Traditional Networking vs Cisco ACI

Design Aspect	Traditional Network Design Details	Application-Centric Cisco ACI Design Details
1. Core	Build a robust, reachable L2/L3 network infrastructure first. Applications adapt to the available network segments and services.	Define application requirements first. The infrastructure automatically configures itself to meet those needs based on policy.
2. Fundamental Unit	VLANs & Subnets: Primary building blocks for segmentation and addressing. Policies tied to these constructs.	Endpoint Groups (EPGs): Logical grouping of endpoints (VMs, servers, containers) based on application function/tier (e.g., Web, App, DB). Policies are tied to EPGs.
3. Segmentation Design	VLANs (L2): Define broadcast domains. Often span multiple racks or rows. Requires Spanning Tree Protocol (STP) management. Subnets/VRFs (L3): Define routing domains, often mapped 1:1 with VLANs. Inter-VLAN routing needed.	Bridge Domains (BDs) & VRFs within Tenants: BDs provide L2 forwarding (can be flood or optimized). VRFs provide L3 isolation. Both are logical constructs mapped onto a VXLAN overlay, decoupled from physical topology. EPGs are mapped to BDs.
4. Security Policy Design	Access Control Lists (ACLs): Applied on router/switch interfaces (SVIs) or firewalls. Based on IP addresses, ports, protocols. Typically a "permit" model (allow specific traffic, implicit/explicit deny). Focus on north-south and inter-zone traffic.	Contracts: Define communication rules between EPGs. Specify Provider/Consumer EPGs and Filters (ports/protocols). Enforced by leaf switches. Whitelist model (deny by default, permit via contract). Enables micro-segmentation easily.
5. Addressing & Forwarding	Manual IP planning per subnet/VLAN. Routing protocols (OSPF, BGP, etc.) configured on L3 devices. STP manages L2 loops. ARP used for L2 resolution within VLANs.	IP addresses assigned to endpoints, but policy is not primarily based on them. ACI fabric uses an underlay routing protocol (IS-IS) and a VXLAN overlay. A mapping database tracks endpoint locations (IP/MAC -> Leaf/VXLAN Tunnel Endpoint). BDs handle L2 forwarding (ARP suppression optional). VRFs handle L3 routing within the fabric.
6. Service Insertion (Firewalls, Load Balancers)	Traffic manually steered to physical/virtual appliances using Policy-Based Routing (PBR), VRF stitching, or VLAN redirection. Complex cabling and configuration.	Service Graphs: Define L4-L7 service insertion chains via the APIC. Traffic is automatically redirected through service devices (physical or virtual) based on policy, without complex manual routing changes. Can be managed or unmanaged devices.
7. Provisioning Workflow	1. Application team requests ports/connectivity. 2. Network team identifies/creates VLANs & Subnets. 3. Configure switch ports (access/trunk). 4. Configure SVIs/router interfaces. 5. Update 6. Configure ACLs/Firewall rules. (Often manual CLI/GUI per device).	1. Define Application Profile, EPGs, Contracts in APIC. 2. Associate EPGs with VMM domains (like vCenter) or physical ports. 3. APIC automatically configures leaf switch ports, VXLAN, policies. 4. (Optional) Integrate L4-L7 via Service Graphs. (Centralized GUI or API).
8. Automation & Orchestration	Limited built-in automation. Relies on scripting (Python, Ansible) or external NMS/automation tools targeting individual device CLIs/APIs.	Built-in controller (APIC) provides central automation point. Rich REST API allows integration with higher-level orchestration tools (vRealize, Terraform, CloudForms, Ansible ACI Modules).
9. Scalability Considerations	STP limitations (blocked links, convergence time). Large routing tables. Complex ACL management. Manual configuration overhead limits operational scale.	Spine-Leaf Clos fabric provides predictable high bandwidth and low latency. VXLAN overlay scales endpoint mobility. Centralized policy management scales operations. Avoids STP.
10. Visibility & Troubleshooting	Device-centric. Use ping, traceroute, show commands (ARP, MAC, routes, interface counters, ACL hits) on individual devices. Correlation across devices is manual.	Centralized visibility via APIC: Health Scores (fabric, tenants, apps), Endpoint Tracker, Policy Verification tools, Atomic Counters (for traffic verification per policy rule), Fault monitoring. Both logical (policy) and physical (fabric) views.
11. Required Skillset	Deep L2/L3 protocols, STP, routing (OSPF, BGP), vendor CLI, firewall policy syntax.	Core networking concepts + ACI policy model (EPG, Contract, etc.), APIC operation, VXLAN fundamentals, API usage, integration points (VMM, L4-L7), potentially automation tools.

tomislavk.blog