Surveillance Data Sharing

TCP/IP Training

Application with Mikrotik router

January 2020
Niamey, Niger

Program

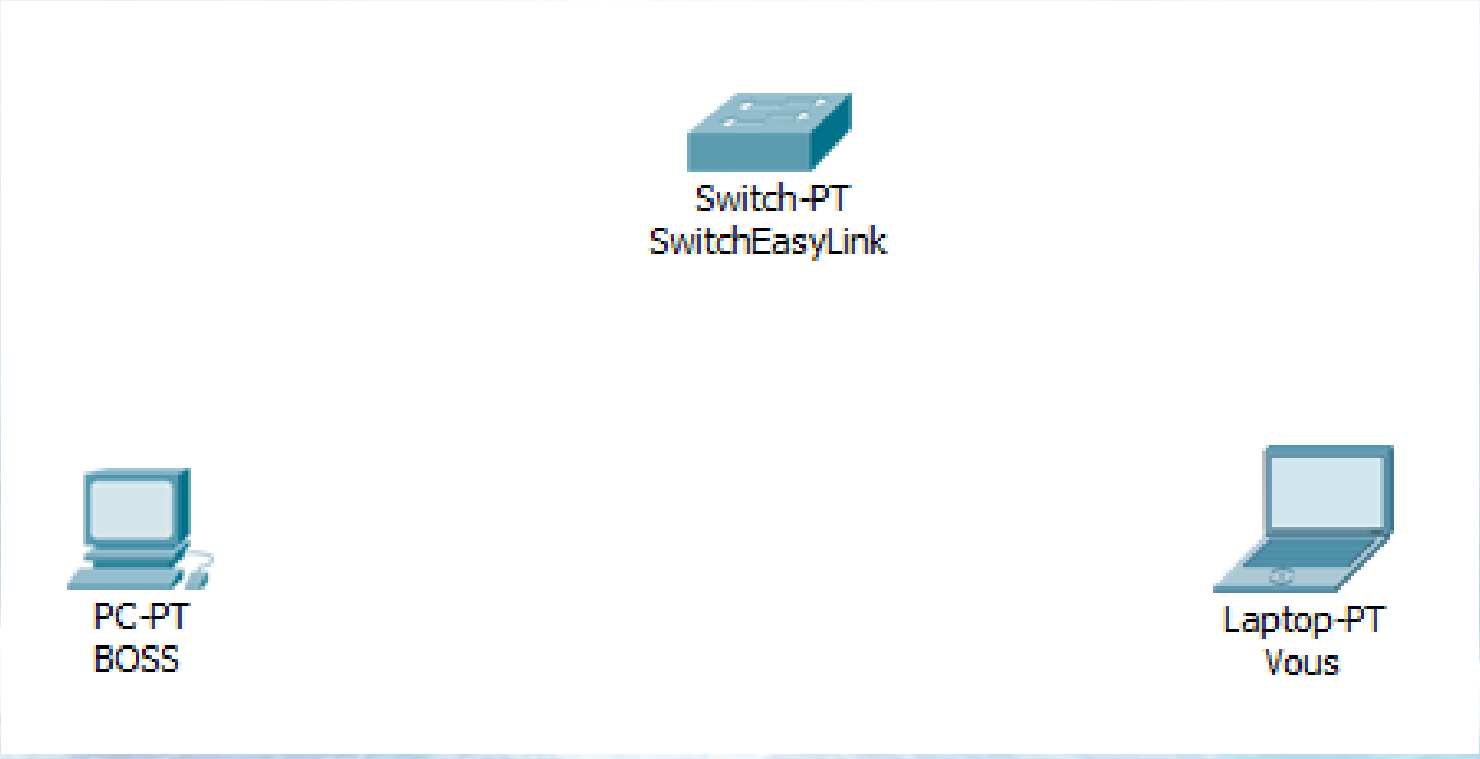
- TCP/IP basics :
  - IP addresses
  - Network sizing
  - Static routing
- TCP/IP Advanced :
  - Bridge
  - Multicast traffic
  - Dynamic routing using RIP or OSPF
  - VLAN
- What you want to see

OSI layers

- For us, only the first 3 layers will impact us:
  - First layer: the PHYSICAL Layer
    - Cables (FTP, fiber, coaxial, …)
    - This layer has to be verified FIRST
  - Second layer: LINK Layer
    - Machines
    - Switchs
    - HUBs
    - To verify this layer, you can do a PING
  - Third layer: Network Layer
    - Routers
    - Firewall
    - Internet Access Point
    - To verify this layer you can do a PING

