1. Sprint 2

In the follow out of sprint one, the team is now required to create a network simulation matching the created structured cabling project. In this sprint the focus is on the layer two infrastructure, and the layer three fundamentals (IPv4 addressing, and static routing).

For such purposes, the Cisco Packet Tracer tool must be used.

1.1. Teamwork organization

Each team member is assigned the task of creating the Packet Tracer simulation for same building that was assigned in the first sprint.

Each of these simulations will encompass a single building, however, **they must include the campus backbone**. As we'll see ahead, this means each simulation must include a switch representing the main cross-connect, and switches representing each other building intermediate cross-connect.

The team member assigned with **building A** has one additional final task: putting together into a single Packet Tracer simulation all simulations created by every team member. If there's a good coordination between team members work, this is just about a simple copy and paste operation between Packet Tracer instances. The best option for cutting points is the connection of each building to the backbone network, each building's main switch should be kept and the backbone connections between those switches rebuilt. Bear in mind connections between those switches must be in trunk-mode.

1.2. Packet Tracer version

To avoid any issues when putting together all team members' work into a single Packet Tracer simulation, the same Packet Tracer version must be used by all team members. They all should use the version provided in the laboratory classes.

1.3. Devices naming

When a new device is added to the Packet Tracer simulation, a display name is automatically assigned, but then it should be changed to a meaningful name. During the planning meeting, the team should establish some rules regarding this, it will facilitate the team work, and this should be included in the **planning.md** document.

The display name is just for Packet Tracer to display, at the OS level, each device has a hostname (DNS name), that can be settled by using the **hostname** command, however, no spaces are allowed.

2. Layer two configuration

The goal is creating a logical and not physical network layout, which should nevertheless be representative of the structured cabling project from the preceding sprint.

Namely:

- Every cross-connect (distributor), including consolidation points (CP), in the structured cabling project is to be represented in the simulation by a layer two network switch. Use **PT-empty** switch models, and add to them the required port types.

- Cable types interconnecting different cross-connects (switches in the simulation) must match the cable types (copper of fibre) settled in the structured cabling project. And the same goes for horizontal cabling subsystems.
- Redundant cable links between cross-connects present in the structured cabling project should as well be present in the simulation. Nevertheless, multiple cable links between two cross-connects (link aggregation) can be represented as a single connection between two switches in the simulation.

2.1. Virtual LANs

In <u>each building</u> the following unique five VLANs must be defined:

- A VLAN for all end-user outlets on the ground floor.
- A VLAN for all end-user outlets on floor one of the building.
- A VLAN for the Wi-Fi network (for all access-points' outlets within the building).
- A VLAN for the building DMZ (for servers, administration workstations, and industrial machines at buildings C, D, and E).
- A VLAN for VoIP (for IP-phones).

Despite being assigned to a specific building, these VLANs must be available on every switch, on every building, meaning all and every switch should have all buildings' VLANs it the local VLAN database and all switches interconnections must be configured in trunk-mode with all VLANs.

In addition to those, **a VLAN must be established for the campus backbone**, unlike the others, this is the same VLAN for all buildings, likewise this VLAN must be available on every switch, of every building, and be present on every switch's VLAN database.

So, **to summarize and clarify,** for a project including the five buildings, there'll be a total of (5 x 5) + 1 = **26 VLANs** (this is the case for a team with five members). If the team decides not to use any of those as the default VLAN, there's also the **default VLAN**, teams can keep the use of VLANID 1 for the default VLAN.

Again, all these VLANs must be available at every switch of every building. This doesn't mean they are going to be used (have end devices connected to them), on each building only the VLANs belonging to that building will be used. Nevertheless, being available means the administrator may at any time connect a device anywhere in the infrastructure to any VLAN, is just a matter of assigning the corresponding switch port to the desired VLAN.

2.2. Spanning tree protocol

If your layout encompasses redundant cable links between switches, then STP is a must. Switches have STP enabled by default, so there's nothing to do here, simply **don't disable STP on any switch**.

