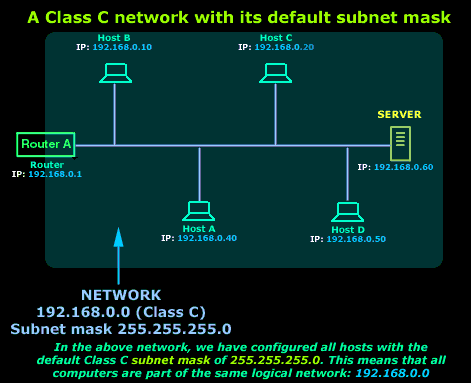
When dealing with subnet masks in the real world, we are free in most cases to use any type of subnet mask in order to meet our needs. If for example we require one network which can contain up to 254 computers, then a Class C network with its default subnet mask will do fine, but if we need more, then we might consider a Class B network with its default subnet mask.

Note that the default subnet masks have been set by the IEEE committee, the same guys that set and approve the different standards and protocols.

**Understanding the concept:**

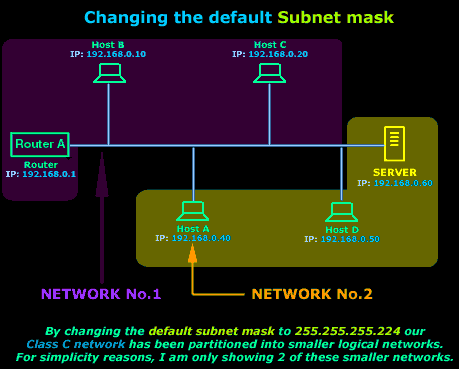
Let's stop here for one moment and have a look at what I mean by partitioning one network into smaller ones by using different subnet masks.

The picture below shows our example network (192.168.0.0). All computers here have been configured with the default Class C subnet mask (255.255.255.0):



Because of the subnet mask we used, all these computers are part of the one network marked in blue. This also means that any one of these hosts (computers, router and server) can communicate with each other.

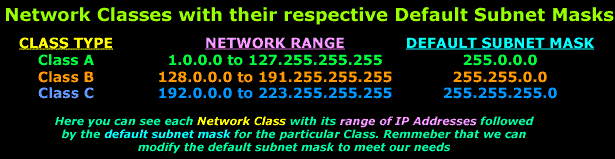
If we now wanted to partition this network into smaller segments, then we would need to change the subnet mask appropriately so we can get the desired result. Let's say we needed to change the subnet mask from 255.255.255.0 to 255.255.255.224 on each configured host.The picture below shows us how the computers will see the network once the subnet mask has changed:



In reality, we have just created 8 networks from the one large (blue) network we had, but I am keeping things simple for now and showing only 2 of these smaller networks because I want you to understand the concept of subnetting and see how important the subnet mask is.

**Default Subnet masks of each Class:**

The picture below shows our 3 Network Classes with their respective default subnet mask:



**ROUTER:**

1. Router is hardware manageable device, which is used to communicate two different networks.
2. Router performs routing and path determination.
3. It does not perform broadcast information.
4. Routers can regenerate signals, concentrate multiple connections and manage data transfer.
5. They can also connect to a WAN, which allows them to connect LANs that are separated by great distances.

Routers are very common today in every network area, this is mainly because every network these days connect to some other network, whether it's the Internet or some other remote site. Routers get their name from what they do.... which is route data from one network to another.

For example, if you had a company which had an office in Sydney and another one in Melbourne, then to connect the two you would use a leased line to which you would connect a router at each end. Any traffic which needs to travel from one site to another will be routed via the routers, while all the other unecessary traffic is filtered (blocked), thus saving you valuable bandwidth and money.

There are two type of routers: 1) Hardware routers 2) Software routers.

**Hardware routers** are dedicated hardware that run special software created by their vendors to give them the routing capabilities, plus a whole lot more functions. Hardware routers a most common amongst companies as they are faster and more reliable. In the earlier days, hardware routers would start from a couple of hundred dollars, however their prices today are extremely low for cheaper-brand models.

The picture below shows a new-generation cisco 2900 series router that offers a lot more than simple routing capabilities:



**Software routers** perform similar tasks as the above hardware routers (route data), but they don't come in small flashy boxes. A software router could be Windows , Linux or Novell NetWare server. All network servers have built-in routing capabilities.

**Cisco Router Basics:**

Cisco has a number of different routers, amongst them are the popular 880 series, 2900 series and 3900 series.   
  
Below are a pictures few of the routers mentioned (880 & 2900 series):



The basic components of any Cisco router are :

1) Interfaces

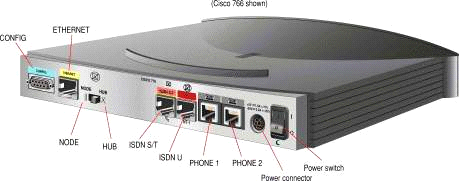
2) The Processor (CPU)

3) Internetwork Operating System (IOS)

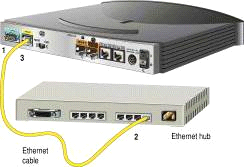
**Interfaces**

These allow us to use the router ! The interfaces are the various serial ports or ethernet ports which we use to connect the router to our LAN. There are a number of different interfaces but we are going to hit the basic stuff only.

In the picture below you can see the back view of a Cisco router, you can clearly see the various interfaces it has:



we have an Ethernet interface that connects to a device in your LAN, usually a hub or a computer. If connecting to a Hub uplink port, then you set the small switch to "Hub", but if connecting to a PC, you need to set it to "Node". This switch will simply convert the cable from a straight through (hub) to a x-over (Node):



**Cisco Router Modes:**

One of the greatest perhaps features of Cisco routers is that most commands used in the IOS software they run on, are identical across multiple platforms. For example, commands for configuring a gigabit ethernet interface on a Cisco 2821 are exactly the same when configuring a gigabit ethernet interface on a Cisco 3945. This feature makes working with pretty much any Cisco model, a extremely comfortable and pleasant experience.

**Setup Mode:**

The setup mode is a step-by-step process which helps you configure basic aspects of the router. When using this setup mode, you actually have 2 options:

1) Basic Management Setup, which configures only enough connectivity for management to the system.

2) Extended Setup, which allows you to configure some global parameters and interfaces.

It should be noted that when you are prompted to enter a value at the console prompt, whatever is between the square brackets [ ] is considered to be a default value. In other words, if you hit enter without entering anything, the value in those brackets will be set for the specific question.

I'll try to keep this as simple and straightforward as possible.

Cisco routers have different configuration modes (depending on the router model), and by this I mean there are different modes in which different aspects of the router can be configured.

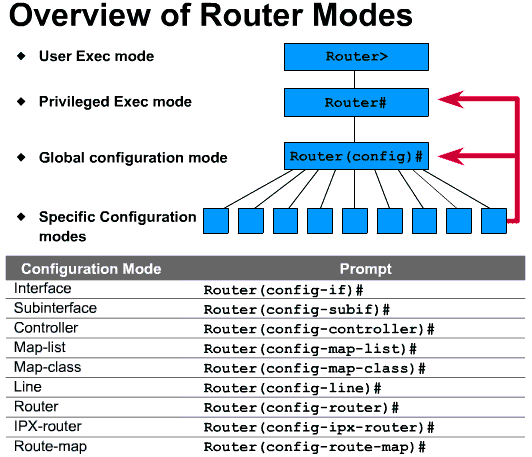
These are:

1) User Exec Mode (>)

2) Privileged Mode (#) which has as a subset, the Global Configuration mode -

To be able to get into either User Exec or Privileged mode, you will most likely need a password. This password is set during the initial configuration of the router or later on. Once in Privileged Mode, you can then enter Global Configuration Mode (password not needed to enter this mode) to then further configure interfaces, routing protocols, access lists and more.

The picture below shows you a quick view of the modes. Notice the red arrow, it's pointing towards the Global Configuration Mode and Privileged mode meaning that some of the specific configuration modes can be entered from Global Configuration Mode and other from Privileged mode:



**Configuring IP, Mask and Enabling the Interface**:

1. Router#configure terminal
2. Router(config)#interface <type><no>
3. Router(config-if)#ip address <ip><mask>
4. Router(config-if)#no shutdown
5. Router(config-if)#exit

**IP Routing:**

When we want to connect two or more networks using different n/w addresses then we have to use IP Routing technique. The router will be used to perform routing between the networks. A router will perform following functions for routing.

