

# Three-Building Network Design Documentation

Danielius Beržanskis

November 2025

## Contents

<b>1</b>	<b>Executive Summary</b>	<b>3</b>
<b>2</b>	<b>Network Topology Overview</b>	<b>3</b>
<b>3</b>	<b>Device Inventory</b>	<b>3</b>
3.1	Routers . . . . .	3
3.2	Layer 3 Switches . . . . .	4
3.2.1	SW-TTC . . . . .	4
3.2.2	SW-CC . . . . .	4
3.3	Access Switches . . . . .	4
3.4	Servers . . . . .	4
3.5	Cables . . . . .	4
<b>4</b>	<b>IPv4 Addressing Scheme</b>	<b>5</b>
4.1	Cyber security Learning center . . . . .	5
4.2	Main TTC building . . . . .	5
<b>5</b>	<b>IPv6 addressing</b>	<b>5</b>
5.1	Cyber security Learning center . . . . .	5
5.2	Main TTC building . . . . .	6
<b>6</b>	<b>VLAN Design and SVI placement</b>	<b>6</b>
6.1	Cyber Security Learning Center . . . . .	6
6.1.1	Vlan10 . . . . .	6
6.1.2	Vlan30 . . . . .	6
6.1.3	Vlan50 . . . . .	6
6.1.4	Vlan60 . . . . .	7
6.2	Main TTC building . . . . .	7
6.2.1	Vlan20 . . . . .	7
6.2.2	Vlan40 . . . . .	7
6.2.3	Vlan70 . . . . .	7

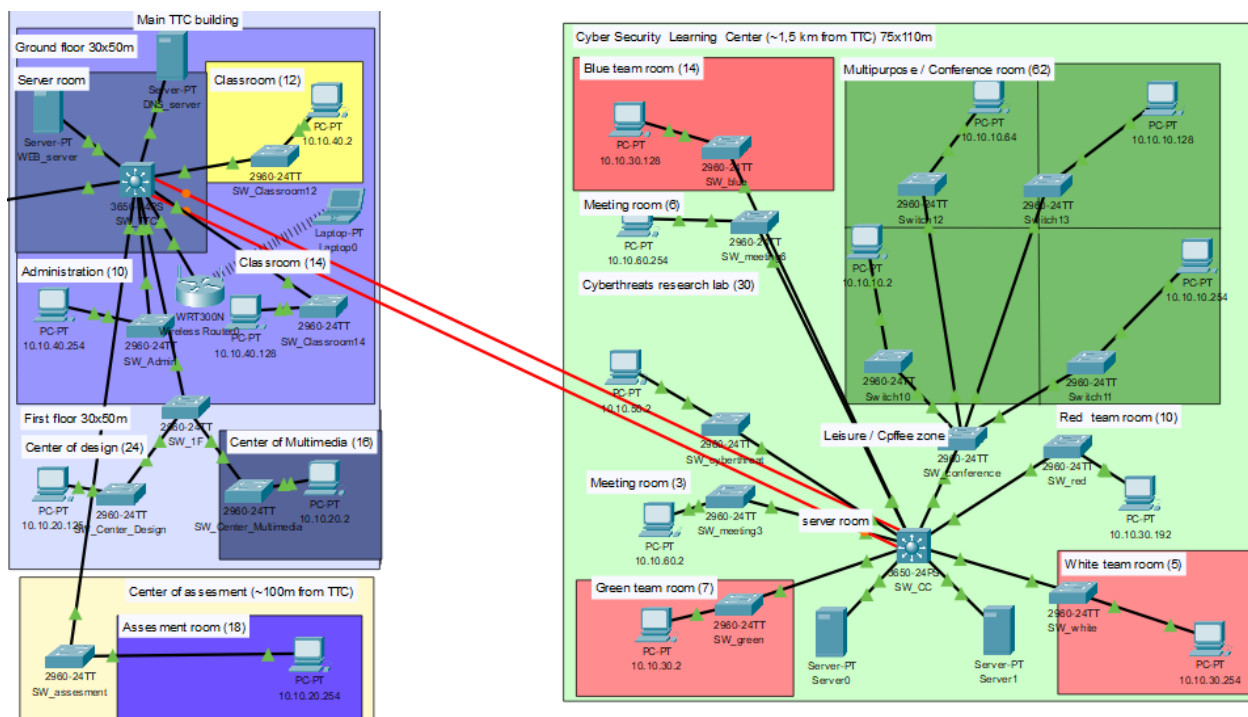
<b>7</b>	<b>Routing Configuration</b>	<b>8</b>
7.1	Default Routes . . . . .	8
7.2	OSPF . . . . .	8
<b>8</b>	<b>Access Control Lists (ACLs)</b>	<b>8</b>
<b>9</b>	<b>NAT Configuration</b>	<b>9</b>
9.1	PAT . . . . .	9
9.2	PAT translations . . . . .	10
9.2.1	ACL's used . . . . .	10
9.2.2	Address assignment . . . . .	10
<b>10</b>	<b>WIFI</b>	<b>10</b>
<b>11</b>	<b>Security Considerations</b>	<b>10</b>
11.1	Auto secure . . . . .	11