2.3. VLAN Trucking Protocol (VTP)

This is one convenient way to ensure all switches have the same complete VLAN database. To achieve that:

- All switches must use the same VTP domain name (**vtp domain …**).
- All switches except one should be in VTP client mode (**vtp mode client**).
- One switch will be in server mode (**vtp mode server**). This is the switch where the VLAN database is manually defined (**vlan**), and changed whenever needed.

As far as switches interconnection ports are in trunk mode (**switchport mode trunk**), and the VTP domain name is the same, VTP will ensure the VLAN database propagation (copying) from the switch in server mode into all switches that are in client mode.

2.4. VTP servers

For the sake of each building Packet Tracer simulation, one switch must assume the VTP server role, this is supposed to be the switch representing the highest cross-connect level within the building. So for building A it's the main cross-connect (the campus distributor) and for the remaining buildings it's the intermediate cross-connect (the building distributor).

On the sprint end, when the team member assigned with **building A** undertakes the task of putting together all simulations in one, all switches in VTP server mode must be changed to client mode, except for the one representing the main cross-connect.

2.5. VLAN database

All Packet Tracer simulations must use the same VLAN database (to be defined manually on the VTP server switch). Resulting from the planning meeting there should be a table or list of VLANs to be used by all team members (must be included in the **planning.md** document).

Each VLAN should have a unique meaningful name, and a unique VLANID. In Cisco devices VLANIDs between 2 and 1000 can be used without interfering with other features. **For this project, each team is required to use a specific range of values for VLANIDs,** please check the **"Per team specific data - mandatory use by teams"** chapter in the last pages of this document.

2.6. VTP domain

VTP only propagates the VLAN database between switches belonging to the same VTP domain, thus, so that later all simulations may be putted together easily, all team members must use the same VTP domain name on every switch. The VTP domain name can be 1 to 32 characters long, spaces are not supported. The VTP domain name for each team is established at the **"Per team specific data - mandatory use by teams"** chapter in the last pages of this document. The VTP domain name should be also registered in the **planning.md** document.

3. Layer three configuration

Over the established layer two infrastructure, IPv4 networks will then be defined, more precisely **one IPv4 network for each VLAN**.

The IPv4 traffic forwarding between VLANs is implemented by **a router in each building**. In each building the corresponding router is connected to the backbone VLAN and provides access to every VLAN/IPv4 network in the building.

3.1. IPv4 networks

The IPv4 network address assigned to each VLAN must meet the following requirements regarding the maximum number of nodes it will be able to support.

3.1.1. Building A and backbone

- End user outlets on the ground floor: 40 nodes
- End user outlets on floor one: 40 nodes
- Wi-Fi network: 24 nodes
- Local servers and administration workstations (DMZ): 70 nodes
- VoIP (IP-phones): 20 nodes
- Backbone: 120 nodes

3.1.2. Building B

- End user outlets on the ground floor: 60 nodes
- End user outlets on floor one: 70 nodes
- Wi-Fi network: 100 nodes

- Local servers and administration workstations (DMZ): 12 nodes
- VoIP (IP-phones): 35 nodes

3.1.3. Building C

- End user outlets on the ground floor: 40 nodes
- End user outlets on floor one: 44 nodes
- Wi-Fi network: 60 nodes
- Local servers, administration workstations, and machines (DMZ): 250 nodes
- VoIP (IP-phones): 40 nodes

3.1.4. Building D

- End user outlets on the ground floor: 40 nodes
- End user outlets on floor one: 50 nodes
- Wi-Fi network: 60 nodes
- Local servers, administration workstations, and machines (DMZ): 250 nodes
- VoIP (IP-phones): 25 nodes

3.1.5. Building E

- End user outlets on the ground floor: 40 nodes
- End user outlets on floor one: 45 nodes
- Wi-Fi network: 60 nodes
- Local servers, administration workstations, and machines (DMZ): 250 nodes
- VoIP (IP-phones): 40 nodes

Each team is assigned with an **addresses block to be used** in the **"Per team specific data - mandatory use by teams"** chapter at the last pages of this document.

For each team, all used IPv4 network addresses must be non-overlapping and they have to belong to the provided addresses block.

In the sprint planning, the team has to establish:

- The IPv4 network address assigned to the backbone network.
- The IPv4 node address each router will use in the backbone network.
- The addresses block each team member will use. During the sprint, the team member in charge of a building will use this addresses block to assign IPv4 addresses to every network within the building.

