Three-Building Network Design Documentation

Danielius Beržanskis

November 2025

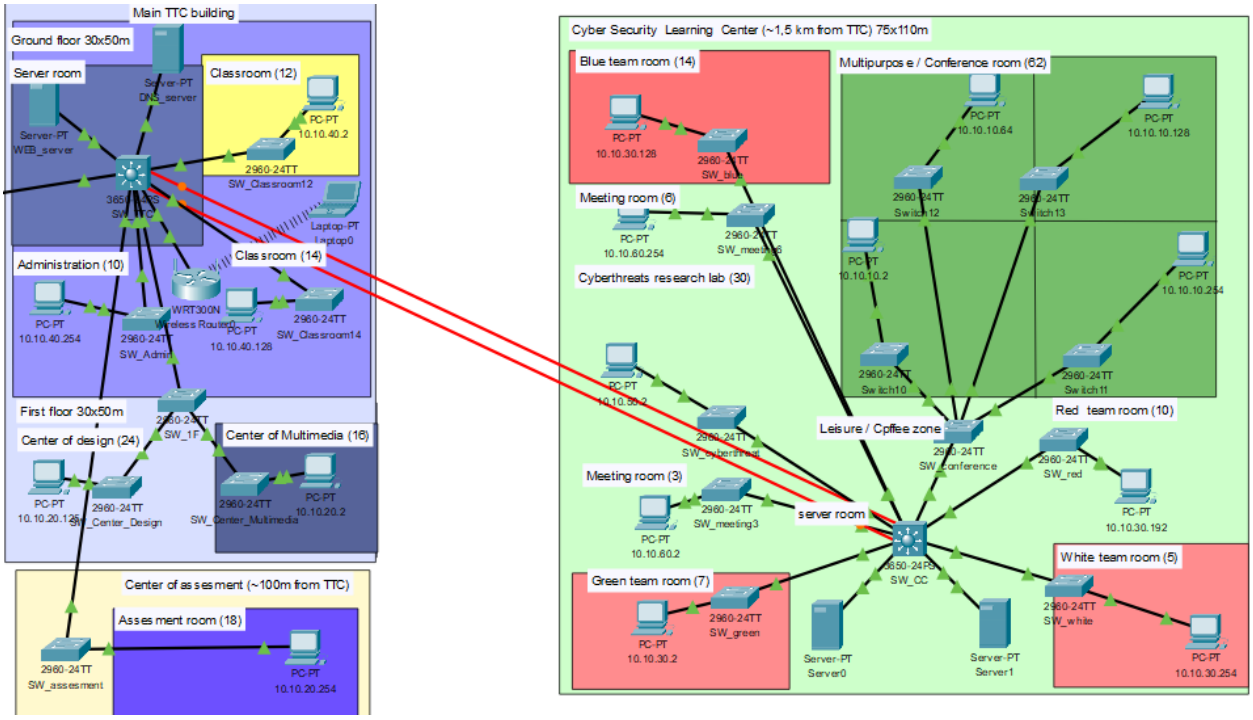
Contents

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.
- **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 Assesment
- **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 IPv6 DHCPv6 pools

- Both L3 switches act as independent stateless DHCPv6 servers with DNS of 2001:77C:FAC1:70::53

6.1 Cyber security Learning center

- **POOL-VLAN10** - 2001:77c:fac1:10::/64
- **POOL-VLAN30** - 2001:77c:fac1:30::/64
- **POOL-VLAN50** - 2001:77c:fac1:50::/64
- **POOL-VLAN60** - 2001:77c:fac1:60::/64

6.2 Main TTC building

- **POOL-VLAN20** - 2001:77C:FAC1:20::/64
- **POOL-VLAN40** - 2001:77c:fac1:40::/64
- **POOL-VLAN70** - 2001:77c:fac1:70::/64
- **POOL-VLAN60** - 2001:77c:fac1:60::/64

