

Plan de VLANs — Facultad Enfermería

Resumen rápido

Diseño por funciones (VLANs), con control de acceso, QoS para videoconferencias/VoIP y dimensionamiento para ~300 PCs., 70 impresoras, 50 teléfonos de oficina, hasta 200 teléfonos de usuarios, hasta 700 estudiantes concurrentes, y más. Incluye subredes propuestas, rangos DHCP, reglas básicas de ACL, hardware y despliegue.

VLANs propuestas (tabla)

VLAN	Nombre	Subred	DHCP_scope	Notas
3001	Management	192.168.1.0/24	Reservado (estático)	Acceso a switches, APs, NMS. Solo admin
3200	Servidores	192.168.100.0/24	Reservado (estático)	Web, AD, NFS, NVR, DB Usuarios, marcar DSCP en VLAN 30
3110	PCs/Usuarios	192.168.8.0/22	192.168.8.100 – 192.168.8.254	DSCP 46 (EF) para voz y 34 (AF41) para videoconferencia. activar <i>Trust DSCP</i> en los uplinks.
3120	WiFi Invitados	192.168.20.0/22	192.168.21.1 – 192.168.23.254	Sin acceso a recursos internos
3140	VoIP/ Teléfonos	192.168.30.0/24	Reservado (estático)	Voice VLAN. Prioridad alta, DSCP 46 (EF) para voz y 34 (AF41) para videoconferencia. activar <i>Trust DSCP</i> en los uplinks.
3130	Impresoras	192.168.40.0/24	Reservado (estático)	ACL: sólo VLAN PCs y admins
3150	VPN	192.168.50.0/24	Reservado (estático)	Vpn acceso remoto
3160	CCTV- Vigilancia	192.168.60.0/24	Reservado (estático)	Acceso a VLAN100 y VLAN10 según perfil Cámaras IP. Limitar ancho por puerto QoS “policed” o “shaped” a 2–4 Mbps por cámara. acceso a vLan Servidores (NVRs) y vLan PCs según perfil
3170	CCTV-Utec	192.168.70.0/24	Reservado (estático)	Cámaras IP. Limitar ancho por puerto QoS “policed” o “shaped” a 2–4 Mbps por cámara. acceso a vLan Servidores (NVRs) y vLan PCs según perfil

Comenzamos con el 3 (pensando en la unificación del edificio) pues Nutrición tienen el 1 y quizá el 2 según la siguiente lista:

1005 - Red Equipos Ubiquiti
1010 - Red Switches
1030 - Red Sala de Informática
1050 - Red Cantina
1100 - Red Inalambrica Administrativa
1110 - Red Inalambrica Informatica
1120 - Red Inalambrica Docentes
1130 - Red Inalambrica Funcionarios
1140 - Red Inalambrica Estudiantes
1150 - Red Inalambrica EDUROAM
220 - Red Interna Servidores
221 - Red Interna Estaciones

Plan DHCP / Reservas

- DHCP separado por VLAN (servidor DHCP con múltiples scopes / DHCP relay en el router/L3-switch).
 - Para servidores/administración, impresoras, teléfonos usa IPs estáticas.
-

QoS (Calidad de Servicio) — prioridad para videoconf y VoIP

Política general:

1. Activar Trust DSCP (Differentiated Services Code Point) en uplinks (trunks) y en equipos que pueden marcar tráfico (APs, routers).
 2. Marcar/Mapear: - VoIP: DSCP EF (46) máxima prioridad. - Videoconf interactiva (Zoom): AF41 o DSCP 34 alta prioridad. - Resto tráfico de datos: BE (0).
 3. En access switches: mls qos trust dscp (o configuración equivalente). Configurar colas e intervalos.
 4. Limitar cámaras si saturan: shape o policing por puerto para cámaras (ej. 2–4 Mbps por cámara dependiendo de resolución).
-

ACLs y control de acceso (ejemplos)

Principio: por defecto negar, permitir lo necesario.

Permitir PCs a impresoras
Bloquear acceso PCs a cámaras
Permitir acceso PC a DNS/AD/Servidores necesarios
Denegar resto

ACLs aplicadas en el L3-router entre VLANs; para mayor seguridad usar firewall y stateful inspection.

Diseño físico / switches

Actualmente contamos con:

4 HPE JG962A - piso 2
4 HPE JG962A - piso 1
2 HPE JG962A - piso PB
1 HPE JG962A - Bas
1 DCN S5750E - piso PB
1 Aruba Network 7010 -ARCNO103 - Bas
1 Huawei Cloud Engine S5735-L24P4X-A1 - Bas
1 Huawei Ekit Engine S310-24P4X – Bas
2 Huawei Ekit Engine S310-24P4X – U.Inf.- Bas
4 Huawei Ekit Engine S310-24P4X – U.Inf.- Piso 3
1 D-Link DES-3028 - Servidores
1 Aruba Instant 1930 24P1G-T/4P10G SFP+ - Servidores
5 Linksys LGS328MPC - Utec
1 Linksys LGS328MPC - U.Inf (roto?)
1 Tp-Link - TP-SG3428MP – U.Inf.
1 Bdcorn s5612e

31 Switches Total

Cámaras CCTV

- Separar cámaras en VLANs 3160/3170 según función.
 - NVR(s) en VLAN 3200 (servidores) con reglas que permitan sólo acceso desde VLAN 3200 a VLAN 3160/3170.
 - Limitar ancho por puerto/canal (shape) y usar multicast si sistema lo soporta.
-

Servidores y almacenamiento

- Servidores en VLAN 3200.
 - VLAN de management (3001) con acceso SSH/HTTPS restringido a IPs de administración.
-

Monitorización / Logging

- NMS (Zabbix, PRTG, LibreNMS) en VLAN 3001.
 - Syslog centralizado y RMON/SNMPv3 para switches.
 - Registrar tasas de utilización por VLAN para ajustar QoS.
-

Tareas operativas

- Documentar cada puerto: etiqueta física + inventario.
- Versionar configuración (backup configs iniciales)
- Esquema lógico VLANs del primer cuadro (Usuarios, WiFi, Cámaras, Impresoras, Servidores)
- Rutas inter-VLAN (en pfSense)
- Configurar VLANs en core/distribution.

- Configurar trunks 802.1Q con native VLAN controlada.
- Configurar DHCP scopes y DHCP-relay (IP helper) en L3.
- Implementar ACLs restrictivas en L3 y reglas en firewall.
- Configurar QoS: marcar, mapear y priorizar colas.
- Cargar configuración base (VLANs, trunks, nombres de puertos) de un modelo de switch, grabar, probar, guardar. Modificar .conf para cargar (importar) en siguiente switch del mismo modelo.
- Conectarlo al pfSense (en trunk).
- Monitoreo y ajustes.
- Verificar que los dispositivos obtienen IP del nuevo DHCP (pfSense).
- Validar acceso (Internet, impresoras, servidores, etc.).
- Generar documentación
- Mapear puertos → ubicación física / VLAN / dispositivo.
- Registrar IPs asignadas y reservas DHCP.