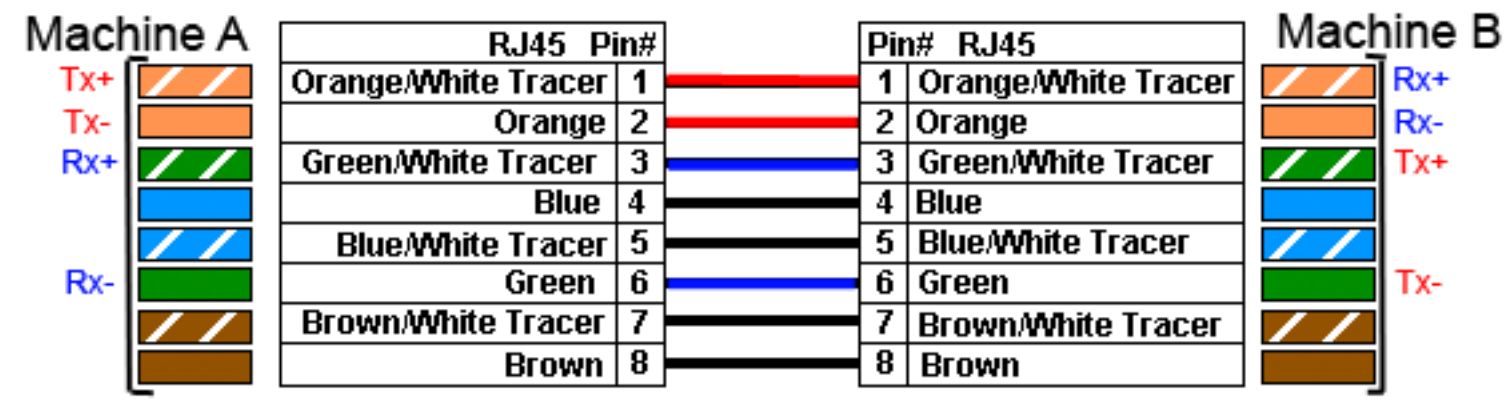
Example

- Simple Case :



First step: PHYSICAL Layer

- In our case, cables are missing
- We will use FTP cables :



- T568A and T568B norms => different colors
- In all cases, one pair to transmit, one pair to receive

Straight or Crossed cables

- Old equipment cannot negociate, then you have to use crossed cables
- Most of the cases now you can use straight cables
- Always verify datasheets
- Be carefull: FTP cables with RJ45 connectors do not necessary transmit Ethernet data
- As cables and connectors costs drops, industrials used them to transmit other signals (like VHF, telephony, power, E&M, …)

Second step: Switch

- Connection to a switch:
  - Equipment and switch negociate
- What is happening in the switch :
  - Eletric activity detection
  - Dialog initiation
  - Negociation
  - Communication establishement
  - MAC address linked to interface

MAC address

- Address linked to a machine
- PC, switch, router, phones, everything connected to a network
- It is unique
- MAC address translation is possible but not of our concern
- Representation: XX:XX:XX:XX:XX:XX, 6 octets
- Some MAC addresses are reserved for bands, protocoles, …

What do we need more?

- Everything seems to be ok to communicate:
  - A physical network
  - A switch
  - Adresses
- We have to use a communication protocole now:
  - TCP/IP
- In order to work, this protocol needs other adresses
  - IP adresses

IP address

- An IP Address is composed of:
  - A 4 octets host address
  - A 4 octets networt mask
- In binary, an IP address will be like the following:
  - Host address: 10000000.00001000.01000010.10000010
  - Network mask: 11111111.11111111.11111110.00000000
- What is the result in decimal as it is usually writen ?

Decimal/Binary

- Translation sheet:

Poids	128	64	32	16	8	4	2	1
Nombre Binaire	0	0	1	0	1	1	1	0
Conversion	0	0	32	0	8	4	2	0
Somme	46							

Poids	128	64	32	16	8	4	2	1
Nombre Binaire	1	1	1	1	1	1	1	1
Conversion	128	64	32	16	8	4	2	1
Somme	255							

- DECBIN and BINDEC can be used with Excel sheets

Network Mask

- We use the mask to determine the sub-network address

- Example with our address:
  - @host: 10000000.00001000.01000010.10000010
  - or 128.8.66.130
  - Mask: 11111111.11111111.11111110.00000000
  - or 255.255.254.0
- What is the sub-network used in that case ?

Host address AND Mask = Sub-Network

- AND rules :
  - 0 AND 0 = 0
  - 0 AND 1 = 0
  - 1 AND 1 = 1

	128	64	32	16	8	4	2	1
Adresse	1	1	1	1	0	1	0	1
Masque	1	1	1	1	1	1	1	0
Sous réseau	1	1	1	1	0	1	0	0
Consersion	128	64	32	16	0	4	0	0
Somme	244							

- In our case, what is the sub-network ?

/X

- Lets consider the followin sub-network:
  - 128.8.66.0/23
  - /23 ? What does it mean ?
- Human want to simplify everything
- Masks are limited to continuous 1, so we cannot have 10101100 as network mask
- Masks end with 11100000, 10000000 or 11111110, it means that there is 1 left to a 1
- We speak about significant bits
- If we consider this mask: 255.255.255.0, in binary it will be 24 significant bits followed by 8 zeros
- We decided to write /24
- In our case, we hat 23 significant bits, then the mask can be writen /23

Network sizing

- Thanks to the sub-network we can:
  - Determine the maximal size of our network
  - Determine the broadcast address
- In other words, we will be able to size our network!
- Lets use again our example:
  - 128.8.66.0/23
- The first address will be: 128.8.66.1/23, easy!
- The last address will be: 128.8.67.255/23,
  - hummmm, ok why ??

Last address

- To determine the last address we go back to binary, amazing!