7 VLAN Design and SVI placement

7.1 Cyber Security Learning Center

7.1.1 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

7.1.2 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

7.1.3 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

7.1.4 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

7.2 Main TTC building

7.2.1 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

7.2.2 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

7.2.3 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

8 Routing Configuration

8.1 Default Routes

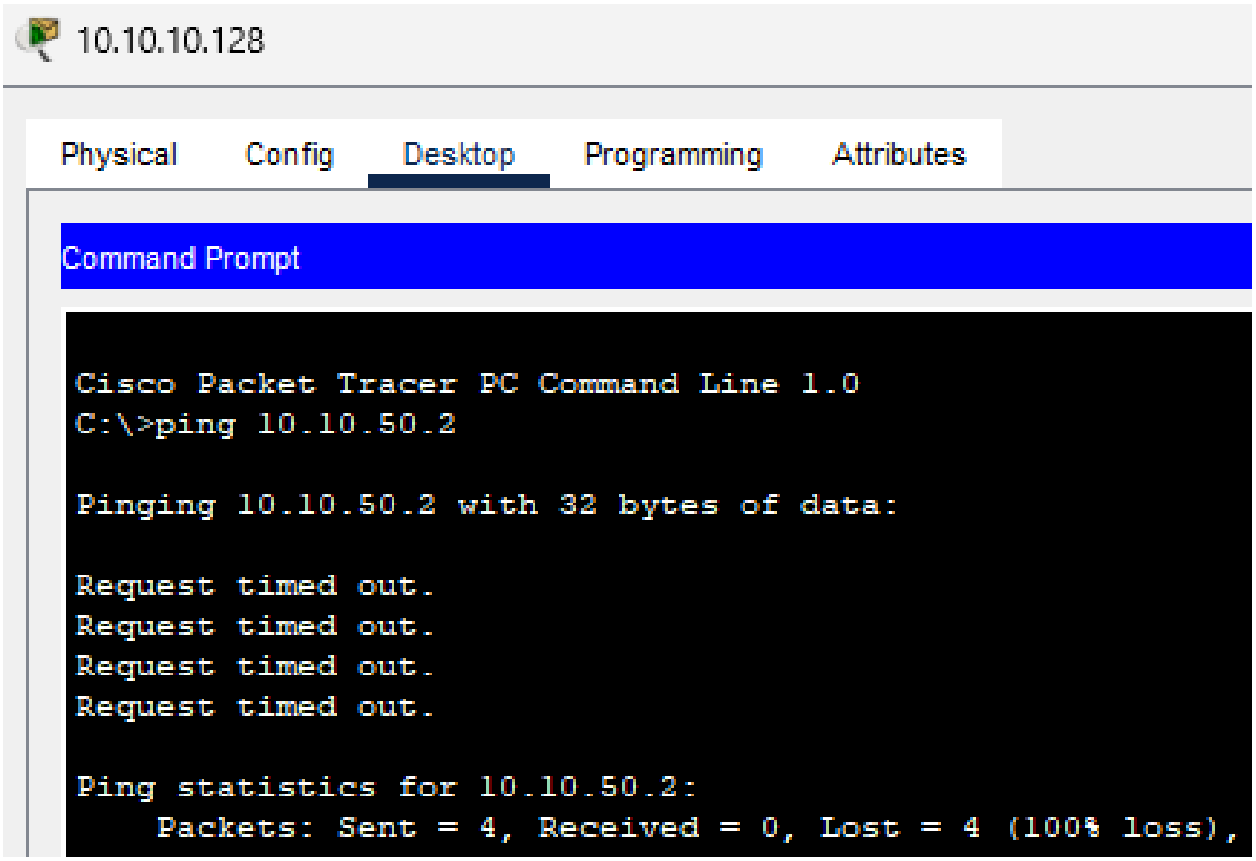
- The main router and both of the L3 switches have default static routes for accessing the internet.