1. Path determination
2. Packet forwarding

**(1) Path determination**

The process of obtaining path in routing table is called path determination. There are three different methods to which router can learn path.

i) Automatic detection of directly connected n/w.

ii) Static & Default routing

iii) Dynamic routing

**(2) Packet forwarding**

It is a process that is by default enable in router. The router will perform packet forwarding only if route is available in the routing table.

**Static Routing:**

In this routing, we have to use IP route commands through which we can specify routes for different networks. The administrator will analyze whole internetwork topology and then specify the route for each n/w that is not directly connected to the router.

**Steps to perform static routing**

(1) Create a list of all n/w present in internetwork.

(2) Remove the n/w address from list, which is directly connected to n/w.

(3) Specify each route for each routing n/w by using IP route command.

Router (config)#ip route <destination n/w><mask><next hop ip>

**Next hop IP**: It is the IP address of neighbor router that is directly connected our router.

**Static Routing Example: -**

Router#confter

Router (config) #ip route 10.0.0.0 255.0.0.0 192.168.10.2

**Advantages of static routing**

(1) Fast and efficient.

(2) More control over selected path.

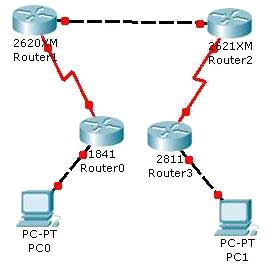
(3) Less overhead for router.

**Disadvantages of static routing**

(1) More overheads on administrator.

(2) Load balancing is not easily possible.

(3) In case of topology change routing table has to be change manually.



**Dynamic Routing:**

In dynamic routing, we will enable a routing protocol on router. This protocol will send its routing information to the neighbor router. The neighbors will analyze the information and write new routes to the routing table.

The routers will pass routing information receive from one router to other router also. If there are more than one path available then routes are compared and best path is selected. Some examples of dynamic protocol are: -

RIP, IGRP, EIGRP, OSPF

**Configuring RIP:**

Router#confter

Router (config) #router rip

Router(config-router\network <own net address>

Router(config-router)#network <own net address>

--------------

--------------

Router(config-router)#exit

**Configuring IGRP:**

Router(config)#router igrp<as no>(1 – 65535)

Router(config-router)#network <net address>

Router(config-router)#network <net address>

Router(config-router)#exit

**Configuring EIGRP:**

Router(config)#router eigrp<as no>

Router(config-router)#network <net addr.>

Router(config-router)#network <net addr.>

Router(config-router)#exit

**Commands to configure OSPF:**

Router#conf t

Router(config)#router ospf<process no>

Router(config-router)#network <net address><wild mask> area <area id>

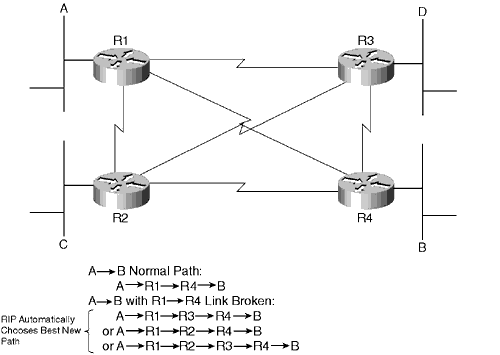
Router(config-router)#network <net address><wild mask> area <area id>

Router(config-router)#exit

**Wild Mask –** Complement of subnet mask

**Example** 255.255.0.0

0.0.255.255



**Access Control List:**

ACL are the basic security feature that is required in any network to control the flow of traffic. Most of time our network may have servers and clients for which traffic control is required.We can also use ACL to classify the traffic.

**Types of ACL based on Feature**: -

(1) Standard ACL

(2) Extended ACL

**Types of ACL based on Order of rules**: -

(1) Deny, permit

(2) Permit, deny

**Applying ACL on interface**

Router#confter

Router(config)#interface <type><no>

Router(config-if)#ip access-group <ACL no.><in|out>

Router(config-if)#exit

e.g

Router(config)#access-list 25 permit 192.168.10.32 0.0.0.31

Router(config)#access-list 25 permit 192.168.10.64 0.0.0.3

Router(config)#access-list 25 permit 192.168.10.68

Router(config)#access-list 25 permit 192.168.10.69

Router(config)#access-list 25 permit 192.168.10.70

Router(config)#interface serial 0

Router(config-if)#ip access-group 25 out

**IP Standard ACL (Named):**

In Numbered ACL editing feature is not available that is we are not able to delete single rule from the ACL. In Named ACL editing feature is available.

Router#configter

Router(config)#ip access-list standard <name>

Router(config-std-nacl)#<deny|permit><source>

Router(config-std-nacl)#exit

Router#confter

Router(config)#ip access-list standard abc

Router(config-std-nacl)#deny 172.16.0.16

Router(config-std-nacl)#deny 172.16.0.17

Router(config-std-nacl)#deny 172.16.0.18

Router(config-std-nacl)#permit any

Router(config-std-nacl)#exit

**IP Extended ACL (Numbered**):

Extended ACL are advanced ACL. ACL, which can control traffic flow on the basis of five different parameters that are: -

(i) Source address

(ii) Destination address

(iii) Source port

(iv) Destination port

(v) Protocol (layer 3/layer 4)

**The syntax to create Extended ACL:**

Router#confter

Router(config)#access-list <no><deny|permit><protocol><source> [<s.port>]

<destination> [<d.port>]

router(config)#exit

**To display ACL:**

Router#show access-lists or

Router#show access-list <no>

**To display ACL applied on interface:**

Router#showip interface

Router#showip interface <type><no>

Router#showip interface Ethernet 0

**Network Address Translation (NAT):**

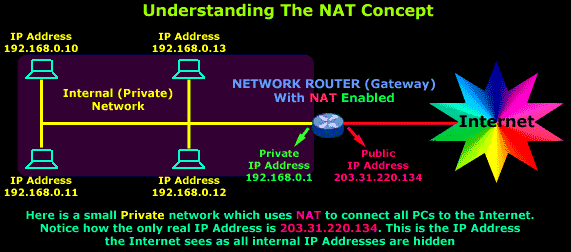
 It allows a single device to act as an Internet gateway for internal LAN clients by translating the clients' internal network IP Addresses into the IP Address on the NAT-enabled gateway device.

In other words, NAT runs on the device that's connected to the Internet and hides the rest of your network from the public, thus making your whole network appear as one device (or computer, if you like) to the rest of the world.

NAT is transparent to your network, meaning all internal network devices are not required to be reconfigured in order to access the Internet. All that's required is to let your network devices know that the NAT device is the default gateway to the Internet.

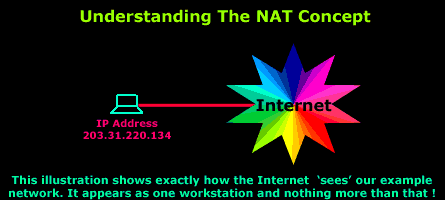
NAT is secure since it hides your network from the Internet. All communications from your private network are handled by the NAT device, which will ensure all the appropriate translations are performed and provide a flawless connection between your devices and the Internet.

The diagram below illustrates this:



As you can see, we have a simple network of 4 hosts (computers) and one router that connects this network to the Internet. All hosts in our network have a private Class C IP Address, including the router's private interface (192.168.0.1), while the public interface that's connected to the Internet has a real IP Address (203.31.220.134).

If you're having trouble understanding, the following diagram shows how the Internet would see the above setup:



Such configurations will allow the Internet to access an internal webserver or ftp server you might have, without directly compromising your network security. Of course special actions need to be taken to ensure that your visitors are restricted to the resources you want and that's where the firewall comes into the picture.

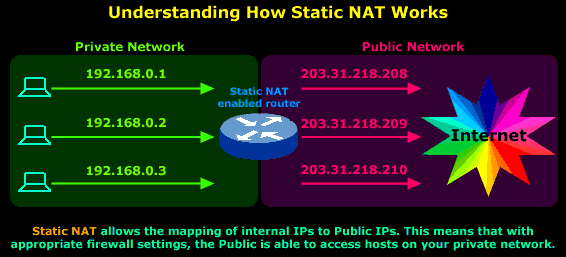
**Types Of NAT:**

1. **Static NAT**
2. **Dynamic NAT**
3. **Overload NAT.**

**What exactly does Static NAT do ?**

Static NAT allows the mapping of public IP Addresses to hosts inside the internal network. In simple english, this means you can have a computer on your private network that exists on the Internet with its own real IP.