Poids	128	64	32	16	8	4	2	1
Adresse	0	1	0	0	0	0	1	0
Masque	1	1	1	1	1	1	1	0
Masque\	0	0	0	0	0	0	0	1
Last Adresse	0	1	0	0	0	0	1	1
Consersion	0	64	0	0	0	0	2	1
Somme	67							

- Invert operation : X = 0 => X\ = 1 and vise versa
- To get the last address, we make a logical OR between the host address and the inverse of the mask.
- This address will be the broadcast address

Broadcast

- A broacast address has to be defined in each sub-network in order to send data to every hosts
- This is really usefull for maintenance data and some applications which need to send data to everyone
- A live streaming can be considered as broadcasting, the only difference is that the broadcast is limited to people who watch the video, in that case it is called multicast
- Multicast is for « interested » hosts, Broacast is for everyone

To resume

- An IP address is composed of a host address and a network mask
- The sub-network must be determined to size the network
- Then the fist and the last address can be found, and the last one will be used to broadcast

- Lets size our network!

Other way to use network sizing

- ASECNA will build a new building in Niamey
- In this building 1000 people will work with PCs
- Considering everything, about 1200 equipment will be connected to the network
  - Which network mask do you use ?
  - Choose a sub-network and:
    - Give the first host address
    - Give the last host address
    - Calculate how many hosts can be connected
    - Give the broacast address

Any questions so far?

What is happening in a switch?

- When we give an IP address to a PC, it will put it in each sended Ethernet frame
- It will also put a destination address, it is always better to specify an address when we want to send something to someone!
- So the switch will receive the Ethernet frame with two addresses
- It will send an ARP request: « Hello everyone, Who has X.X.X.X. ? »
- In « Hello everyone » we can ear « Broadcast » right?
- The switch send on the broadcast address its request in order to know where it can send the Ethernet frame. If someone answer, the frame will be send and the switch will write in the ARP table that X.X.X.X correspond to that MAC address

Interest of the ARP table

- The ARP table will allow the switch to be faster
- For the following frame to the same destination, it will not send a new ARP request (not yet)
- This table is updated periodically
- Sometimes this mechanism is not working well and a reboot is needed
- This update can be important when an IP address is shared between two equipment (VRRP address usually used in redundant architectures)

Can we see that ?

- Yes!
- But it is better to know what you are looking for
- WIRESHARK can be used to watch traffic (using for example a port mirroring)
- I am not an expert with Wireshark but when I know what to find its a usefull tool
- For example, if you are searching for a ping you will filter the result on ICMP protocol then it will be easier to find it

Reserved Addresses

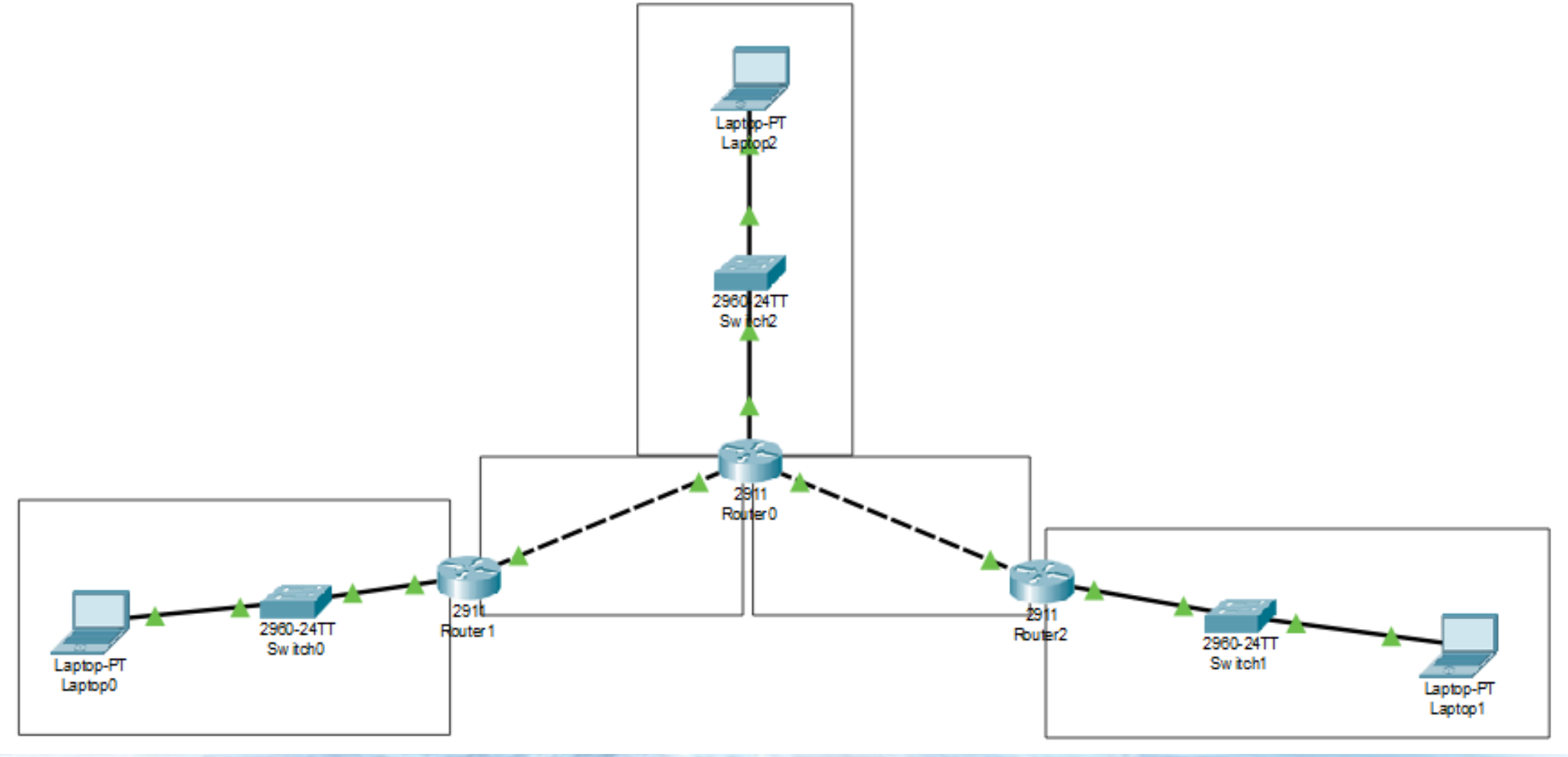
- Some addresses are reserved, they can easilly be find in Wikipedia
- Private ones interest us today :
  - 10.0.0.0/8 => more than 16 millions addresses
  - 172.16.0.0/12 => more than 1 million
  - 192.168.0.0/16 => more than 65000
- Private addresses cannot be routed on the Web
- We ussually address private networks in these ranges
- As a consequence, to go on the Internet we need a public address