# 1 Executive Summary

This document outlines the design and implementation of a network spanning three buildings. It includes routing, switching, addressing, security, and server configurations using both IPv4 and IPv6.

## 2 Network Topology Overview

- Logical layout across three buildings
- **Core devices:** 1 router, 2 Layer 3 switches, multiple access switches
- Interconnection: fiber/copper links



## 3 Device Inventory

### 3.1 Routers

- **R-TTC** - Main router of the project. The only part that connects to the outside of the network. Has a configured PAT that takes private addresses and turns them into public ones.

## 3.2 Layer 3 Switches

### 3.2.1 SW-TTC

- Main layer 3 switch for the Main TTC building.
- Does all the routing via OSPF for Main TTC building
- has a default route for the main router
- Connects to Cyber Security Learning Center via EtherChannel
- Has SVI's for Main TTC building VLAN's
- Connects to all of the essential Main TTC building access switches

### 3.2.2 SW-CC

- Main layer 3 switch for the Cyber Security Learning Center.
- Does all the routing via OSPF for Cyber Security Learning Center
- has a default route for the SW-TTC
- Connects to Main TTC building via EtherChannel
- Has SVI's for Cyber Security Learning Center VLAN's
- Connects to all of the essential Cyber Security Learning Center access switches

## 3.3 Access Switches

- A total of 18 access switches (5 - Main TTC building, 1 - Center of assesment, 12 - Cyber Security Learning Center)

## 3.4 Servers

- **WEB server** - provides HTTP services to all users including both ipv4 and ipv6.
- **DNS server** - provides DNS services only for ipv6
- **Server0 and Server1** - showcase servers that have entire subnets dedicated to them for the 200 VM's each

## 3.5 Cables

- **Copper Straight-through cables** connect routers to L3 switches, then to access switches and then to PC.
- **Copper cross-over cables** connect routers to each other
- **2 fiber cables** connect L3 switches making it a EtherChannel. This is primarily done for speed as the buildings are 1,5 km apart

## 4 IPv4 Addressing Scheme

### 4.1 Cyber security Learning center

- **10.10.10.0/24** - Multipurpose / Conference room
- **10.10.30.10/24** - White, Red, Green, Blue teams rooms
- **10.10.50.10/24** - Cyberthreats research lab
- **10.10.60.0/24** - Meeting rooms
- **10.10.71.0/24** - **10.10.90.0/24** - 20 servers with 200 VM's each
- **10.255.255.2/24** - port channel connecting to SW-TTC

### 4.2 Main TTC building

- **10.10.20.0/24** - Center of design, Center of Multimedia, Center of Assessment
- **10.10.40.10/24** - Both classrooms and Administration
- **10.10.70.10/24** - Web server and DNS server
- **10.255.255.1/24** - Port-channel connecting to SW-CC
- **10.10.95.1/24** - connection to the WIFI router

## 5 IPv6 addressing

- As IPv6 has more addresses than IPv4 any form of NAT is not needed.
- DHCPv6 pools are created and SLAAC can be configured but due to Packet Tracer supporting IPv6 poorly static addressing method has been chosen
- **Network:** 2001:77c:fac1::/48

### 5.1 Cyber security Learning center

- **2001:77c:fac1:10::/64** - Multipurpose / Conference room
- **2001:77c:fac1:30::/64** - White, Red, Green and Blue teams rooms
- **2001:77c:fac1:50::/64** - Cyberthreats research lab
- **2001:77c:fac1:60::/64** - Meeting rooms
- **2001:77c:fac1:99::2/64** - Port-channel - connecting to SW-TTC

## 5.2 Main TTC building

- **2001:77c:fac1:20::/64** - Center of design, Center of Multimedia, Center of Assessment
- **2001:77c:fac1:40::/64** - Both classrooms and Administration
- **2001:77c:fac1:70::/64** - WEB server and DNS server
- **2001:77c:fac1:99::1/64** - Port-channel - connecting to SW-CC