The diagram below has been designed to help you understand exactly how Static NAT works:



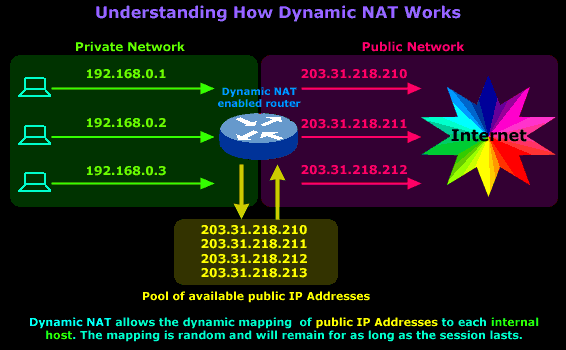
In this diagram you can see that we have our private network connected to the Internet via our router, which has been configured for Static NAT mode. In this mode each private host has a single public IP Address mapped to it,e.g private host 192.168.0.1 has the public IP Address 203.31.218.208 mapped to it. Therefore any packets generated by 192.168.0.1 that need to be routed to the Internet will have their source IP field replaced with IP Address 203.31.218.208.

**Dynamic NAT:**

With Dynamic NAT, we also map our internal IP Addresses to real public IP Addresses, but *the mapping is not static*, meaning that for each session our internal hosts communicate with the Internet, their public IP Addresses remain the same, but are likely to change. These IPs are taken from a pool of public IP Addresses that have been reserved by our ISP for our public network.

With Dynamic NAT, translations don't exist in the NAT table until the router receives traffic that requires translation. Dynamic translations have a timeout period after which they are purged from the translation table, thus making them available for other internal hosts.

The diagram below illustrates the way Dynamic NAT works:



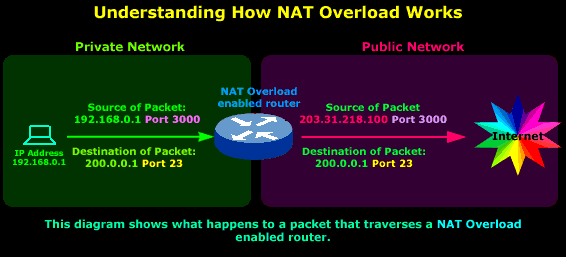
The diagram above is our example network and shows our router, which is configured to perform Dynamic NAT for the network. We requested 4 public IPs from our ISP (203.31.218.210 to 203.31.218.213), which will be dynamically mapped by our router to our internal hosts. In this particular session our workstation, with IP Address 192.168.0.1, sends a request to the Internet and is assigned the public IP address 203.31.218.210. This mapping between the workstation's private and public IP Address will remain until the session finishes.

**NAT Overload:**

NAT Overload is a mix of Static & Dynamic NAT with a few enhancements thrown in (PAT- Port Address Translation) to make it work the way we need. By now you understand how both Static & Dynamic NAT work so we won't get into the details again. NAT Overload takes a Static or Dynamic IP Address that is bound to the public interface of the gateway (this could be a PC, router or firewall appliance) and allows all PCs within the private network to access the Internet.

If you find yourself wondering how this is possible with one only IP Address, you will be happy to find that the answer lies within PAT.

The diagram below shows you how a single session is handled by a NAT Overload enabled device:



So we have a host on a private network, its IP Address is 192.168.0.1 and it's sending a packet to the Internet, more specifically to IP Address 200.0.0.1, which we're assuming is a server. The Port, which is 23, tells us that it's trying to telnet to 200.0.0.1, since this is the default port telnet uses.

**Configuring NAT**

Router#conf t

Router(config)#int serial 0

Router(config-if)#ipnat outside

Router(config-if)#int eth 0

Router(config-if)#ipnat inside

Router(config-if)#exit

Router(config)#ipnat inside source static 172.16.0.7 200.1.1.3

Router(config)#ipnat inside source static tcp 172.16.0.5 80 200.1.1.4 80

Router(config)#ipnat inside source static udp 172.16.0.6 53 200.1.1.4 53

Router(config)#access-list 30 deny 172.16.0.5

Router(config)#access-list 30 deny 172.16.0.6

Router(config)#access-list 30 deny 172.16.0.7

Router(config)#access-list 30 permit any

Router(config)#ipnat pool abc 200.1.1.8 200.1.1.12 netmask 255.255.255.240

Router(config)#ipnat inside source list 30 pool abc overload

**The VLAN Concept - Introduction to VLANs:**

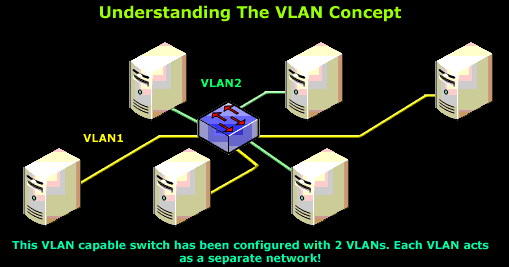
All the above problems, and a lot more, can be forgotten with the creation of VLANs...well, to some extent at least.

As most of you are already aware, in order to create (and work with) VLANs, you need a layer 2 switch that supports them. A lot of people new to the networking field bring the misconception that it's a matter of simply installing additional software on the clients or switch, in order to "enable" VLANs throughout the network - this is totally incorrect!

Because VLANs involve millions of mathematical calculations, they require special hardware which is built into the switch and your switch must therefore support VLANs at the time of purchase, otherwise you will not be able to create VLANs on it!

Each VLAN created on a switch is a separate network. This means that a separate broadcast domain is created for each VLAN that exists. Network broadcasts, by default, are filtered from all ports on a switch that are not members of the same VLAN and this is why VLANs are very common in today's large network as they help isolate network segments between each other.

To help create the visual picture on how VLANs differentiate from switches, consider the following diagram:



What we have here is a small network with 6 workstations attached to a VLAN capable switch. The switch has been programmed with 2 VLANs, VLAN1 and VLAN2 respectfully, and 3 workstations have been assigned to each VLAN.

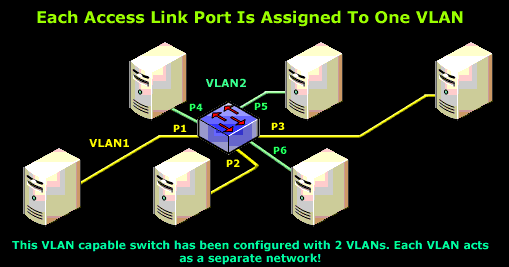
**VLAN Links – Interfaces:**

When inside the world of VLANs there are two types of interfaces, or if you like, links. These links allow us to connect multiple switches together or just simple network devices e.gPC, that will access the VLAN network. Depending on their configuration, they are called Access Links, or Trunk Links.

**Access Links:**

We must note that the 'Access Link' term describes a configured port - this means that the ports can be configured as the second type of VLAN links - Trunk Links. What we are showing here is what's usually configured as an Access Link port in 95% of all switches. Depending on your needs, you might require to configure the first port (top left corner) as a Trunk Link, in which case, it is obviously not called a Access Link port anymore, but a Trunk Link!

When configuring ports on a switch to act as Access Links, we usually configure only one VLAN per port, that is, the VLAN our device will be allowed to access. If you recall the diagram below which was also present during the introduction of the VLAN concept, you'll see that each PC is assigned to a specific port:



In this case, each of the 6 ports used have been configured for a specific VLAN. Ports 1, 2 and 3 have been assigned to VLAN 1 while ports 4, 5 and 6 to VLAN 2.

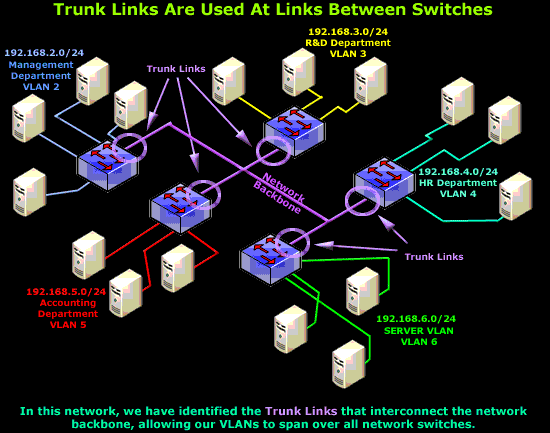
In the above diagram, this translates to allowing only VLAN 1 traffic in and out of ports 1, 2 and 3, while ports 4, 5 and 6 will carry VLAN 2 traffic. As you would remember, these two VLANs do not exchange any traffic between each other, unless we are using a layer 3 switch (or router) and we have explicitly configured the switch to route traffic between the two VLANs.