Lets talk about routing

- What we have seen until now is limited to layer 2
- Lets see what's going on in layer 3
- So we will discuss about static routing to start
- Routing is needed when 2 (or more) different networks need to communicate

- The best is to work on an example:

Static routing example



Static routing example

- With a star topology:
  - HUB network: 10.220.0.0/16
  - Site 1 network : 10.221.0.0/16
  - Site 2 network : 10.222.0.0/16
  - Site X network : 10.22X.0.0/16
- Propose an architecture in order to allow Site X to communicate with HUB station
- What can you do in order to allow all PC to communicate with each other ?

Gateway

- Navigation analogy:
  - I am in my town, I can walk inside without problem
  - If I want to go the next town I need to cross the highway
  - To cross it I use a gateway
- It’s the same with networks, to get in another one, I need a gateway
- And how it’s working ?

Gateway

- A route is a way to go somewhere
- A static route is a fixed path to go to a destination, there is no other route to go there
- If the route is cut, i cannot go there
- A cutted route, or no route, is the same thing when we talk about network, we cannot go throught the jungle, Ethernet frames need routes
- Example:
  - To go to Paris by plane from Niamey, I need to go to the airport
  - I can write it like a static route: To reach Paris I need to reach the airport first

Static Routes

- static route add X.Y.Z.0/24 @gateway
- It is a static route that says:
  - in order to reach the sub-network X.Y.Z.0/24 Go to the gateway first

- static route add 0.0.0.0/0 @gateway
- It is a gateway by default
- It means that an Ethernet frame send outside my network will be send automatically to this gateway
- This configuration is usually used on your PC

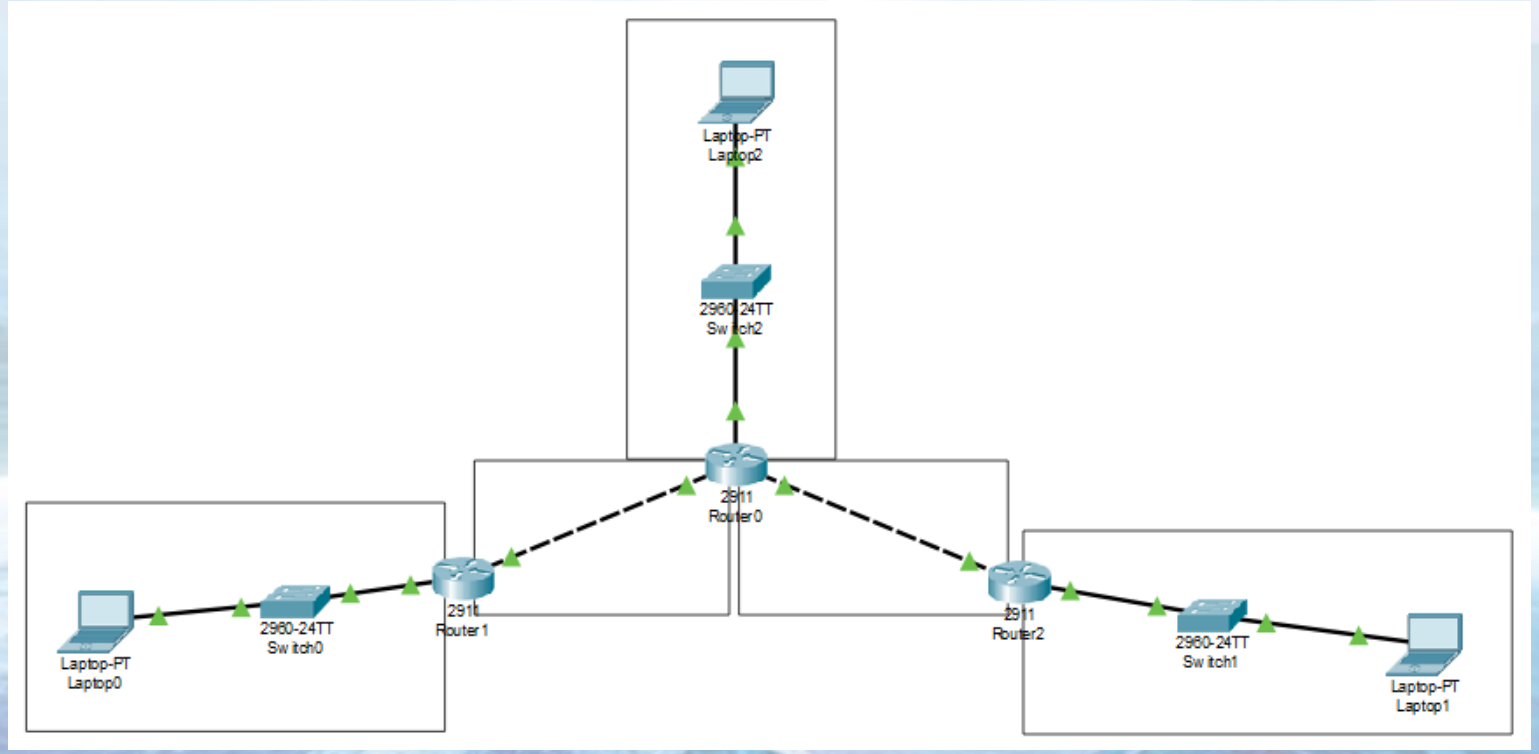
Any questions before we go further?

