DUAL-CAMPUS PACKET TRACER NETWORK – COMPREHENSIVE GUIDE

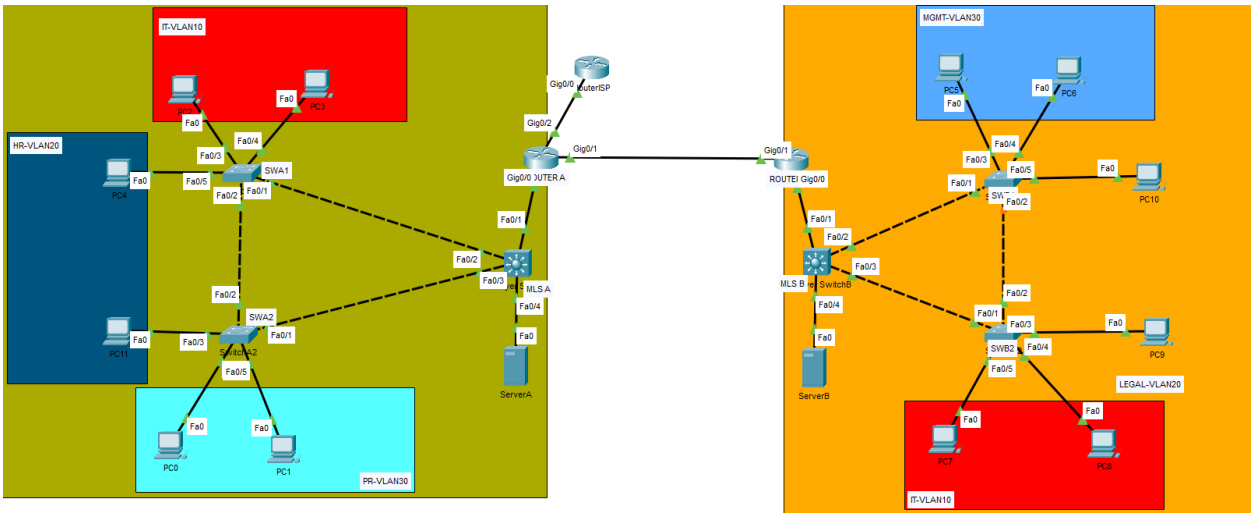
This **laboratory** presents a dual-campus network that mirrors the design principles used in contemporary enterprise environments. Campus A and Campus B are interconnected by a GRE tunnel which is subsequently secured with IPsec transport mode, ensuring confidentiality without sacrificing the flexibility of GRE encapsulation.

At the access layer, the topology showcases a disciplined Layer-2 architecture: Rapid-PVST+ provides sub-second convergence, the root-bridge role is placed deliberately, and PortFast combined with BPDU-Guard protects the edge from accidental loops. Up the stack, multilayer switches handle inter-VLAN routing and forward traffic over dedicated /30 point-to-point networks to their respective border routers. Static, summarised routes keep the control-plane simple and deterministic while still allowing complete reachability.

Beyond basic forwarding, the project integrates a full suite of enterprise services. DHCP pools deliver addresses to every VLAN, NAT overload translates private users to a public prefix, and static one-to-one mappings expose campus servers to the Internet. Granular ACLs enforce policy—blocking HR access to the management LAN, for example—while an SSH-only management plane is confined to the IT subnets, illustrating best-practice hardening.

A concise verification checklist accompanies the build; anyone who clones the repository can confirm every feature in under ten minutes. The lab is therefore ideal for **CCNA-level candidates** who want a compact yet realistic playground, as well as for seasoned engineers seeking a quick reference campus design.

