CLOUDSWITCHED

FREE RESOURCE — NETWORK PLANNING WORKSHEET

VLAN Planning Worksheet

Plan your VLAN architecture with subnet allocation, inter-VLAN ACLs, switch port assignments and QoS marking — in one structured worksheet. Use it for a green-field design, a refresh or to document and rationalise an existing setup. Fillable in any modern PDF viewer.

4	50+	A4	Free
PLANNING SECTIONS	FILLABLE CELLS	PRINT & RUNBOOK READY	TYPE & TICK IN ANY VIEWER

SUBNETS & DHCP · INTER-VLAN ACLS · PORT ASSIGNMENTS · QOS & DSCP

PREPARED FOR	PREPARED BY	VERSION	FORMAT
Cloudswitched Knowledge Library	Cloudswitched Ltd.	2026 Edition	Planning Worksheet

00

How to use this worksheet

Use this worksheet to plan VLAN architecture for a **new network**, or to document and rationalise an **existing** one. Complete each section in order — the VLAN table on the next page is the source of truth that the later inter-VLAN ACL, port assignment and QoS sections all reference back to.

The four sections together give you a complete segmentation design that supports **security, performance and manageability**: who lives in which subnet, who can talk to whom, where each VLAN terminates on the switch fabric, and which traffic gets priority on a congested link.

WHAT THIS WORKSHEET IS

A structured snapshot of your VLAN segmentation plan — the artefact your network engineer, a new MSP, an auditor or an incident responder needs on day one. Pair it with the Cloudswitched Network Documentation Template and Network Security Audit Checklist for a full review cycle.

COMMON PITFALLS TO AVOID

Leaving the **native VLAN as VLAN 1** (it should be unused or moved). Forgetting to **default-deny** back from guest and IoT VLANs to corporate. Marking VoIP with **DSCP EF** but not extending the trust boundary down to the phone port. Documenting a VLAN here that **does not exist on the switch** — or worse, a VLAN on the switch that nobody documented.

The four planning sections

- **01 VLAN Architecture Plan** — VLAN ID, name, subnet, mask, gateway, DHCP scope, purpose.
- **02 Inter-VLAN Access Control** — which VLANs can reach which, what traffic is permitted, justification.
- **03 Switch Port Assignments** — trunk and access ports per switch, with location.
- **04 QoS & Traffic Prioritisation** — DSCP marking, priority queues, bandwidth guarantees.

COMMON UK SME VLAN STARTER SET

A reasonable starting layout: **Management (1)**, **Servers (10)**, **Corporate (20)**, **VoIP (30)**, **Wireless (40)**, **IoT (50)**, **Development (60)**, **Guest (99)**. The first row of the table on the next page is pre-filled with this pattern as an example — overwrite or extend as your environment requires.

01

VLAN Architecture Plan

Define every VLAN with its **ID, name, subnet, mask, gateway, DHCP scope** and **purpose**. The first eight rows show a common UK SME starter pattern — overwrite the example IDs and addresses to match your environment, then add rows for any extra segments.

VLAN ID	NAME	SUBNET	MASK	GATEWAY	DHCP START	DHCP END	PURPOSE
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	.100	.250	Staff workstations
30	**VoIP**	10.0.30.0	/24	10.0.30.1	.100	.250	IP phones (QoS tagged)
40	**Wireless**	10.0.40.0	/24	10.0.40.1	.50	.250	Corporate WiFi clients
50	**IoT**	10.0.50.0	/24	10.0.50.1	.50	.250	Printers, cameras, smart devices
60	**Development**	10.0.60.0	/24	10.0.60.1	.50	.200	Dev / test environment
99	**Guest**	10.0.99.0	/24	10.0.99.1	.50	.200	Guest WiFi (internet only)

SEGMENTATION POLICY

Inter-VLAN routing performed by *(firewall / L3 switch)* _____

Native VLAN moved off VLAN 1 ☐ Yes ☐ No

Voice and data VLANs separated ☐ Yes ☐ No

Guest VLAN fully isolated from corporate ☐ Yes ☐ No

02

Inter-VLAN Access Control

Define which VLANs can communicate with each other and what traffic is permitted. Adopt a **default-deny** posture: list the explicit allows here, and let everything else fall through to deny on the firewall or L3 switch.

