Defensible Schools Cheatsheet v7.2

VPN Remote Access?

ICT Staff | ICT External

Internet

- Google DNS (DNS)
- Open DNS (DNS)
- HEAnet — DNS 87.32.4.16, 87.32.4.24 — PAN Level 1-5 Content Filtering
- Virgin Media (DNS)
- eir (DNS)
- Amazon Web Services — IAM (AD or ?) — Backups
- Google Compute Cloud (GCP) — IAM (AD or ?) — Backups
- Microsoft Azure — IAM (AD or ?) — Backups
- Google for Education Google Apps (GApps) — Fileserver — Storage — Email — Google Apps
- Microsoft Education Office 365 (O365) — Fileserver — Storage — Email — Office 365 — Word — Excel — Powerpoint

School Campus

1Gbps or 400 / 40Mbps

Redundant ISP different paths

1Gbps or /100 / 20Mbps

Main Building (DCC + Services)

- DP
- WAP NP
- HL
- Ceiling Mount
- Cat6a cabling EVERYWHERE
- General Assembly
- Principal's Office — PC NP, P NP, WAP NP, HL, AP, Ceiling Mount
- Staff Room — PC NP, PC NP, WAP NP, HL, AP, Ceiling Mount, P NP
- Classroom 1 — WAP NP, HL, AP, Ceiling Mount, TP NP, DP NP
- Classroom 2 — TP NP, DP NP, AP, Ceiling Mount, WAP NP, HL

Albeit 1x WAP NP per classroom this DOES NOT MEAN 1x AP per classroom!!!!!!

"PREDICTIVE MODELING and WLAN COVERAGE AND CAPACITY DESIGN" must be done

The DESIGN will dictate the AP mounting locations and RF characteristics.

Requirements should dictate if / where halls / roaming / outdoor coverage is required

DCC(Data Communications Centre)

- Structured Cabling
- Primary ISP_A Link
- Secondary ISP_B Link
- Telco MDF
- Phone lines for Security / Fax Phone
- ICT Designed Rack Layout

Rack / Cabinet (42 RU):
- 24 port patch panel
- 24 port patch panel
- ISP A | ISP B
- HEAnet Router
- HEAnet VLAN 2 — ACL 102in/101out
- VPN | NAT | IPS | DHCP
- FW+WAN ROUTER — IPFIX
- FW+WAN ROUTER
- COLLAPSED CORE?
- COLLAPSED CORE?
- 24x port patch panel
- 48x POE+ edge switch
- 24x port patch panel
- 48x POE+ edge switch
- 24x port patch panel
- UPS

2x 1Gbps or 2x 10Gbps — SM x2

Layer 3 on Layer 2 LAG or L3 x 2

Main Building / L2 Roaming Domain / L3 Subnets

- .1 gateways
- .2-49 DHCP Reserved Fixed
- Default 8 hour DHCP lease
- OpenDNS paid DNS

VLAN	Subnet	SSID	DHCP
VLAN 1 — Common Vendor Defalt / Security Risk			
VLAN 2 — No Subnet ISOLATED			
VLAN 3 — Native on Infra Links			
VLAN 4-15 — Reserved			
	Subnet: 10.0.16/20		
VLAN 16	Subnet: 10.0.16/22	Wifi Student	DHCP lease 4 hours
VLAN 20	Subnet: 10.0.20/23	Wifi Teacher	DHCP lease 12 hours
VLAN 22	Subnet: 10.0.22/23	Wifi Guest	DHCP lease 1 hour
VLAN 24	Subnet: 10.0.24/24	Wired Student	
VLAN 25	Subnet: 10.0.25/24	Wired Teacher	
VLAN 26	Subnet: 10.0.26/24	Wired Untrusted	Printer, Light Honeynet
VLAN 27	Subnet: 10.0.27/24	SERVICES	DNS, DHCP, Print Server, IAM (AD or ?), Radius, Backups, Storage, Fileserver, VDI
VLAN 28	Subnet: 10.0.28/24	Infra Mgmt	
VLAN 29	Subnet: 10.0.29/24	OOB	
VLAN 30	Subnet: 10.0.30/24	Security	
VLAN 31	Subnet: 10.0.31/24	Smart IoT	