8.2 OSPF

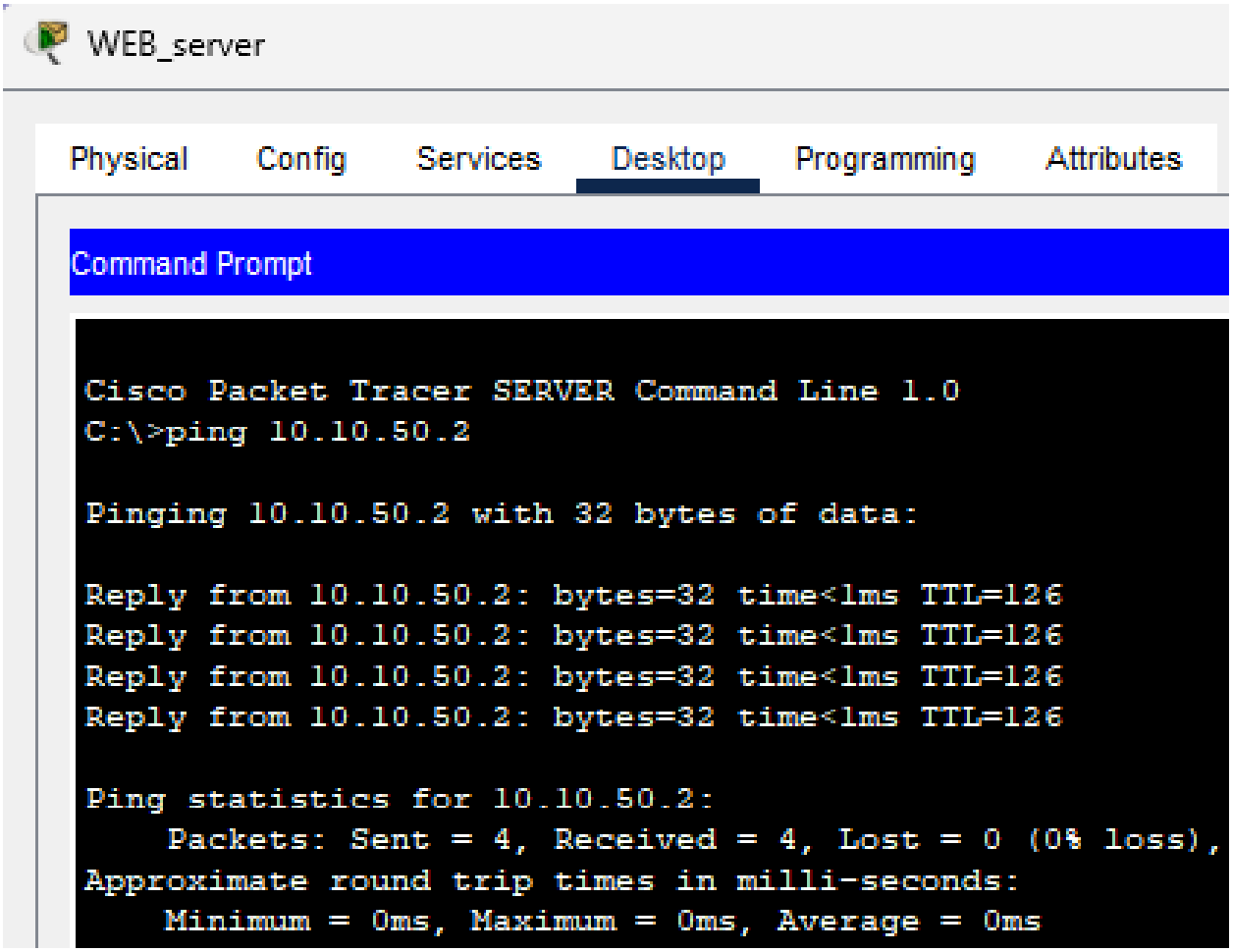
- The main router and both of the L3 switches have ospf enabled sharing their own networks to OSPF neighbors
- The area in which the network operates is 0

9 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:

- 

- Example of success:

- 

10 NAT Configuration

10.1 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`

10.2 PAT translations

10.2.1 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

10.2.2 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

11 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

12 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

12.1 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
- CBAC firewall feature
- All other auto secure features