## 6 VLAN Design and SVI placement

### 6.1 Cyber Security Learning Center

#### 6.1.1 Vlan10

- **Name** - conference
- **Rooms** - Multipurpose / Conference
- **IPv4 address** - 10.10.10.1/24
- **IPv6 address** - 2001:77c:fac1:10::1/64
- **DHCPv6 pool** - POOL-10

#### 6.1.2 Vlan30

- **Name** - colors
- **Rooms** - Red, Blue, White, Green team rooms
- **IPv4 address** - 10.10.30.1/24
- **IPv6 address** - 2001:77c:fac1:30::1/64
- **DHCPv6 pool** - POOL-30

#### 6.1.3 Vlan50

- **Name** - cybersecurity
- **Rooms** - Cyberthreats research lab
- **IPv4 address** - 10.10.50.1/24
- **IPv6 address** - 2001:77c:fac1:50::1/64
- **DHCPv6 pool** - POOL-50

#### **6.1.4 Vlan60**

- **Name** - meetings
- **Rooms** - Both the meeting rooms
- **IPv4 address** - 10.10.60.1/24
- **IPv6 address** - 2001:77c:fac1:60::1/64
- **DHCPv6 pool** - POOL-60

### **6.2 Main TTC building**

#### **6.2.1 Vlan20**

- **Name** - centers
- **Rooms** - Center of Design, Center of Multimedia, Center of Assesment
- **IPv4 address** - 10.10.20.1/24
- **IPv6 address** - 2001:77c:fac1:20::1/64
- **DHCPv6 pool** - POOL-20

#### **6.2.2 Vlan40**

- **Name** - classrooms
- **Rooms** - Both Classrooms and Administration
- **IPv4 address** - 10.10.40.1/24
- **IPv6 address** - 2001:77c:fac1:40::1/64
- **DHCPv6 pool** - POOL-40

#### **6.2.3 Vlan70**

- **Name** - management
- **Rooms** - Server room
- **IPv4 address** - 10.10.70.1/24
- **IPv6 address** - 2001:77c:fac1:70::1/64
- **DHCPv6 pool** - POOL-70

## 7 Routing Configuration

### 7.1 Default Routes

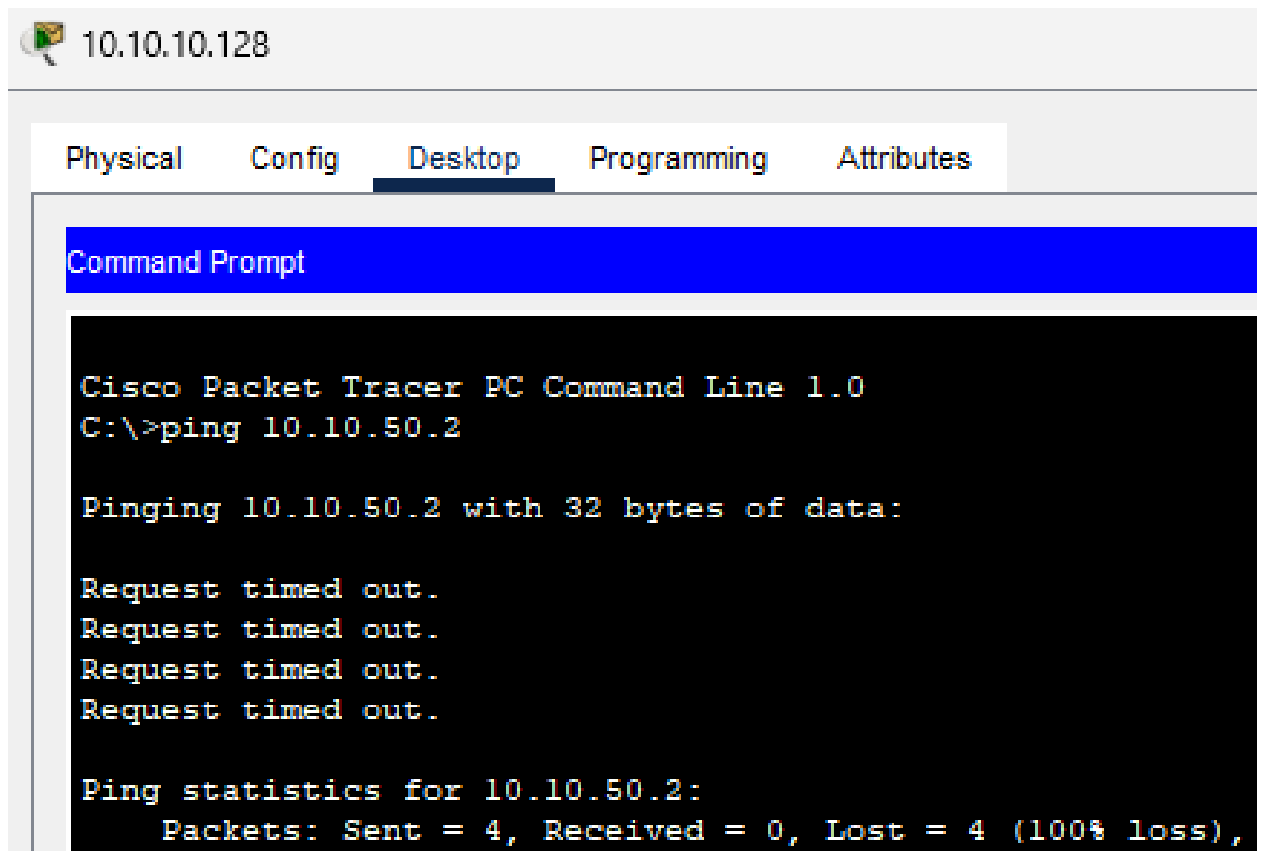
- The main router and both of the L3 switches have default static routes for accessing the internet.