Important: addresses blocks assigned to each team member can´t overlap each other's, and they can't overlap either with the IPv4 network address assigned to the backbone network.

The team master is responsible for registering this information and make it available to the team (**planning.md**).

3.2. End devices in the Packet Tracer simulation

For each VLAN **in use** at a building, there must be at least one end-device connected to that VLAN. So in the Packet Tracer simulation, for each building there should be:

- A workstation (PC) connected to the VLAN for end-user outlets on the ground floor.
- A workstation (PC) connected to the VLAN for end-user outlets on the floor one.

- A Wireless laptop, associated with a wireless access-point (not a wireless router) connected to the VLAN for the Wi-Fi network.
- A server connected to the DMZ VLAN.
- A VoIP phone connected to the VoIP VLAN.

End devices must be connected to the correct VLANs by configuring the corresponding switch ports in access mode (**switchport mode access**), and assigning to them the correct VLANs (**switchport access vlan …**).

Except for the VoIP phones, all other end devices are required to have a static and manually defined IPv4 configuration, including the default gateway.

For VoIP phones, the **7960 model** is to be used, the corresponding port on the switch must also be configured in access mode (**switchport mode access**), however, the access VLAN must be disabled (**no switchport access vlan**) and the voice VLAN must be used instead (**switchport voice vlan …**).

The IPv4 configuration of the VoIP phones is out of scope for now and will be left for the next sprint.

3.3. Routers and static routing

In each building there must be a router. **Please use a 2811 model, and no other model,** other router models may not support VoIP in Packet Tracer, required in the next sprint.

The router in each building will assure IPv4 traffic forwarding between local IPv4 networks (within the building) and to other buildings' IPv4 networks. Traffic to other buildings will be routed through the backbone IPv4 network to the appropriate router.

IPv4 node addresses being used by every router on the backbone network are established in the planning meeting, together with the addresses blocks assigned to each building, they make it possible to build the static routing table on every router.

Each team member is assigned the task of creating the Packet Tracer simulation for one building. Each of these simulations will encompass a single building, however, **they must include the campus backbone**. The main-connect and all intermediate cross-connects must be represented by a switch, and a router (2811 model) must be connected to each.

Because each router is connected to six different IPv4 networks, one might expect a router with six network interfaces would be required. However, the same way a single trunk-mode connection between two switches is able to connect several different VLANs, for a connection to a router the same applies, and on the router side each VLAN appears as different logical network interface (sub interface). **So in fact to connect the router to those six networks, a single connection to a trunk-mode port in the switch is does it.**

Regarding the configuration of routers outside the scope of the building, it should encompass only the connection to the backbone VLAN and corresponding IP address. The full configuration of each building's router is up to the team member in charge of that building.

3.4. Internet connection

Building A has an internet connection. The member in charge of this building will represent in by a DSL modem connection to a fake ISP router. The IPv4 node address in use by the fake ISP router is different for each team, it's provided ate the **"Per team specific data - mandatory use by teams"** chapter in the last pages of this document.

The fake ISP router must have a static routing table such as it will forward the matching traffic into the infrastructure.

4. Sprint 2 backlog

Task	Task description
T.2.1	Development of a layer two and layer three Packet Tracer simulation for building A, and also encompassing the campus backbone. Integration of every members' Packet Tracer simulations into a single simulation.
T.2.2	Development of a layer two and layer three Packet Tracer simulation for building B, and also encompassing the campus backbone.
T.2.3	Development of a layer two and layer three Packet Tracer simulation for building C, and also encompassing the campus backbone.
T.2.4	Development of a layer two and layer three Packet Tracer simulation for building D, and also encompassing the campus backbone.
T.2.5	Development of a layer two and layer three Packet Tracer simulation for building E, and also encompassing the campus backbone.

Task T.2.5 is to be ignored by teams with 4 members only.

5. Sprint 2 outputs/products

For each task on this sprint, the main output is the Packet Tracer simulation file for the corresponding building, it should be named **buildingN.pkt**, with N replaced by the letter identifying the building. Each team member is to commit that file into the personal sprint folder.