Mikrotik Routers

- As you will see, Mikrotik routers are user-friendly and easy to configure
- They can be updated without license
- They come with basic fonctionnality and can be upgraded without license
- Very important: A complete help space is online where configurations are explained and where you can see examples as well
- These routers have firewall functions also

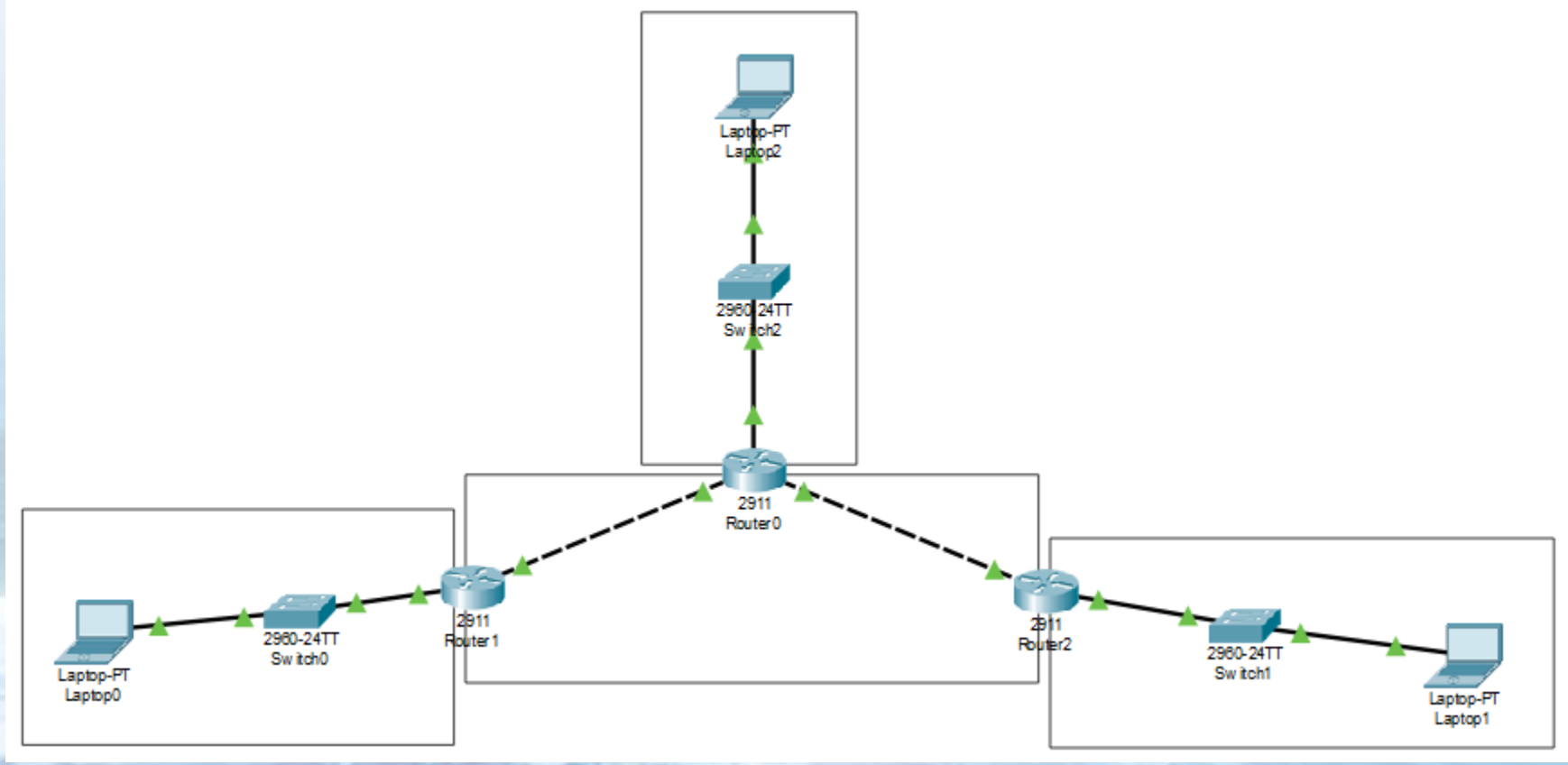
Practice

- Lets apply what we have seen
- We have 5 routers, the idea is to build a routed network with one HUB and 4 sites :



Practice

- What can you do to get that one now ?