**Trunk Links:**

What we've seen so far is a switch port configured to carry only one VLAN, that is, an Access Link port. There is, however, one more type of port configuration which we mentioned in the introductory section on this page - the Trunk Link.

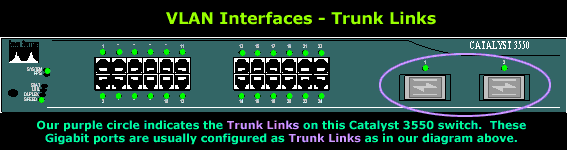
A Trunk Link, or 'Trunk' is a port configured to carry packets for any VLAN. These type of ports are usually found in connections between switches. These links require the ability to carry packets from all available VLANs because VLANs span over multiple switches.

The diagram below shows multiple switches connected throughout a network and the Trunk Links are marked in purple colour to help you identify them:



As you can see in our diagram, our switches connect to the network backbone via the Trunk Links. This allows all VLANs created in our network to propagate throughout the whole network. Now in the unlikely event of Trunk Link failure on one of our switches, the devices connected to that switch's ports would be isolated from the rest of the network, allowing only ports on that switch, belonging to the same VLAN, to communicate with each other.

So now that we have an idea of what Trunk Links are and their purpose, let's take a look at an actual switch to identify a possible Trunk Link:



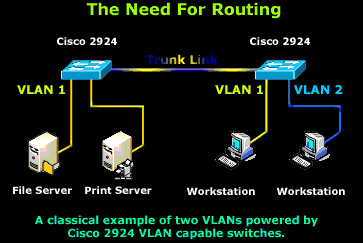
**InterVLAN Routing - Routing between VLAN Networks:**

**The Need For Routing:**

Each network has it's own needs, though whether it's a large or small network, internal routing, in most cases, is essential - if not critical. The ability to segment your network by creating VLANs, thus reducing network broadcasts and increasing your security, is a tactic used by most engineers. Popular setups include a separate broadcast domain for critical services such as File Servers, Print servers, Domain Controllers e.t.c, serving your users non-stop.

The issue here is how can users from one VLAN (broadcast domain), use services offered by another VLAN?

Thankfully there's an answer to every problem and in this case, its VLAN routing:

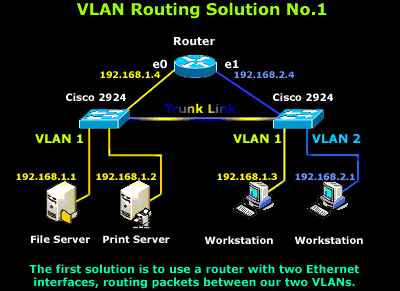


The above diagram is a very simple but effective example to help you get the idea. Two VLANs consisting of two servers and workstations of which one workstation has been placed along with the servers in VLAN 1, while the second workstation is placed in VLAN 2.

In this scenario, both workstations require access to the File and Print servers, making it a very simple task for the workstation residing in VLAN 1, but obviously not for our workstation in VLAN 2.

**VLAN Routing Solution No.1: Using A Router With 2 Ethernet Interfaces**

A few years ago, this was one of the preferred and fastest methods to route packets between VLANs. The setup is quite simple and involves a Cisco router e.g 2500 series with two Ethernet interfaces as shown in the diagram, connecting to both VLANs with an appropriate IP Address assigned to each interface. IP Routing is of course enabled on the router and we also have the option of applying access lists in the case where we need to restrict network access between our VLANs.

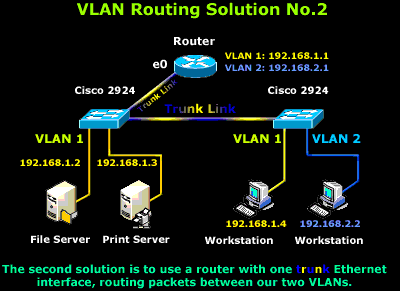


In addition, each host (servers and workstations) must either use the router's interface connected to their network as a 'default gateway' or a route entry must be created to ensure they use the router as a gateway to the other VLAN/Network. This scenario is however expensive to implement because we require a dedicated router to router packets between our VLANs, and is also limited from an expandability prospective.

In the case where there are more than two VLANs, additional Ethernet interfaces will be required, so basically, the idea here is that you need one Ethernet interface on your router that will connect to each VLAN.

**VLAN Routing Solution No.2: Using A Router With One Ethernet (Trunk) Interface**

This solution is certainly fancier but requires, as you would have already guessed, a router that supports trunk links. With this kind of setup, the trunk link is created, using of course the same type of encapsulation the switches use (ISL or 802.1q), and enabling IP routing on the router side. This method of InterVLAN routing is also known as 'Router on a Stick'.

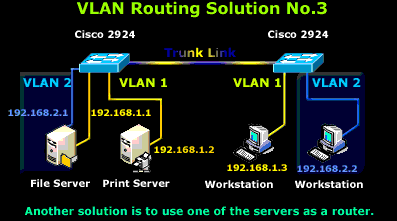


The downside here is that not many engineers will sacrifice a router just for routing between VLANs when there are many cheaper alternatives, as you will soon find out. Nevertheless, despite the high cost and dedicated hardware, it's still a valid and workable solution and depending on your needs and available equipment, it might be just what you're looking for!

Closing this scenario, the router will need to be configured with two virtual interfaces, one for each VLAN, with the appropriate IP Address assigned to each one so routing can be performed.

**VLAN Routing Solution No.3: Using A Server With Two Network Cards**

We would call this option a "Classic Solution". What we basically do, is configure one of the servers to perform the routing between the two VLANs, reducing the overal cost as no dedicated equipment is required.

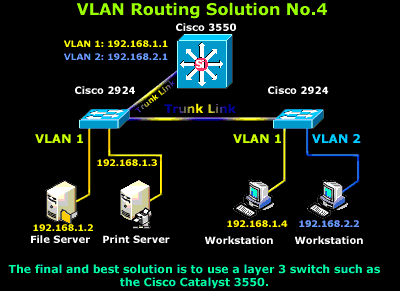


In order for the server to perform the routing, it requires two network cards - one for each VLAN and the appropriate IP Addresses assigned, therefore we have configured one with IP Addresses 192.168.1.1 and the other with 192.168.2.1. Once this phase is complete, all we need to do is enable IP routing on the server and we're done.

Lastly, each workstation must use the server as either a gateway, or a route entry should be created so they know how to get to the other network. As you see, there's nothing special about this configuration, it's simple, cheap and it gets the job done.

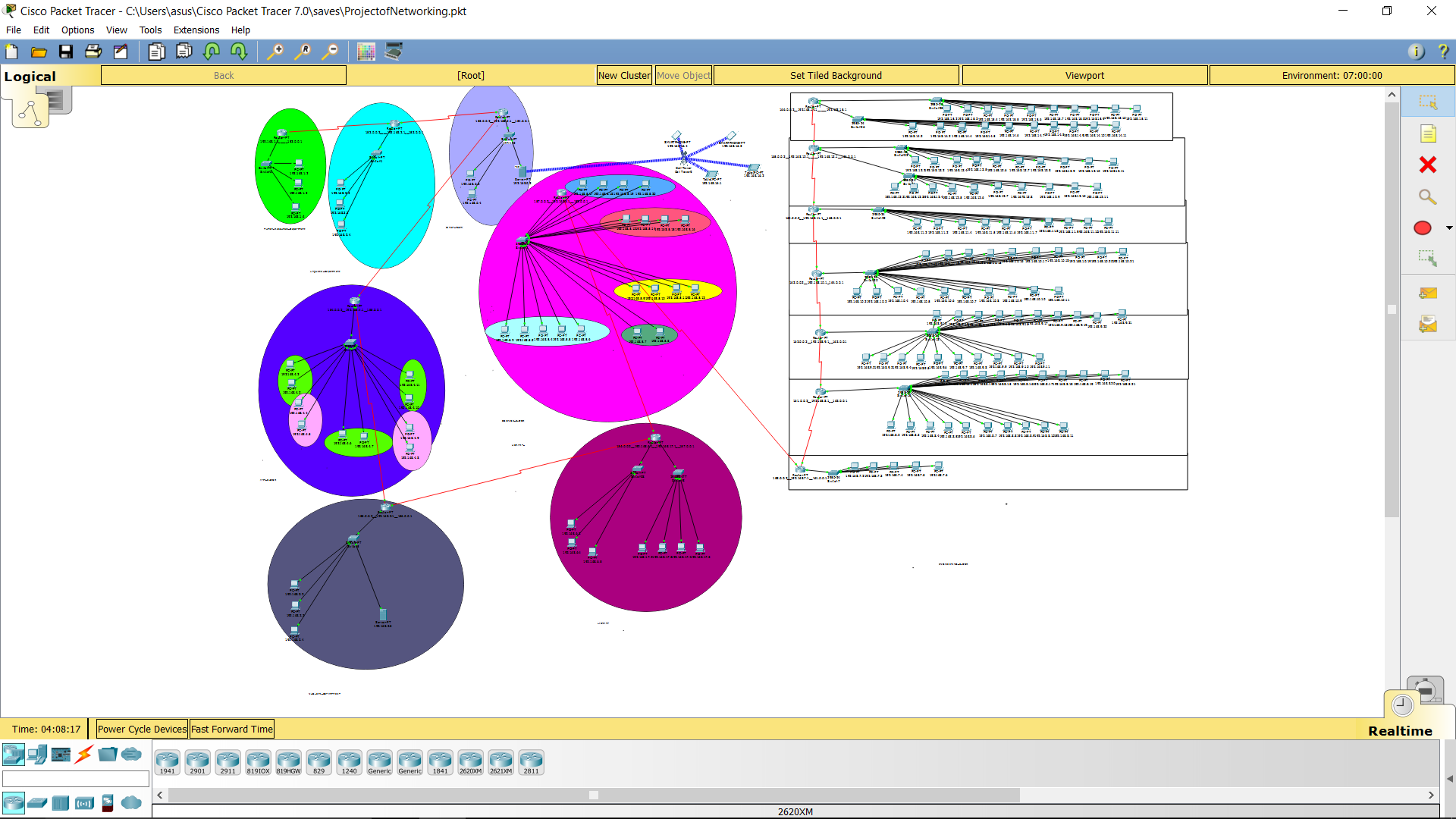
**VLAN Routing Solution No.4: InterVLAN Routing**