Second Building

IDF (10-42 RU) — DHCP Relay
- 24x port patch panel
- 48x POE+ edge switch
- 24x port patch panel
- 48x POE+ edge switch
- 24x port patch panel
- UPS

L2 Roaming Domain / L3 Subnets

- .1 gateways
- 2-49 DHCP Reserved Fixed
- Default 8 hour DHCP lease
- OpenDNS paid DNS

VLAN	Subnet	SSID	DHCP
VLAN 1 — Common Vendor Defalt / Security Risk			
VLAN 2 — No Subnet ISOLATED			
VLAN 3 — Native on Infra Links			
VLAN 4-15 — Reserved			
	Subnet: 10.0.32/20		
VLAN 32	Subnet: 10.0.32/22	Wifi Student	DHCP lease 4 hours
VLAN 36	Subnet: 10.0.36/23	Wifi Teacher	DHCP lease 12 hours
VLAN 38	Subnet: 10.0.38/23	Wifi Guest	DHCP lease 1 hour
VLAN 40	Subnet: 10.0.40/24	Wired Student	
VLAN 41	Subnet: 10.0.41/24	Wired Teacher	
VLAN 42	Subnet: 10.0.42/24	Wired Untrusted	Printer, Light Honeynet
VLAN 43	Subnet: 10.0.43/24	SERVICES	
VLAN 44	Subnet: 10.0.44/24	Infra Mgmt	
VLAN 45	Subnet: 10.0.45/24	OOB	
VLAN 46	Subnet: 10.0.46/24	Security	
VLAN 47	Subnet: 10.0.47/24	Smart IoT	

Third Building

As per second building only with VLAN: 48-63 Subnet: 10.0.48/20

2-20 Gbps spoke from main building

Applications

Teaching

ActivInspire

Productivity and Admin

Alladin

Google Apps | Docs | Sheets | Slides | Email

Office 365 | Word | Excel | Powerpoint | Email

Legacy / Department / 3rd Party

Wifi (WLAN)

Cloud or Local Controller?

Design + RF

- PREDICTIVE SURVEY REQUIRED !!
- 802.11n/ac
- SSID1: "School"
- SSID2: "School-Guest"
- SSID3: "School-Staff"
- SSID4: "School-x"
- 5GHz | Dualband+Steer
- 2.4GHz | WPAv2
- 20MHz | DFS Channels
- Minimum Data Rate 24 Mbps
- RSSI: =< -63 (Primary Coverage)
- SNR: 25 dB
- RSSI: =< -75 (Secondary Coverage)
- MCA (MultiChannel Architecture)
- Static Channels not RRM

AAA

- Radius
- PPSK/DPSK
- 802.1X

Vendors

Ubiquiti
- Low (CAPEX)
- No Commercial Support
- Cloud or Local Mgmt
- Lack ENT featureset
- YRC Support
- No LIC/Mgmt = function
- Alert/Monitor/Analytics
- UI/UX + Expertise
- Lifecycle Mgmt
- Native SW / FW / Router
- Not PDST qualified

Aerohive
- Medium (CAPEX)
- Commercial Support
- Cloud or Local Mgmt
- ENT featureset
- YRC LIC/Support
- No LIC/Mgmt = function
- PPSK
- Alert/Monitor/Analytics
- UI/UX + Expertise
- Lifecycle Mgmt
- Native SW / FW / Router

Aruba
- High (CAPEX)
- Commercial Support
- Cloud or Local Mgmt
- ENT featureset
- YRC LIC/Support
- No LIC/Mgmt functions
- Alert/Monitor/Analytics
- UI/UX + Expertise
- Lifecycle Mgmt
- Native SW

Cisco
- High (CAPEX)
- Commercial Support
- Local Mgmt
- ENT featureset
- YRC Support
- No LIC/Mgmt = function
- Alert/Monitor/Analytics
- UI/UX + Expertise
- Lifecycle Mgmt
- Native SW / FW / Router

