Network approaches for offices, plants, and mixed environments compared

Why one network design does not fit every space

An office, a factory floor, and a site that holds both have very different demands on the network that connects them. In an office, the main concerns are speed for cloud applications, reliable Wi-Fi for many users, and strong access controls to keep sensitive data inside the right departments. On a plant floor, the network might connect programmable logic controllers, robotic arms, and sensors that report temperature or vibration in real time. The traffic patterns are different, the tolerance for latency is lower, and the devices often run for years without an update. A mixed environment, say, a warehouse with an attached office block, has to satisfy both sets of needs without letting one side compromise the other.

Choosing the right segmentation approach for these settings is not a one-size-fits-all decision. It depends on what you are protecting, how much traffic moves between zones, and whether your priority is compliance, operational uptime, or both. This article lays out the main segmentation strategies and explains where each one fits best, so you can talk through your options with a network architecture consultant and make an informed choice for your own site.

Flat networks and why they cause trouble

A flat network puts every device, workstation, server, printer, controller, camera, on the same subnet. It is simple to set up, and in a small office with a handful of devices it can work fine. But as the environment grows, the problems multiply. Broadcast traffic from one device reaches every other device, which wastes bandwidth. A malware infection on a single workstation can spread laterally to the file server, the backup system, and any connected plant equipment. In a mixed environment, a flat network is especially dangerous because an office PC that gets compromised can reach the programmable logic controller that runs a conveyor belt. That is the kind of scenario that keeps plant managers up at night.

Flat networks also make it hard to enforce compliance with standards such as PCI DSS or NIST SP 800-82. Auditors look for clear separation between systems that handle sensitive data and systems that do not. Without segmentation, you cannot show that separation exists, and you may have to treat the entire network as a single high-risk zone.

VLANs: the workhorse of logical segmentation

A virtual local area network (VLAN) lets you split a single physical switch into multiple logical networks. Devices on different VLANs cannot talk to each other unless a router or a layer-3

switch explicitly allows it. VLANs are cheap to implement, they require managed switches and a bit of configuration, and they scale well. In an office, you might put the finance team on VLAN 10, HR on VLAN 20, and guest Wi-Fi on VLAN 30. In a plant, you could put the robotic controllers on VLAN 100, the quality inspection cameras on VLAN 110, and the environmental monitoring sensors on VLAN 120.

The key advantage of VLANs is that they enforce separation without needing separate physical cables and switches. That saves money and makes changes easier: you can reassign a device to a different VLAN from the management console instead of pulling cables. The trade-off is that VLANs rely on correct configuration. A misconfigured trunk port or a forgotten routing rule can open a hole between segments, so you need someone who understands switch administration and can audit the setup regularly. For a mixed environment, VLANs are often the first tool an IT or OT consultant reaches for because they give you granular control without a forklift upgrade.

Physical separation: air gaps and dedicated infrastructure

Sometimes logical separation is not enough. Environments that handle classified data, legacy industrial systems that cannot be patched, or safety-critical control loops sometimes use physical separation. An air gap means the two networks have no physical connection at all, no cable, no wireless link, no shared switch. Data can move between them only by removable media or by a human who copies it from one system to the other. That is the most secure arrangement possible, but it is also the most inconvenient. In practice, true air gaps are rare outside military or highly regulated industrial settings because the operational friction is high.

A less extreme version is dedicated physical infrastructure: separate switches, separate cabling, and possibly separate firewalls for the office network and the plant network. This approach is common in older plants where the OT equipment predates modern networking and uses proprietary protocols that do not run well over VLANs. It also helps when you need to guarantee bandwidth for time-sensitive control traffic. The downside is cost, two sets of switches, twice the cabling, more power and rack space, and the operational burden of managing two parallel networks. For a mixed environment with a small office attached to a large plant, physical separation might be overkill, but for a large site with hundreds of controllers, it can be the clearest way to keep production traffic isolated from the office LAN.

Firewalls and DMZs at the boundary

Wherever two segments meet, you need a controlled crossing point. A firewall enforces rules about which traffic can pass and inspects it for threats. In a segmented network, firewalls sit at the boundaries between zones. For example, a firewall between the office VLAN and the plant VLAN can allow only specific protocols (such as Modbus TCP on a known port) and block

everything else. This is far more secure than letting the VLANs route through a general-purpose switch that also handles internet traffic.