And at last....InterVLAN routing! This is without a doubt the best VLAN routing solution out of all of the above. InterVLAN routing makes use of the latest i0n technology switches ensuring a super fast, reliable, and acceptable cost routing solution.

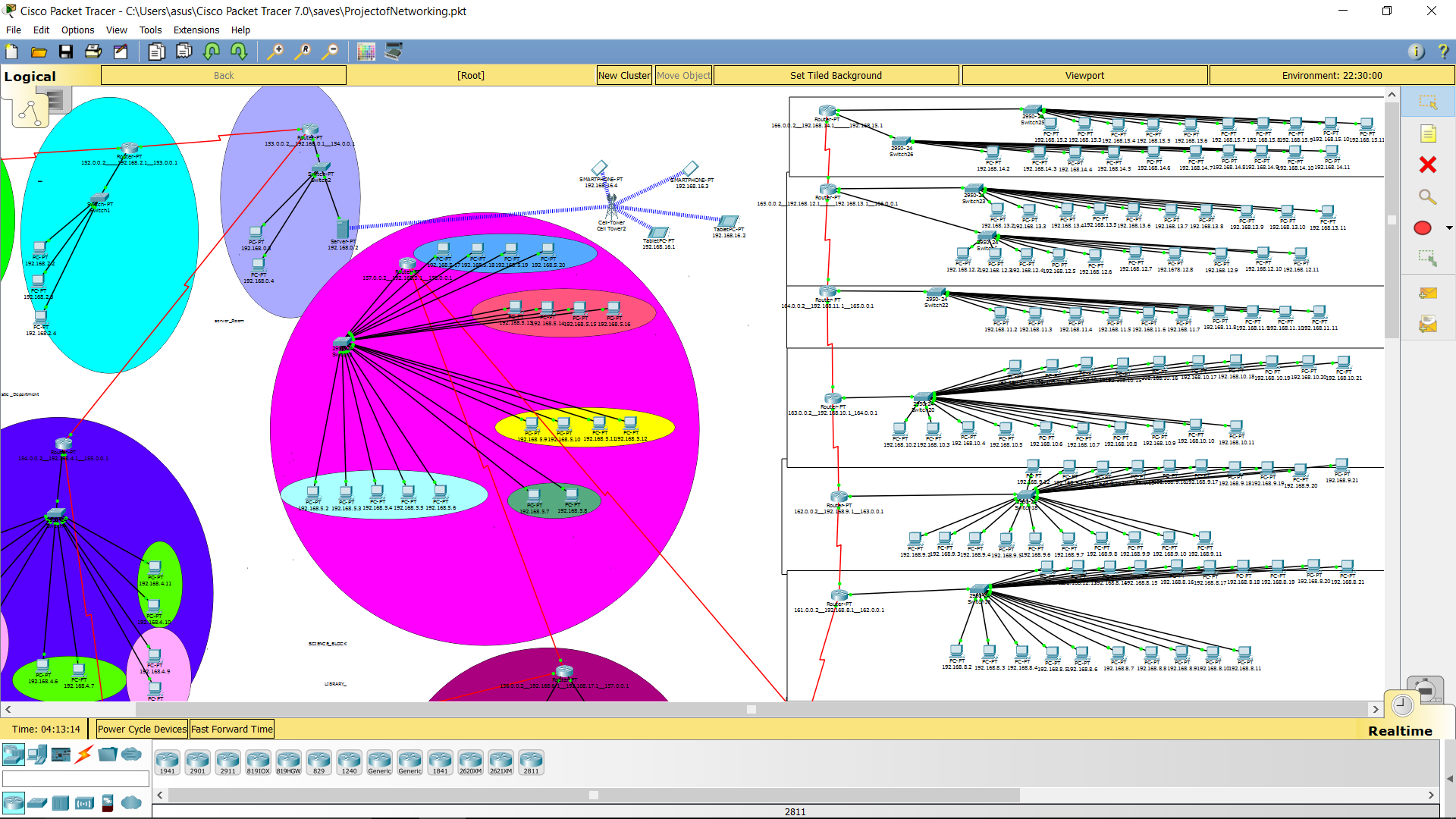


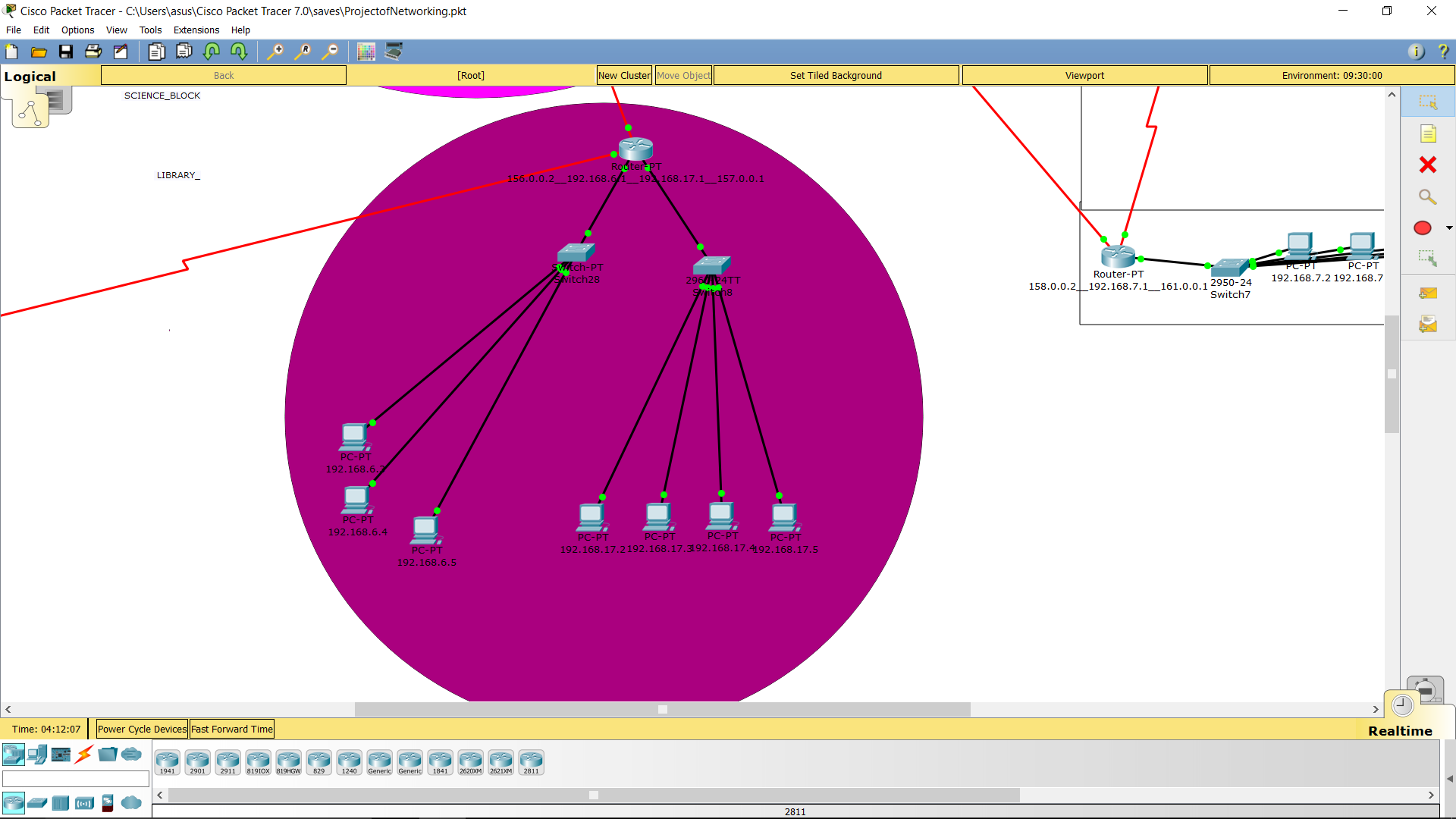
The Cisco Catalyst 3550 series switches used here are layer 3 switches with built-in routing capabilities, making them the preferred choice at a reasonable cost. Of course, the proposed solution shown here is only a small part of a large scale network where switches such as the Catalyst 3550 are usually placed as core switches, connecting all branch switches together (2924's in this case) via superfast fiber Gigabit or Fast Ethernet links, ensuring a fast and reliable network backbone.