Bridge

- A router cannot have 2 interfaces in the same network
- To take advantage of layer 2 features, you must configure a bridge
- A bridge is created with the association of multiple interfaces in the same sub-network
- So, in our case, the idea is to create a transmission network using for example 192.168.10.0/28
- Lets go!

Multicast traffic

- With that network we are able to transmit unicast traffic between sites
- RADAR traffic is usually multicast
- Multicast traffic use:
  - Multicast server
  - Multicast clients
- Multicast is natively blocked on routers to reduce unwanted traffic and save bandwidth

Multicast traffic

- To transmit multicast traffic via a routed network we must use a special routing protocol
- Between others, we will choose PIM
- PIM stand for Protocol Independant Multicast
- Like it says, PIM does not care about the used routing protocol, it will go above it
- Then PIM can be used everywhere (the only condition is to have PIM compatible routers)

Multicast traffic: PIM

- This protocol works using routers cooperation
- PIM interfaces must be declared and you have to specify on which multicast server
- Then multicast clients will send traffic requests
- PIM is independant from the used routing protocol
- To limit the bandwidth used by PIM traffic, a router is chosen to receive IGMP requests and send it to corresponding multicast servers
- It is called the Rendez-Vous Point
- This router must be joined by all routers

- We will configure PIM in our network

Any questions ?

A bit of dynamism now ?

Before we go further

- With what we have seen until now, you are able to configure and manage your network
- IP is nice because you can find a lot of help and support
- Mikrotik's help is really well done and usefull (you can also help yourself with CISCO university)
- By knowing basics you will be able to implement them on your equipment (whatever the brand)
- Good to know: When you build a network, try to use only standardized protocols. As technology moves really fast, it will expand the life of your network and allow you to use COTS equipments

Lets go further

- Everything we did was static, now we will add some dynamism to our network

What is DHCP?

- A DHCP server allows you to configure IP address and gateway of all DHCP clients
- No dual IP address
- Not always usefull
- To configure DHCP, you have to determine interfaces and address range

Dynamic routing

- Complex architectures imply complex protocols
- For example when to architecture is meshed, using dynamic protocol become usefull
- Dynamic protocols allows:
  - Redundancy in case of node loss
  - Quickly reconfigure the network in case of network update
- We will see dynamic routing using RIP and then OSPF

RIP Protocol

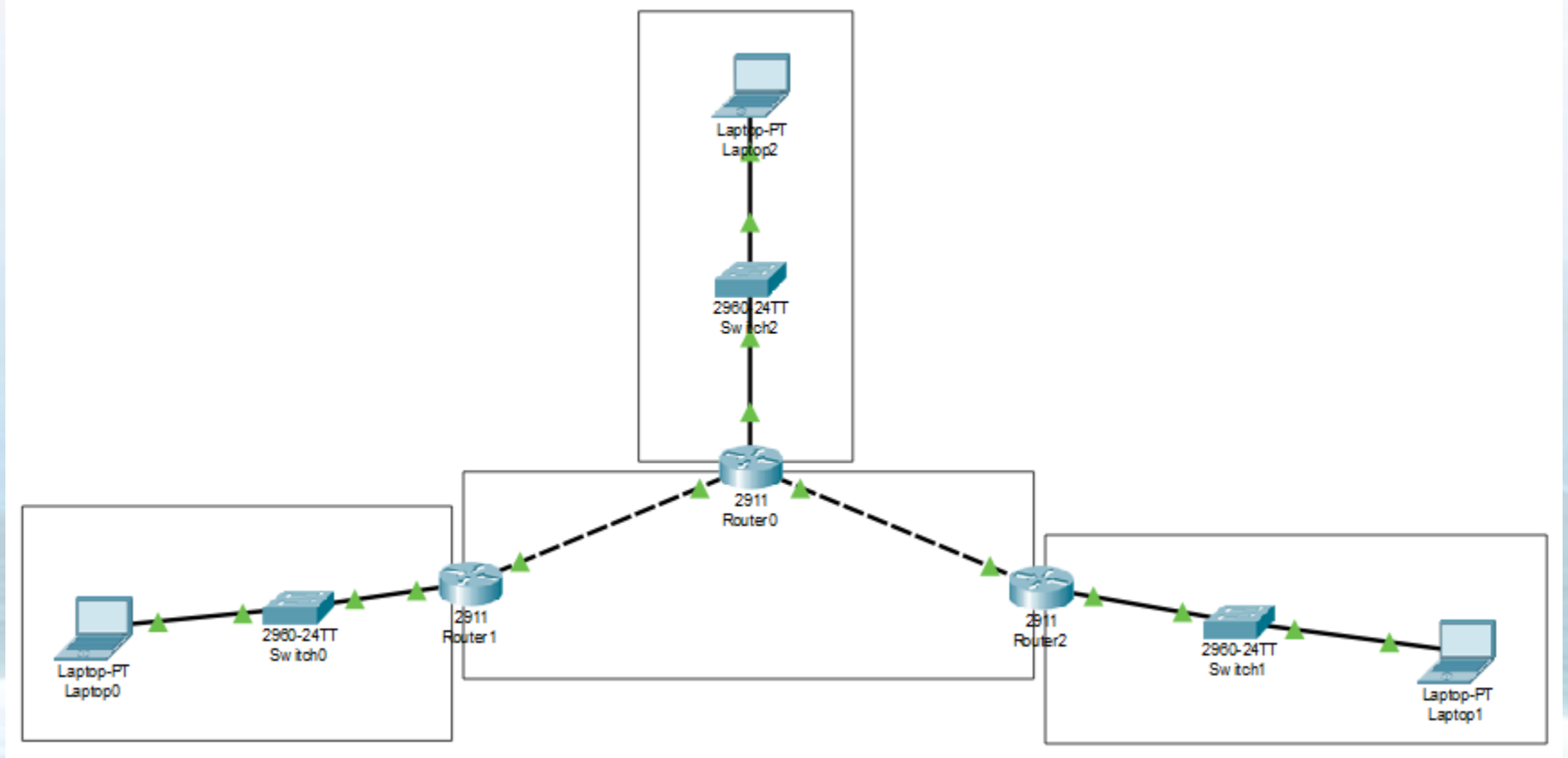
- RIP is the first protocol created for dynamic routing
- It is not used in actual networks but it’s a good way to understand protocols
- The idea is to use router collaboration inside the network, every routers will share its routing table to its neibourgs
- As a result, each router will have a global vision of reachable networks
- Path weight is used to select a path between others
- Path weight is calculated in term of hops between source and destination
- If a route is not available, the next shortest route will be used

