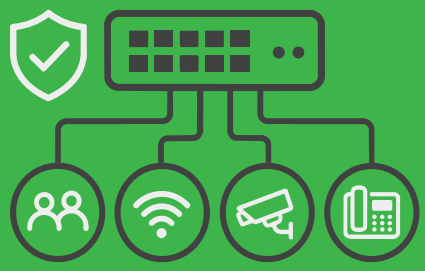
DUXNET

Best Practice Guide to VLANs & Network Segmentation

One network. Different jobs. Keep them separate.



WHY NETWORK SEGMENTATION MATTERS

A flat network may be quick to set up, but it becomes harder to manage as more users, devices and applications are added.

Staff computers, guest Wi-Fi, CCTV cameras, VoIP phones, access control, IoT devices and network management do not all need the same access. Putting everything on one network can make troubleshooting harder, increase unnecessary traffic and give devices access to parts of the network they do not need.

VLANs allow you to separate different types of traffic logically while still using the same switching infrastructure.

Good segmentation makes it easier to:

- Control which devices can communicate
- Isolate guest and untrusted traffic
- Troubleshoot network problems
- Apply different policies to different device groups
- Manage growing networks more consistently

Remember: Creating a VLAN is only part of the job. Routing and access rules determine what traffic is allowed between networks.

QUICK NETWORK SEGMENTATION REFERENCE

Use this as a practical starting point during presales, design and deployment.

Network Scenario	Segmentation Focus	Common Mistake to Avoid
Small office	Staff | Guest | Management	Putting everything on one flat network
Retail or hospitality	Business systems | Staff | Guest | CCTV/IoT	Allowing guest or IoT devices to reach systems
School or campus	Staff | Students | Guest | CCTV | Voice	Giving every user and device network access
CCTV deployment	Cameras | Recorders | Management	Mixing surveillance traffic with normal devices
VoIP deployment	Voice | Data	Adding phones without planning VLAN & network
Multi-site network	Standardised VLAN structure & naming	Using different VLAN plans with no documentation

WHAT CAUSES VLAN AND SEGMENTATION PROBLEMS?

VLANs are simple in principle, but small configuration differences can cause large connectivity problems.

Common causes include:

- Creating the VLAN on one switch but not across the full network path
- Incorrect tagged, untagged or port VLAN settings
- Uplinks that are not carrying the required VLAN
- Devices receiving an IP address from the wrong subnet
- Missing or incorrect DHCP configuration
- SSIDs mapped to the wrong VLAN
- Inter-VLAN routing that is either too open or too restrictive
- Management traffic mixed with normal user traffic
- Different VLAN numbering or naming across sites
- Configuration changes that are not documented

Do not troubleshoot the endpoint until you have checked the path. One incorrect port, uplink or VLAN setting can affect an entire group of users.

PRE-DEPLOYMENT CHECKLIST

Before creating VLANs, confirm:

- Which users and devices need to be separated
- Which networks need to communicate with each other
- Which networks must remain isolated
- VLAN names and IDs
- IP subnet and gateway for each VLAN
- DHCP requirements for each network
- Which ports will connect to end devices
- Which uplinks need to carry multiple VLANs
- SSID-to-VLAN requirements for wireless networks
- Router or firewall requirements for traffic between VLANs
- How switches and other network devices will be managed
- Whether the same VLAN structure will be used across multiple sites

Plan the segmentation before configuring the switch. A simple network diagram and VLAN table created before deployment can prevent hours of fault-finding later.

VLAN & SEGMENTATION BEST PRACTICES

1. Segment by function

Create VLANs for a clear operational reason, not simply because the switch supports them. Group devices according to what they do and what they need to access. Staff, guests, CCTV, voice, IoT and network management should be treated as separate requirements.

2. Keep guest traffic away from internal resources

Guest Wi-Fi should provide internet access without exposing internal systems, printers, cameras or business devices. Always confirm that guest isolation works after deployment.

3. Protect network management

Switches, access points and other infrastructure should not be managed from every user network. Where appropriate, use a dedicated management network and restrict access to device management interfaces.

4. Plan VLANs end to end

A VLAN must work across the complete path between the endpoint and the services it needs. Check every switch, uplink, access point, router and firewall involved. A correct setting on one device does not fix an incorrect setting elsewhere.

5. Control traffic between VLANs

Segmentation does not automatically mean isolation. If VLANs communicate through a router or firewall, define the required traffic and allow only what the application needs.

6. Standardise your design

Where possible, use consistent naming, VLAN structures and configuration standards across similar customer sites. Standardisation makes installations easier to understand, document and support.

7. Document everything

Record the VLAN name and ID, subnet and gateway, DHCP scope, purpose, tagged and untagged ports, uplink requirements, SSID mappings and inter-VLAN access requirements. A VLAN called “30” tells the next technician very little. “CCTV – VLAN 30 – 192.168.x.x/24” gives useful context.

8. Test before handover

Do not stop when devices receive an IP address. From each VLAN, confirm that users and devices receive the correct IP information, reach their gateway, reach the required services, cannot reach restricted networks, and have DNS and internet access where required.

Segmentation is only useful if it works as designed.

PRO INSTALLER TIPS

- Give VLANs clear names based on their purpose
- Keep the design as simple as the network allows
- Avoid carrying unnecessary VLANs across every uplink
- Confirm SSID-to-VLAN mappings on wireless deployments
- Check port settings before replacing hardware
- Test from an actual endpoint on each VLAN
- Save a working configuration after commissioning
- Document changes when VLANs are added later
- When changing management VLANs remotely, make sure you have a recovery plan if access is lost
- Do not assume that VLAN separation alone replaces firewall or access-control policies

BASIC VLAN FAULT-FINDING FLOW
DEVICE ON THE WRONG NETWORK OR NOT CONNECTING?

Before blaming the switch, AP or endpoint:

1. Check the endpoint port
Confirm that the port is assigned to the correct VLAN.

2. Check the VLAN path
Confirm that the required VLAN exists across every switch between the device and its gateway.

3. Check uplink configuration
Verify that the VLAN is correctly carried across the required uplinks.

4. Check IP addressing
Confirm that the device receives an IP address, subnet and gateway from the correct network.

5. Check the gateway
Test connectivity between the device and its VLAN gateway.

6. Check routing and access rules
If the device can reach its gateway but not another network, review routing, firewall or access-control rules.

7. Check the application
Once network connectivity is confirmed, move on to DNS, internet access or the specific service being used.

In many cases, a VLAN problem is a configuration mismatch somewhere along the path — not a hardware failure.

REALITY CHECK

Many networks start small and grow over time.

A guest Wi-Fi network is added. Then cameras. Then VoIP. Then access control, IoT devices and more users.

If everything keeps being added to the same network, the environment becomes increasingly difficult to control and support.

Good segmentation introduces structure before growth becomes a problem.

A FLAT NETWORK IS EASY TO BUILD.
A STRUCTURED NETWORK IS EASIER TO MANAGE.

LET DUXNET SIMPLIFY AP DEPLOYMENT

Good network segmentation starts before the first VLAN is created.

Duxbury Networking can assist resellers with switch selection, network planning and practical pre-deployment guidance to help build networks that are easier to install, manage and support.

Speak to our team for guidance on planning the right network structure for your deployment.