A demilitarised zone (DMZ) is a small, isolated subnet that sits between the internal network and the outside world. In a mixed environment, a DMZ might hold a historian server that collects data from plant controllers and makes it available to office users for reporting. The DMZ server is the only device that both networks can talk to, so a compromise on the office side does not give an attacker direct access to the controllers. Setting up a DMZ properly requires careful firewall rule design and often a separate pair of firewalls for redundancy. It adds complexity, but for environments that need to share operational data with business systems, for example, to feed a manufacturing execution system, a DMZ is the standard architectural pattern recommended by ISA/IEC 62443 and other industrial security standards.



Software-defined networking for dynamic environments

Software-defined networking (SDN) separates the control plane (the logic that decides where traffic goes) from the data plane (the hardware that forwards packets). An SDN controller acts as the brain of the network, and switches and access points follow its instructions. This makes it possible to change segmentation rules on the fly without touching individual devices. If a plant line goes down and you need to temporarily let a vendor's laptop into the control network for diagnostics, an SDN can carve out a temporary segment with isolated access and then tear it down when the work is done.

SDN is still more common in data centres and large enterprise campuses than in small offices or traditional plants, but it is gaining traction in mixed environments where the segmentation

needs change frequently. The trade-off is that SDN introduces a single point of failure in the controller, and the skill set required to configure and maintain it is narrower than for VLANs. For most small to medium sites, VLANs and firewalls remain the practical choice, but SDN is worth knowing about if your network is growing fast or if you run a lot of temporary zones for contractors or seasonal operations.

Putting it together for a mixed environment

A mixed site, a small manufacturing plant with an attached office, might use a combination of approaches. The office side runs VLANs for departmental separation and a guest Wi-Fi VLAN that has no access to internal systems. The plant side uses a physically separate switch stack for the controllers, connected to the office network only through a firewall that allows a narrow set of protocols to a DMZ server. A Hans Study network security assessment can help identify the gaps in such a setup, checking that the firewall rules are tight, that no rogue devices bridge the two sides, and that the segmentation survives a real-world failure scenario. That kind of assessment is a good step before you commit to a full redesign, because it tells you what is already working and what needs the most attention.

In the office, you might also implement 802.1X authentication on the wired ports so that only authorised devices can join the network at all. On the plant floor, where controllers may not support 802.1X, you can use MAC address filtering combined with port security on the switches. It is not as strong as certificate-based authentication, but it raises the bar for an attacker who plugs a laptop into an unused port.

When to call in a network architecture consultant

Segmentation is one of those tasks that looks straightforward on paper but turns into a maze of edge cases when you start mapping out real traffic flows. A network architecture consultant brings experience from other sites, similar offices, similar plants, similar mixed environments, and can spot patterns that an internal team might miss. They can also help you translate compliance requirements (ISO 27001, NIST, ISA/IEC 62443) into concrete VLAN and firewall designs, and they can run a Hans Study network security assessment to validate that the segmentation works as intended before you roll it out across the whole site.

For a mixed environment, the consultant can also mediate between the IT team (who think in terms of Active Directory and cloud access) and the OT team (who think in terms of uptime and safety). Getting those two groups to agree on a segmentation plan is often harder than the technical implementation itself. A good consultant understands both worlds and can help each side see why the other's requirements matter.

Making your choice

Start by mapping your traffic: which devices need to talk to which other devices, and what protocols do they use? Then list the risks you care about most, lateral movement from a compromised workstation, unauthorised access to controllers, compliance audit findings. That exercise alone will point you toward one of the approaches above. For most small offices, VLANs are enough. For most plants, physical separation or a tightly firewalled boundary works best. For mixed environments, a layered approach that uses VLANs inside the office, a DMZ at the boundary, and physical separation or dedicated infrastructure inside the plant is the most common and most practical solution.

No matter which path you take, document the segmentation rules, keep the firewall rules reviewed, and run a periodic verification, either with internal tools or with a consultant, to confirm that no unintended paths have opened up over time. Networks drift as people plug in new devices, change switch configs, or add wireless access points. A segmentation plan that was tight a year ago may have gaps today. Regular checks keep the separation real, not just theoretical.

Hans Study on social media Twitter LinkedIn Instagram YouTube