**SCREENSHOTS**

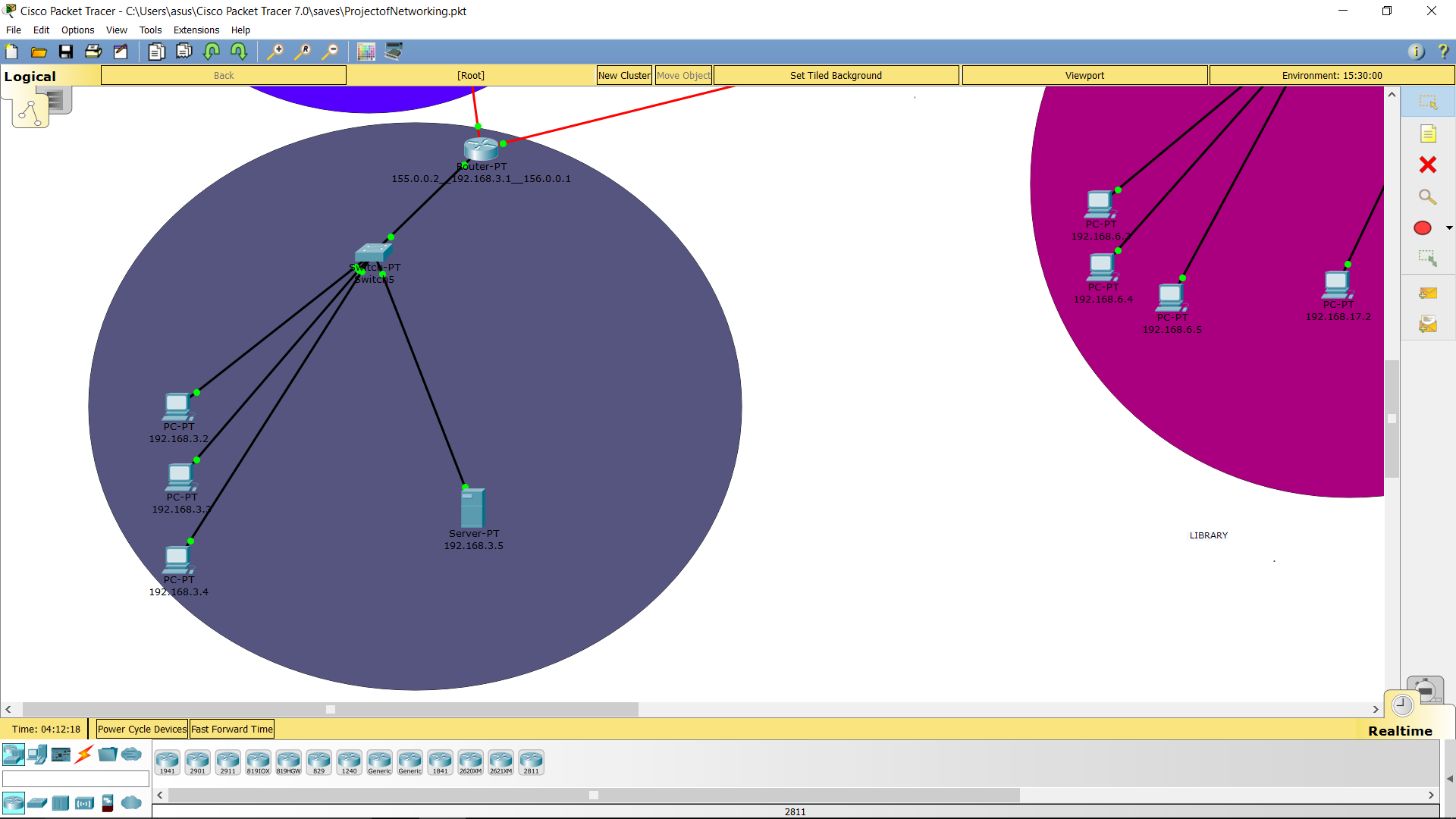
 **WHOLE CAMPUS NETWORK ARCHITECTURE LAYOUT**