RIP Protocol

- Lets implement RIP in our network
- Before that, delete all static routes

- Then configure RIP in each router and precise which networks can be reached
- So, in our case, each router will have:
  - Its local network
  - The transmission network
- Once configured and connected, each router will share its routing table and the network will be up

RIP

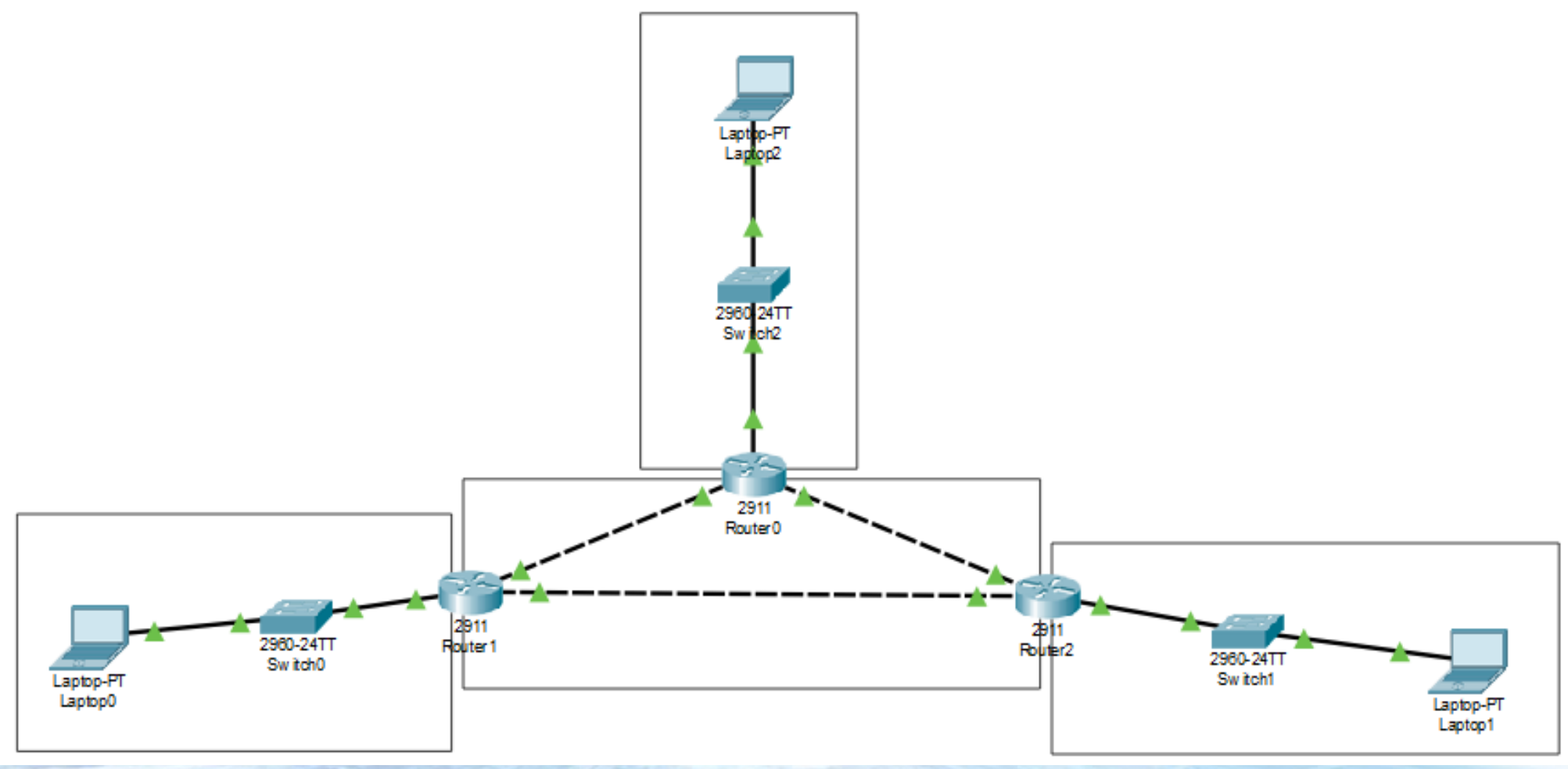

Laptop-PT
Laptop2
2960-24TT
Switch2
2911
Router0
2911
Router1
2911
Router2
2960-24TT
Switch0
2960-24TT
Switch1
Laptop-PT
Laptop0
Laptop-PT
Laptop1