A document (in any standard format) detailing how IPv4 network addresses were established and how static routing tables were created.

Each team member must also commit to the personal sprint folder a text file with a configuration dump for every switch and every router within the encompassed building. These configuration text files can be easily exported in Packet Tracer: within the device's window click the **export** button on the **Running Config**, or the **Startup Config** (if the **Running Config** has been saved).

The default name for the text file maybe kept, as it represents the device's display name. During the sprint, members are to commit changes to these files as change are made to their devices' configurations, this allows the teacher to follow the progresses along the sprint. These files are also a safeguard, if somehow the configuration of a device in Packet Tracer is lost, it may be restored from these files.

For task **T.2.1** there is one additional output to be committed into the personal sprint folder, it's the overall simulation integrating all members work, that file should be named **campus.pkt**. Regarding configuration files, for task T.2.1, they only encompass devices in building A.

6. Per team specific data - mandatory use by teams

6.1. VLANIDs and VTP domain names

Class	Team number (within class)	VTP domain name to be used	VLANIDs range to be used
2DA	1	vtdag1	50 - 90
	2	vtdag2	60 - 100
	3	vtdag3	70 - 110
	4	vtdag4	80 - 120
	5	vtdag5	90 - 130
2DB	1	vtdbg1	100 - 140
	2	vtdbg2	110 - 150
	3	vtdbg3	120 - 160
	4	vtdbg4	130 - 170
	5	vtdbg5	140 - 180
2DC	1	vtdcg1	150 - 190
	2	vtdcg2	160 - 200
	3	vtdcg3	170 - 210
	4	vtdcg4	180 - 220
	5	vtdcg5	190 - 230
2DD	1	vtddg1	200 - 240
	2	vtddg2	210 - 250
	3	vtddg3	220 - 260
	4	vtddg4	230 - 270
	5	vtddg5	240 - 280
2DE	1	vtdeg1	250 - 290
	2	vtdeg2	260 - 300
	3	vtdeg3	270 - 310
	4	vtdeg4	280 - 320
	5	vtdeg5	290 - 330
2DF	1	vtdfg1	300 - 340
	2	vtdfg2	310 - 350
	3	vtdfg3	320 - 360
	4	vtdfg4	330 - 370
	5	vtdfg5	340 - 380
2DG	1	vtdgg1	350 - 390
	2	vtdgg2	360 - 400
	3	vtdgg3	370 - 410
	4	vtdgg4	380 - 420
	5	vtdgg5	390 - 430
2DH	1	vtdhg1	400 - 440
	2	vtdhg2	410 - 450
	3	vtdhg3	420 - 460
	4	vtdhg4	430 - 470
	5	vtdhg5	440 - 480
2DI	1	vtdig1	450 - 490
	2	vtdig2	460 - 500
	3	vtdig3	470 - 510
	4	vtdig4	480 - 520
	5	vtdig5	490 - 530
2DJ	1	vtdjg1	500 - 540
	2	vtdjg2	510 - 550
	3	vtdjg3	520 - 560
	4	vtdjg4	570 - 610
	5	vtdjg5	580 - 620
2DK	1	vtdkg1	590 - 630
	2	vtdkg2	600 - 640
	3	vtdkg3	610 - 650
	4	vtdkg4	620 - 660
	5	vtdkg5	630 - 670
2DL	1	vtdlg1	640 - 680
	2	vtdlg2	650 – 690
	3	vtdlg3	660 – 700
	4	vtdlg4	670 – 710
	5	vtdlg5	680 – 720

2NA	1	vtdbg1	690 -730
	2	vtnag2	700 – 740
	3	vtnag3	710 - 750
	4	vtnag4	720 – 760
	5	vtnag5	730 – 770
2NB	1	vtnbg1	740 – 780
	2	vtnbg2	750 – 790
	3	vtnbg3	760 – 800
	4	vtnbg4	770 - 810
	5	vtnbg5	780 - 820