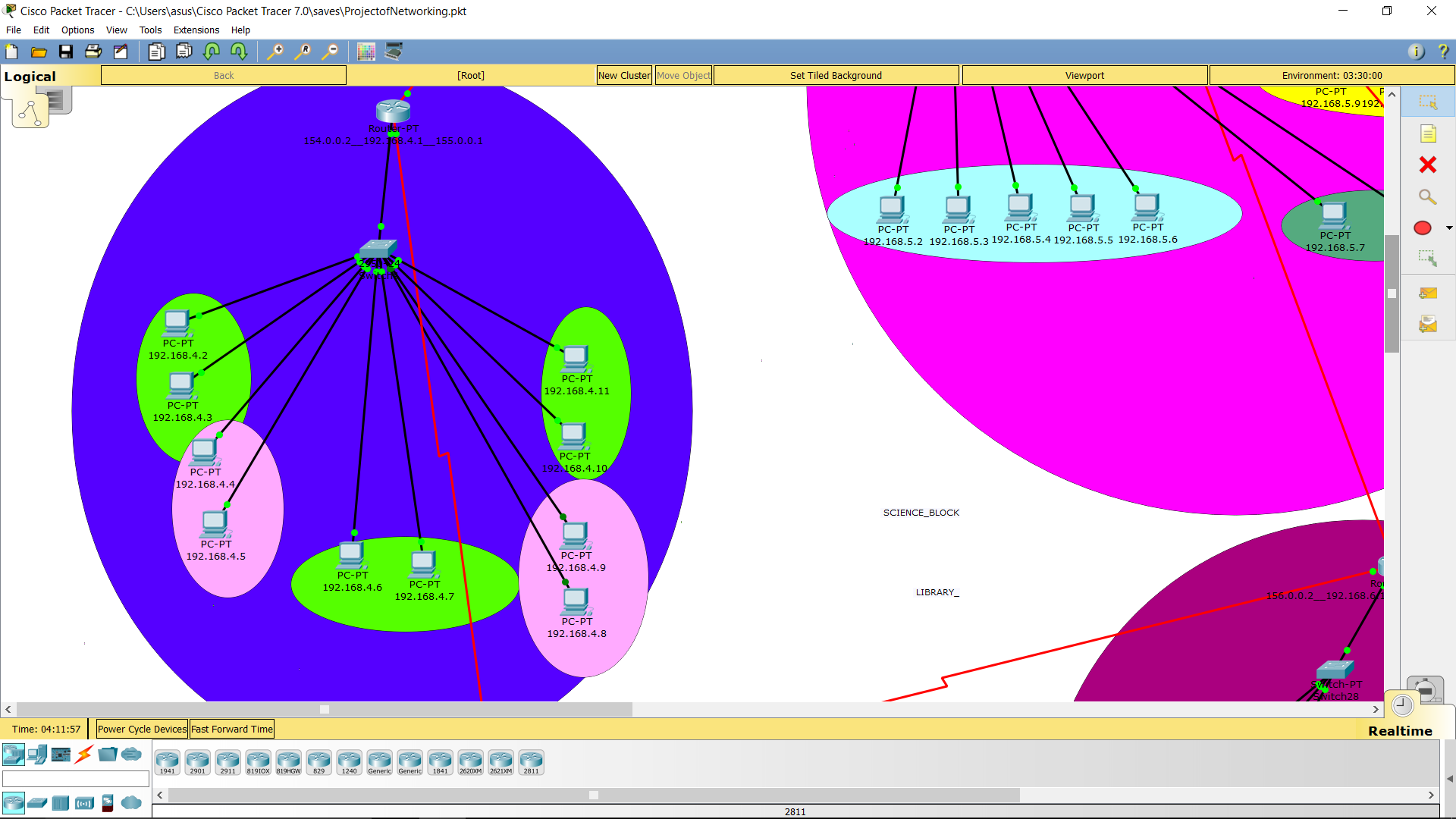
**SCIENCE & LIBRARY DEPARTMENT**



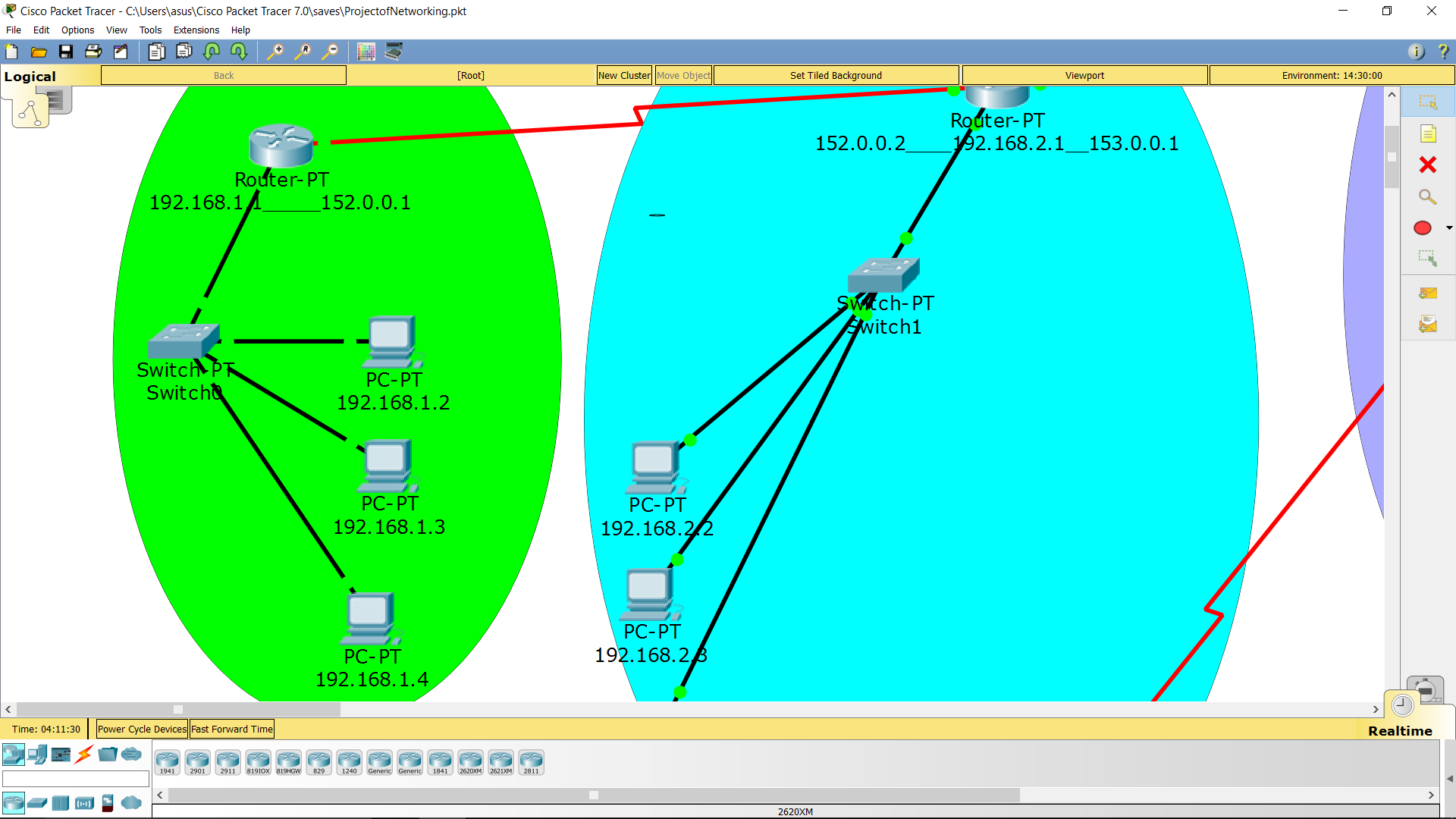


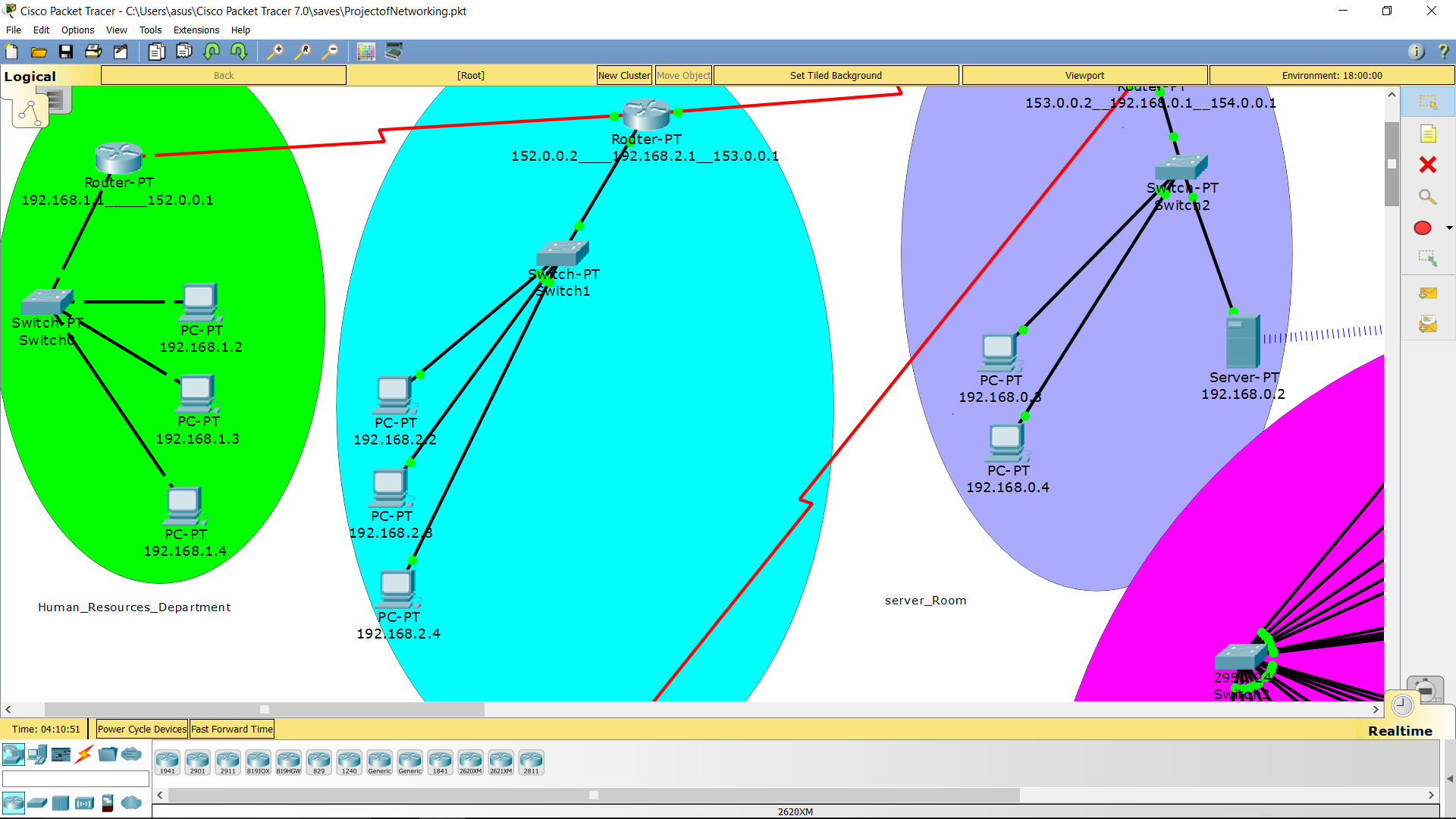
**ART & NUCLEAR DEPARTMENT**



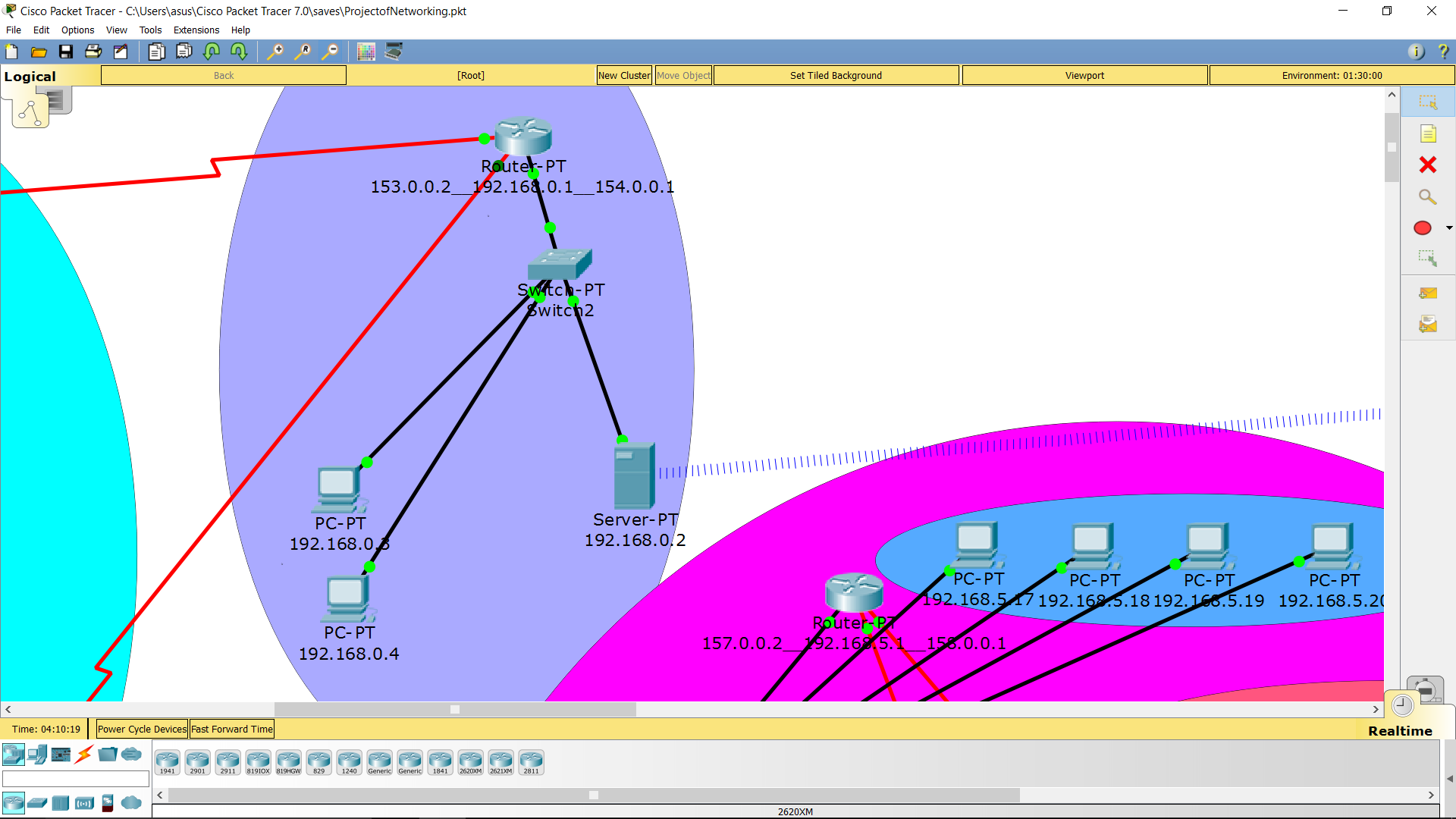


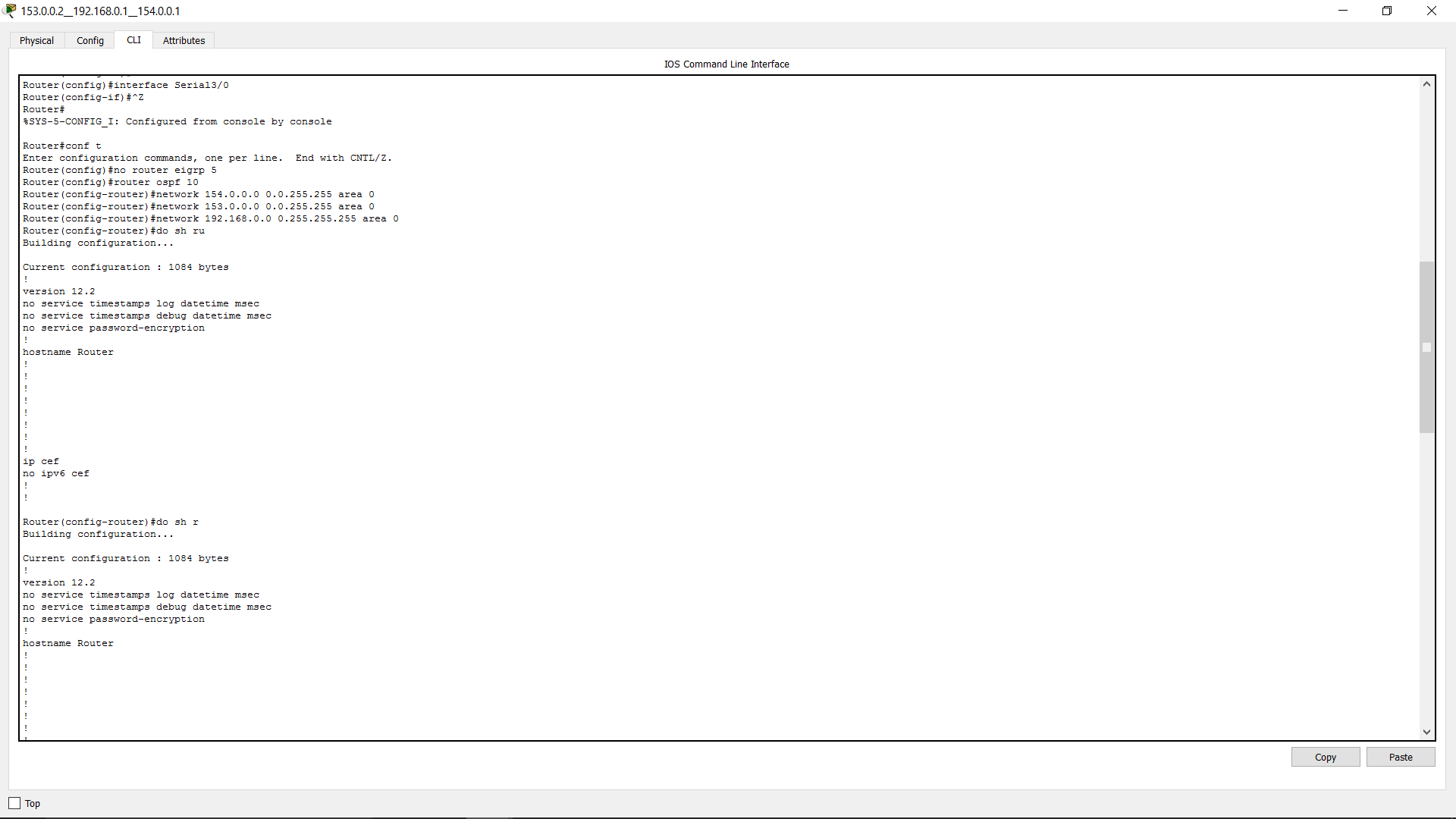
**HUMAN RESOURCES & LINGUISTIC DPRT**





**SERVER ROOM & OSPF COMMANDS**



****

**References:**

1. [**www.google.com**](http://www.google.com/)
2. [**www.wikipedia.com**](http://www.wikipedia.com/)
3. [**www.firewall.cx**](http://www.firewall.cx/)
4. [**www.encyclopedia.com**](http://www.encyclopedia.com/)
5. [**www.ebookee.org**](http://www.ebookee.org/)