### 7.2 OSPF

- The main router and both of the L3 switches have ospf enabled sharing their own networks to OSPF neighbors
- The area in which the network operates is 0

## 8 Access Control Lists (ACLs)

- The ACL's necessary for PAT creation are on R-TTC
- **ACL for limiting Cyberthreats access** - An ACL on SW-CC L3 switch that prevents unauthorized access to the cybersecurity VLAN. Only users from the management VLAN can access this VLAN
- Example of a fail:



The screenshot shows a PC configuration window in Cisco Packet Tracer. The IP address is 10.10.10.128. The 'Desktop' tab is selected, showing a 'Command Prompt' window. The command prompt displays the output of a ping command from C:\>ping 10.10.50.2. The output shows four 'Request timed out.' messages and a final summary: 'Ping statistics for 10.10.50.2: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),'. This indicates a complete failure to reach the destination IP.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.50.2

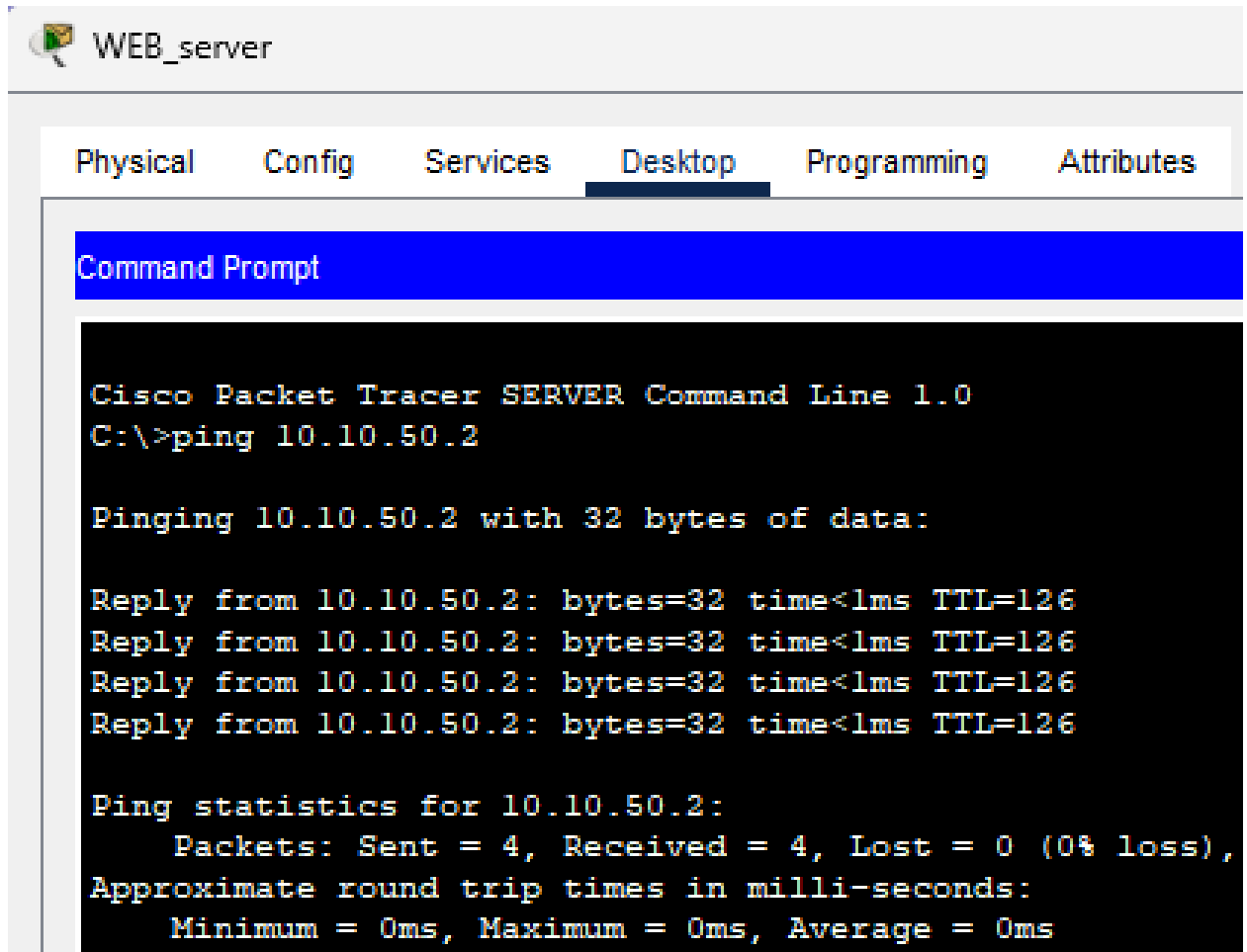
Pinging 10.10.50.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.10.50.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```