SOURCE VLAN	DESTINATION VLAN	PERMITTED TRAFFIC	DENIED TRAFFIC	JUSTIFICATION
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`	All other	Print job submission
Management (1)	**All VLANs**	`SSH, SNMP, HTTPS`	N/A	Management access
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____

POLICY VERIFICATION

Default-deny enforced between VLANs ☐ Yes ☐ No ☐ Partial

Guest isolation verified by penetration test ☐ Yes ☐ No

Management plane restricted to jump-host(s) ☐ Yes ☐ No

ACL change-control owner _____

GUEST VLAN ISOLATION

The guest VLAN must have **zero** access to any internal VLAN. Verify this with regular penetration testing — do not assume the firewall config matches the design. Guest traffic should route directly to the internet via the firewall without touching internal infrastructure, internal DNS or domain controllers.

03

Switch Port Assignments

Document which switch ports are assigned to which VLANs, the mode (trunk or access) and the physical location of the patch panel. This is the bridge between the design above and the actual cabling on the floor.

SWITCH	PORT RANGE	MODE	VLAN(S)	DESCRIPTION	LOCATION
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
_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____

TRUNK & ACCESS HYGIENE

Allowed-VLAN list pruned on every trunk ☐ Yes ☐ No

Unused access ports administratively shut ☐ Yes ☐ No

DTP disabled / switchport mode hard-set ☐ Yes ☐ No

Voice VLAN tagged on access port for IP phones ☐ Yes ☐ No ☐ N/A

04

QoS & Traffic Prioritisation

Define Quality of Service policies for each VLAN to prioritise critical traffic on congested links. Mark at the access edge, trust through the core, and reserve a strict-priority queue for voice.

VLAN	TRAFFIC TYPE	DSCP MARKING	PRIORITY QUEUE	BANDWIDTH GUARANTEE
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 10 Mbps/user
IoT (50)	All traffic	`CS0 (0)`	Best effort	Rate-limited 5 Mbps/device
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____

VOICE QUALITY CONTROLS

Trust boundary set at IP phone access port ☐ `Yes` ☐ `No`

DSCP-to-CoS mapping consistent end-to-end ☐ `Yes` ☐ `No`

Voice quality monitoring in place *(MOS / latency probes)* ☐ `Yes` ☐ `No`

Target voice path: latency < 150 ms, jitter < 30 ms, loss < 1% ☐ `Meeting target` ☐ `Drifting`

QOS FOR VOICE

VoIP needs low latency (<150 ms), low jitter (<30 ms) and minimal packet loss (<1%). Mark voice with **DSCP EF** and place it in a **strict priority queue** to protect call quality. Configure trust boundaries at the access switch port connected to IP phones — do **not** trust DSCP arriving on a corporate workstation port.

05

Sign-off & Next Steps

Capture the top priority actions that come out of this plan and the people who own them. Three is enough — if the list runs longer, you have a programme, not a punch list. Pair this with a follow-up review date so the design does not drift from reality.

Top 3 priority actions

01 _____

02 _____

03 _____

Additional notes

_____

_____

_____

_____

Sign-off

PREPARED BY _____ DATE _____ APPROVED BY _____

Need VLAN architecture design?

Our network engineers can design and implement a VLAN architecture tailored to your security, voice quality and performance requirements — fixed price, fixed window.

info@cloudswitched.com

cloudswitched.com/solutions/cloud-networking

CLOUDSWITCHED

CLOUD NETWORKING & IT INFRASTRUCTURE

info@cloudswitched.com

New London House, 6 London St
London EC3R 7LP · United Kingdom