RIP Protocol

- We can see that the configuration is quicker (think about the add of a new station, in static, and using RIP)
- With this star architecture it’s the only interest

- The idea now is to build a meshed network
- In other words, all stations will be connected

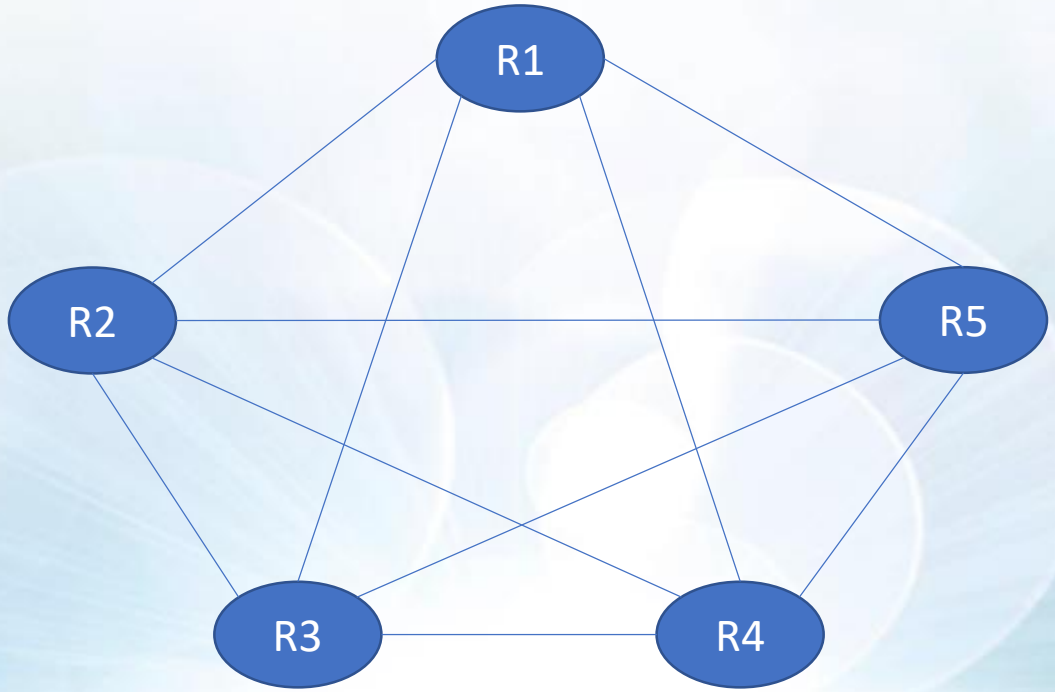
RIP


Laptop-PT
Laptop2
2960-24TT
Switch2
2911
Router0
2911
Router1
2911
Router2
2960-24TT
Switch0
Laptop-PT
Laptop0
2960-24TT
Switch1
Laptop-PT
Laptop1

RIP

- When all is done, make redundancy tests and see what is happening
- Do we have redundancy in case of link failure ?
- What’s going on in case of failure ? Which parameter is impacted ?
- Do we loose packets at the failure ?
- Is there protocols that avoid losses in case of failure ?

Full meshed topology with 5 nodes



OSPF Protocol

- OSPF protocol (Open Shortest Path First) works also thanks to routers cooperation
- The difference with RIP is in the algorism which dertermine the shortest path
- OSPF takes into account the state of links and not only the number of hops
- Navigation analogy:
  - Depending on the traffic jam, the path from A to B is not necessary the shortest way
  - It’s the same for networks, as satellite links add a lot of delay, it may not be the quickest way even if there is only one hop

OSPF Protocol

- As PIM, OSFP use a special router which concentrate protocol data and administrate the network
- It’s the Designated Router
- Is the DR is not fixed by the administrator, the network will elect one but it might not be the best one considering your architecture
- In case of failure, you can also name a redundant Designated Router (it will limit traffic losses as the network will not hace to elect a new one)

OSPF Protocol

- Now we will repalce RIP by OSPF and make the same redundancy tests
- There are protocols which allow the use of multiples routes at a time even if delays are not the same
- Protocols are choosen considering the needs, in a small network OSPF is not necessary the best choice
- As we have seen, protocols use the network by sendind packets. In case of limited bandwidth, it has to be taken into account

Any question before VLANs?

Introduction to VLANs

- Lets go back to layer 2!
- VLAN stand for Virtual Local Aera Network
- It’s a tool that allows to separate networks by the add or an overhead
- VLAN tag will be checked to filter communications
- If an Ethernet frame does not have the good VLAN tag, it will be blocked

SAOMA example

- ASECNA has a network called SAOMA in order to transmit weather sensors information
- This network use VLANs
- What we will see :
  - Native VLAN
  - Access Mode
  - Trunk Mode
  - VLAN Membership

SAOMA VLAN configuration

Any questions ?

What do you want to see next?