- Example of success:



The screenshot shows a Cisco Packet Tracer interface for a device named 'WEB\_server'. The 'Desktop' tab is selected, displaying a 'Command Prompt' window. The command prompt shows the execution of a ping command to 10.10.50.2, which was successful. The output includes the command line, the ping command, the data size, the number of replies, and the statistics for the ping.

```

Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 10.10.50.2

Pinging 10.10.50.2 with 32 bytes of data:

Reply from 10.10.50.2: bytes=32 time<1ms TTL=126
Reply from 10.10.50.2: bytes=32 time<1ms TTL=126
Reply from 10.10.50.2: bytes=32 time<1ms TTL=126
Reply from 10.10.50.2: bytes=32 time<1ms TTL=126

Ping statistics for 10.10.50.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

```

## 9 NAT Configuration

### 9.1 PAT

- PAT was chosen because the public network: 193.219.42.0/24 did not have enough addresses to support the required user amount
- PAT is done by the main router (R-TTC)
- The interface that connects to the L3 switch and all of the VLANs are configured with `ip nat inside`
- The interface that connects to the internet is configured with `ip nat outside`

## 9.2 PAT translations

### 9.2.1 ACL's used

- **ACL 10** permits VLAN 10
- **ACL 20** permits VLAN 20
- **ACL 30** permits VLAN 30
- **ACL 40** permits VLAN 40
- **ACL 50** permits VLAN 50
- **ACL 60** permits VLAN 60
- **ACL 70** permits VLAN 70

### 9.2.2 Address assignment

- 10.10.10.0/24 - 193.219.42.10
- 10.10.20.0/24 - 193.219.42.20
- 10.10.30.0/24 - 193.219.42.30
- 10.10.40.0/24 - 193.219.42.40
- 10.10.50.0/24 - 193.219.42.50
- 10.10.60.0/24 - 193.219.42.60
- 10.10.70.0/24 - 193.219.42.70

## 10 WIFI

- still under developement
- **WIFI** has been implemented on the first floor of Main TTC building allowing wireless connections
- **WIFI** assigns users their ip address from a pool of 10.10.96.0/24

## 11 Security Considerations

- **Cameras** can be easily implemented with a new VLAN
- **Redundancy and failover** can be implemented by configuring more L3 switches
- **WIFI** has a WPA2 Personal security mode enabled with a Passphrase of Danielius

## 11.1 Auto secure

`auto secure` has been implemented on the main router and the 2 L3 switches. The configurations are as follows:

- **Banner** - Authorized access only
- **Enable secret password** - Danielius
- **Local database user login** - Danielius with password of Danielius
- **Login via SSH** - user Danielius with domain name of Danielius.com
- **repeated login restrictions:**
  - Blocking Period when Login Attack detected - 60s
  - Maximum Login failures with the device - 5
  - Maximum time period for crossing the failed login attempts - 60s
- All other auto secure features