6.2. IPv4 addresses to be used and ISP router IPv4 address

Class	Team number (within class)	IPv4 address space to be used (addresses block)	ISP router IPv4 node address
2DA	1	10.165.16.0/20	17.10.10.65/30
	2	10.165.32.0/20	17.10.10.70/30
	3	10.165.48.0/20	17.10.10.73/30
	4	10.165.64.0/20	17.10.10.77/30
	5	10.165.80.0/20	17.10.10.82/30
2DB	1	10.165.96.0/20	17.10.10.85/30
	2	10.165.112.0/20	17.10.10.89/30
	3	10.165.128.0/20	17.10.10.93/30
	4	10.165.144.0/20	17.10.10.98/30
	5	10.165.160.0/20	17.10.10.102/30
2DC	1	10.165.176.0/20	17.10.10.105/30
	2	10.165.192.0/20	17.10.10.109/30
	3	10.165.208.0/20	17.10.10.114/30
	4	10.165.224.0/20	17.10.10.117/30
	5	10.165.240.0/20	17.10.10.122/30
2DD	1	10.166.16.0/20	17.10.10.125/30
	2	10.166.32.0/20	17.10.10.129/30
	3	10.166.48.0/20	17.10.10.134/30
	4	10.166.64.0/20	17.10.10.137/30
	5	10.166.80.0/20	17.10.10.142/30
2DE	1	10.166.96.0/20	17.10.10.145/30
	2	10.166.112.0/20	17.10.10.149/30
	3	10.166.128.0/20	17.10.10.154/30
	4	10.166.144.0/20	17.10.10.157/30
	5	10.166.160.0/20	17.10.10.162/30
2DF	1	10.166.176.0/20	17.10.10.165/30
	2	10.166.192.0/20	17.10.10.169/30
	3	10.166.208.0/20	17.10.10.173/30
	4	10.166.224.0/20	17.10.10.178/30
	5	10.166.240.0/20	17.10.10.182/30
2DG	1	10.167.16.0/20	17.10.10.185/30
	2	10.167.32.0/20	17.10.10.190/30
	3	10.167.48.0/20	17.10.10.193/30
	4	10.167.64.0/20	17.10.10.197/30
	5	10.167.80.0/20	17.10.7.105/30
2DH	1	10.167.96.0/20	17.10.7.109/30
	2	10.167.112.0/20	17.10.7.113/30
	3	10.167.128.0/20	17.10.7.118/30
	4	10.167.144.0/20	17.10.7.122/30
	5	10.167.160.0/20	17.10.7.125/30
2DI	1	10.167.176.0/20	17.10.7.130/30
	2	10.167.192.0/20	17.10.7.133/30
	3	10.167.208.0/20	17.10.7.137/30
	4	10.167.224.0/20	17.10.7.142/30
	5	10.167.240.0/20	17.10.7.146/30
2DJ	1	10.168.16.0/20	17.10.7.149/30
	2	10.168.32.0/20	17.10.7.153/30
	3	10.168.48.0/20	17.10.7.157/30
	4	10.168.64.0/20	17.10.7.162/30
	5	10.168.80.0/20	17.10.7.165/30
2DK	1	10.168.96.0/20	17.10.7.169/30

	2	10.168.112.0/20	17.10.7.173/30
	3	10.168.128.0/20	17.10.7.177/30
	4	10.168.144.0/20	17.10.7.182/30
	5	10.168.160.0/20	17.10.7.185/30
2DL	1	10.168.176.0/20	17.10.7.190/30
	2	10.168.192.0/20	17.10.7.193/30
	3	10.168.208.0/20	17.10.7.197/30
	4	10.168.224.0/20	17.10.5.137/30
	5	10.168.240.0/20	17.10.5.142/30
2NA	1	10.169.16.0/20	17.10.5.145/30
	2	10.169.32.0/20	17.10.5.149/30
	3	10.169.48.0/20	17.10.5.154/30
	4	10.169.64.0/20	17.10.5.157/30
	5	10.169.80.0/20	17.10.5.161/30
2NB	1	10.169.96.0/20	17.10.5.165/30
	2	10.169.112.0/20	17.10.5.170/30
	3	10.169.128.0/20	17.10.5.173/30
	4	10.169.144.0/20	17.10.5.177/30
	5	10.169.160.0/20	17.10.5.181/30