VLAN Planning Worksheet

VLAN architecture with subnet allocation, ACLs, port assignments, and security policies. Plan your network segmentation with this structured worksheet.

8	Segment	ACL	Free
COMMON VLANS	TRAFFIC FOR SECURITY	CONTROL BETWEEN VLANS	PLANNING TOOL

How to Use This Worksheet

Use this worksheet to plan VLAN architecture for a new network or to document and improve an existing setup. Complete each section to create a comprehensive VLAN design that supports security, performance, and manageability.

1 VLAN Architecture Plan

Define each VLAN with its purpose, subnet, and security requirements.

VLAN ID	NAME	SUBNET	MASK				
1	Management	10.0.1.0	/24	10.0.1.1	Static	Static	Network device management
10	Servers	10.0.10.0	/24	10.0.10.1	Static	Static	Production servers
20	Corporate	10.0.20.0	/24	10.0.20.1	10.0.20.100	10.0.20.250	Staff workstations
30	VoIP	10.0.30.0	/24	10.0.30.1	10.0.30.100	10.0.30.250	IP phones (QoS tagged)
40	Wireless	10.0.40.0	/24	10.0.40.1	10.0.40.50	10.0.40.250	Corporate WiFi clients
50	IoT	10.0.50.0	/24	10.0.50.1	10.0.50.50	10.0.50.250	Printers, cameras, smart devices
60	Development	10.0.60.0	/24	10.0.60.1	10.0.60.50	10.0.60.200	Dev/test environment
99	Guest	10.0.99.0	/24	10.0.99.1	10.0.99.50	10.0.99.200	Guest WiFi (internet only)

2 Inter-VLAN Access Control

Define which VLANs can communicate with each other and what traffic is permitted.

SOURCE VLAN	DESTINATION VLAN	PERMITTED TRAFFIC	DENIED TRAFFIC	
Corporate (20)	Servers (10)	HTTP/HTTPS, SMB, RDP	All other	Application & file access
Corporate (20)	VoIP (30)	None	All	Voice traffic isolated
Corporate (20)	Guest (99)	None	All	Guest isolation
VoIP (30)	Servers (10)	SIP (5060-5061)	All other	Phone system server
Guest (99)	Any internal	None	All	Complete isolation
IoT (50)	Servers (10)	HTTPS (443) to print server	All other	Print job submission
Management (1)	All VLANs	SSH, SNMP, HTTPS	N/A	Management access

Guest VLAN Isolation

The guest VLAN must have zero access to any internal VLAN. Verify this with regular penetration testing. Guest traffic should route directly to the internet via the firewall without touching internal infrastructure.

3 Switch Port Assignments

Document which switch ports are assigned to which VLANs.

SWITCH	PORT RANGE	MODE	VLAN(S)		
Core-SW1	1–2	Trunk	All	Uplinks to firewall	Server room
Core-SW1	3–4	Trunk	All	Uplinks to access switches	Server room
Core-SW1	5–24	Access	10	Server connections	Server room
Acc-SW1	1–2	Trunk	All	Uplink to core switch	Floor 1 comms cab
Acc-SW1	3–24	Access	20	Workstation ports	Floor 1
Acc-SW1	25–36	Access	30	VoIP phone ports	Floor 1
Acc-SW1	37–48	Access	50	Printer/IoT ports	Floor 1

4 QoS & Traffic Prioritisation

Define Quality of Service policies for each VLAN to prioritise critical traffic.

VLAN	TRAFFIC TYPE	DSCP MARKING	PRIORITY QUEUE	
VoIP (30)	Voice traffic	EF (46)	Strict Priority	30% minimum
VoIP (30)	Call signalling	CS3 (24)	Priority	5% minimum
Corporate (20)	Business apps	AF31 (26)	Assured Forwarding	25% minimum
Corporate (20)	General web	CS0 (0)	Best Effort	Remaining bandwidth
Guest (99)	All traffic	CS0 (0)	Best Effort	Rate limited to 10 Mbps per user
IoT (50)	All traffic	CS0 (0)	Best Effort	Rate limited to 5 Mbps per device

QoS for Voice

VoIP traffic requires low latency (<150ms), low jitter (<30ms), and minimal packet loss (<1%). Mark voice traffic with DSCP EF and place it in a strict priority queue to ensure call quality. Configure trust boundaries at the access switch port connected to IP phones.

Notes

Need VLAN Architecture Design?

Our network engineers can design and implement a VLAN architecture tailored to your security and performance requirements.

info@cloudswitched.com
New London House, 6 London St, London EC3R

Prepared by: ____________________________ Date: ____________________________ Approved by: ____________________________