NACKADEMIN

IT-Infrastructure (LIA) ITI 22

Philippe Martinet

1. LIA 22 Project Specifications

You've just been employed at Cisco AB to work with one of their five IT-Infrastructure teams. Congratulation!!

Already today, your boss explained to you that the computer network has some critical issues that need to be solved before the Big conference that occurs in 8 weeks. New challenges will occur every Monday. Solutions need to be found and simulated using Packet Tracer (PT) from Cisco.

AT the end of the 8 weeks you'll have to present your solution in front of others IT-teams as well as your boss! and you have to deliver a copy of your final report.

The report need to have at least 10 pages long (in Times, 14pt). You'll describe in details using text, graphs, figures and references how your solution could be implemented physically and how it will solve all the issues of the physical network.

Each team will have to present a solution for every challenges that will occurs every weeks.

The company applies agilt/scrum working methodology. The sprint is one week long. Therefore, every Friday, your team will have to present in 15 minutes their solution of the challenge of the week, the problems they had and how they intended to solve these problems. Each teams will help and discuss every other team's solutions.

2. LIA Project Description

Your LIA project consists of four parts:

1) To install and understand how to use Packet Tracer (PT).
2) Find a solution to every week challenge using PT.
3) Participate at the Friday sprint discussions.
4) Write a final report of 10-20 pages.

Project Deadline: Thursday the 16 of Mars at 11:59 pm.

Presentation of all projects: Friday the 17 of Mars between 9:00 and 12:00,
(20 mn + 10 min discussion for each presentation)

3. First challenge: Address resolution protocol

The first challenge is to:

1) Use **arp** *command for address resolution*
2) Use Wireshark/tcpdump to examine arp exchanges.

Task 1: Install and explore PT Each team have to download, install and configure the computer network simulator Packet Tracer from Cisco. For that you need to create a free account using your email address.

Start at:

https://www.netacad.com/courses/packet-tracer

and then go to:

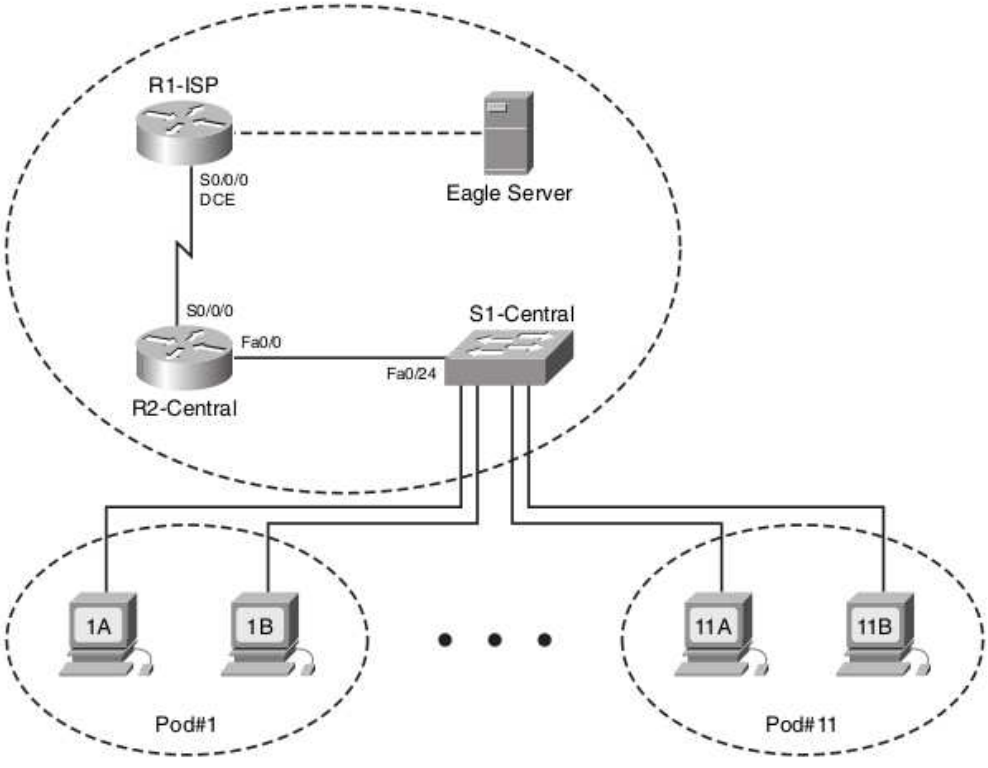
https://skillsforall.com/?utm_source=netacad.com&utm_medium=referral&utm_campaign=packet-tracer&userlogin=0&userlogin=0

And press "Get Started"

Open an account and you should be able to download Packet Tracer (PT).

Task 2: Create the network using PT

Create the following network using PT



Addressing Table:

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	—
	Fa0/0	192.168.254.253	255.255.255.0	—
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	10.10.10.6
	Fa0/0	172.16.255.254	255.255.0.0	—
Eagle Server	—	192.168.254.254	255.255.255.0	192.168.254.253
	—	172.31.24.254	255.255.255.0	—
Host Pod#A	—	172.16.Pod#.1	255.255.0.0	172.16.255.254
Host Pod#B	—	172.16.Pod#.2	255.255.0.0	172.16.255.254
S1-Central	—	172.16.254.1	255.255.0.0	172.16.255.254

Task 3: Create the physical network

Create the same network using the physical devices available at Nackademin.

Task 4: ARP

Apply **arp** to map a layer 3 IP address to a Layer 2 Mac address.

Teori

- ARP is a protocol that enables network devices to communicate with the TCP/IP protocol. Without ARP, no efficient method exists to build the datagram Layer 2 destination address.
- When a frame is placed on the network, it must have a destination MAC address. To dynamically discover the MAC address of the destination device, an ARP request is broadcast on the LAN. The device that contains the destina- tion IP address responds, and the MAC address is recorded in the ARP cache.
- With no cache, ARP must continually request address translations each time a frame is placed on the network. This adds latency to the communica- tion and could congest the LAN.
- ARP is a potential security risk. ARP spoofing, or ARP poisoning, is a technique used by an attacker to inject the wrong MAC address association into a network. An attacker forges a devices MAC address, and frames are sent to the wrong destination. Manually configuring static ARP associations is one way to prevent ARP spoofing.