1. Physical & Logical Topology



2. IP & VLAN Plan

2.1 User & Server Subnets

Campus	VLAN	Use-case	Subnet (/24)	Gateway
A	10	IT workstations	10.0.10.0	10.0.10.1
A	20	HR	10.0.20.0	10.0.20.1
A	30	PR	10.0.30.0	10.0.30.1
A	40	Servers-A	10.0.40.0	10.0.40.1
B	10	IT	10.1.10.0	10.1.10.1
B	20	Legal	10.1.20.0	10.1.20.1
B	30	Mgmt	10.1.30.0	10.1.30.1
B	40	Servers-B	10.1.40.0	10.1.40.1

2.2 Point-to-Point Links

Link	Subnet (/30)	Side A	Side B
MLS-A ↔ Router-A	10.0.254.0	10.0.254.1	10.0.254.2
MLS-B ↔ Router-B	10.1.254.0	10.1.254.1	10.1.254.2
Router-A ↔ Router-B	10.255.255.0	10.255.255.1	10.255.255.2
GRE Tunnel 1	50.50.50.0	50.50.50.1	50.50.50.2
Router-A ↔ ISP	203.0.113.0	203.0.113.2	203.0.113.1

3. Switching Design

The switching layer is engineered around four pivotal principles. First, every switch runs **Rapid-PVST+**, which guarantees sub-second convergence whenever a link or device fails. Second, we establish a deterministic spanning-tree hierarchy by electing **MLS-A as the primary root bridge** and **MLS-B as the secondary root bridge**; this choice keeps traffic on optimal paths even during fail-over. Third, all inter-switch links operate as **802.1Q trunks that carry VLAN 10, 20, 30 and 40 while using VLAN 1 as the native VLAN**, thus ensuring consistent tagging across the campus. Finally, every user-facing access port is configured with **PortFast and BPDU-Guard**, so edge devices come online instantly and any accidental loop is shut down before it can propagate.

4. Routing & Tunnelling

Inter-VLAN traffic remains local to each campus because **the multilayer switches perform Layer-3 routing via their SVIs and have ip routing enabled**. Each MLS connects to its border router through a dedicated **/30 point-to-point network**, which keeps the core free of VLAN tagging. We purposely avoid dynamic protocols and instead employ **summarised static routes** to maintain a deterministic and easily auditable control plane. To link the two campuses logically, we build a **GRE tunnel (Tunnel 1)** and then secure it with **IPsec in transport mode**, thereby achieving confidentiality without losing GRE's capability to carry routed traffic.

5. Enterprise Services

The laboratory hosts several production-style services. **Dedicated DHCP pools** on Server-A and Server-B assign addresses automatically to every user VLAN, while the SVIs provide the helper addresses. **Router-A implements PAT overload** so that all private hosts can reach the Internet, and it also provides **static one-to-one NAT** for the on-premises servers at 10.0.40.10 and 10.1.40.10. Secure administration is enforced through **SSH-only VTY lines, guarded by the IT-MGMT ACL**, which limits logins to the IT subnets. Finally, an extended ACL on MLS-B blocks any traffic originating from the HR segment (10.0.20.0/24) that attempts to reach the management network in Campus B (10.1.30.0/24), thereby demonstrating fine-grained segmentation.

6. Test Plan

The following sequence of tests proves the end-to-end functionality of the design:

1. **T1 – Local gateway reachability:** each PC pings its own default gateway (x.x.x.1) and must receive four successful replies.
2. **T2 – Inter-campus IT connectivity:** a PC in the IT subnet of Campus A (10.0.10.x) pings a PC in the IT subnet of Campus B (10.1.10.x); all packets should be echoed successfully.
3. **T3 – Policy enforcement:** a PC in the HR subnet (10.0.20.x) attempts to ping a host in the management subnet of Campus B (10.1.30.x) and must be blocked, confirming that the ACL is working.
4. **T4 – Secure management from IT:** an IT workstation establishes an SSH session to Router-A and should receive a login prompt, while an HR workstation performing the same action should be refused.
5. **T5 – Path visibility:** a traceroute 10.1.30.1 executed on Router-A must show hop 1 as 10.255.255.2 (Router-B) and hop 2 as 10.1.254.1 (MLS-B).
6. **T6 – IPsec operation:** the commands show crypto isakmp sa and show crypto ipsec sa on either router must display an active QM_IDLE state and increasing encapsulation counters.
7. **T7 – Internet connectivity:** any internal PC pings **8.8.8.8** successfully, and show ip nat translations on Router-A displays dynamic overload entries.

When all seven tests succeed, the lab is fully operational.