Cisco Meraki
- Medium (CAPEX)
- Commercial Support
- Cloud or Local Mgmt
- ENT featureset
- YRC LIC/Support
- No LIC/Mgmt = failure
- Alert/Monitor/Analytics
- UI/UX + Expertise
- Lifecycle Mgmt
- Native SW / FW / Router

Ruckus
- High (CAPEX)
- Commercial Support
- Cloud or Local Mgmt
- ENT featureset
- YRC LIC/Support
- No LIC/Mgmt = function
- DPSK
- Alert/Monitor/Analytics
- UI/UX + Expertise
- Lifecycle Mgmt
- Native SW

Office 365 Online only — Google: Android, ChromeOS

Office 365 Google Apps — Apple: iOS, MacOS; Microsoft: Windows

Guest — BYOD (Bring Your Own Device)

Office 365 Online only — Google: Android, ChromeOS, AcerR11

Office 365 Google Apps — Apple: iOS, iPAD, MacOS, MacbookAir; Microsoft: Windows, AD, Windows10

Student | Teacher

Wired (LAN)

Cloud or Local Controller?

- Firewall + Router
  - Max TCP/UDP sessions
  - Max Throughput +/- features
  - L7 / DPI / QoS / Shaping
  - Routing? IGP/EGP?
  - DHCP
  - Active/Active
- Switching Edge/Core
  - 48x Gigabit POE+
  - Cloud Managed
  - SFP Fiber Ports
  - Layer 2/3 Featuresets
  - Dedicated Mgmt Port
  - Console Port
  - Dual Power Supplies
  - Stackable
  - Virtual Stack
  - 802.1X
  - QoS
  - Wattage for X APs?
  - 10Gbps Uplinks?
  - DHCP / Routing?

Office 365 Online only — Google: ChromeOS, AcerR11

Office 365 Google Apps — Apple: MacOS, MacbookAir; Microsoft: Windows, AD, Windows10

Teacher

Office 365 Online only — Google: ChromeOS, AcerR11

Office 365 Google Apps — Apple: MacOS, MacbookAir; Microsoft: Windows, AD, Windows10

Student

ICT Professional Services

- PDST Procurement Framework
- Network (Wired/Wireless)
- ICT Systems
- SOW(Statement of Work)
- Fixed Cost
- T&M(Time and Materials)
- Defined Deliverables
  - "Biz" + Technical Requirements
  - HLD(High Level Design)
  - Low(Low Level Design)
  - As Built + Diagrams + Configs
  - Playbook + Support Runbooks
  - Live/Tested Services as per above
- PI / PL Insurance
  - EU 12.7m Employers Liability
  - EU 6.5m Public Liability
  - EU 1m Professional Indemnity
  - EU 6.5m Public Liability
- PS Notable Training/Certs

WIRELESS: CWNA, CWNP, CWNE, CCNA Wireless, CCNP Wireless, CCIE Wireless

WIRED: CCNA, CCNP, CCIE, JCNIA, JNCIP, JNCIE, Comptia N+

Key

Advised	Recommendable / Best Current Practice
Questionable	Complexity / Performance / OPEX or TCO
AVOID	Insecure / Legacy / Support or TCO issues
Neutral	Pros / Cons and different TCO + OPEX + CAPEX
WAP NP	Wireless Access Point (Network Point)
TP NP	Teacher Position Network Point
DP NP	Digital Projector Network Point
PC NP	Personal Computer Network Point
PNP	Printer Network Point
DP	Data Point
HL	High Level (2metres+ preferred ceiling)
LL	Low Level (1 meter waist height)
SM	Single Mode (fiber run with SC-SC termination)
	Wireless Access Point (Internal Antenna) 802.11n/ac (Wave 1)
UPS	Uninterruptible Power Supply

mailto:donal@defensible.ie
https://defensible.ie

1. OPTIMISE FOR OPERATIONS and OPEX
2. SECURITY and RESILIENCY — GDPR
3. PERFORMANCE and CHANGE — Metrics
4. NETWORK as CRITICAL INFRA — Fabrics
5. SIMPLICITY + REDUCE COMPLEXITY