School Information Security
Do you know it ?
Can you make it ?

學校資訊及網絡安全
你懂嗎？你做到嗎？

Mr. Albert Wong
IT Manager & Teacher, Ying Wa College (YWC)
Chairman, Association of IT Leaders in Education (AiTLE)
Email : 9028 9443 / albertwong@aitle.org.hk
Website: https://www.aitle.org.hk

資訊科技教育領袖協會 (AiTLE)

- 創立於 2002 年
  - 源於「教育局第一期資訊科技教育策略 AIT 培訓課程」
  - 由不同學校資訊科技統籌及電腦科老師組成
    - 教師團體、專業團體、義務組織
  - 舉辦不同「教師專業發展」及「學生比賽」
    - 講座、工作坊、海外交流團等
  - 幹事及從屬幹事：52 人
  - 會員人數：1,540 人
  - 為學界最大 IT 教師專業團體
  - **Google Educator Group (GEG) Hong Kong - Leader & Co-Leaders**
  - **Microsoft Education Hong Kong – AiTLE Microsoft Expert Teacher (AMET)**

AiTLE 與 Info Sec

資訊保安 @ AiTLE @ 2003

2016-03-22

https://www.aitle.org.hk/?p=3177

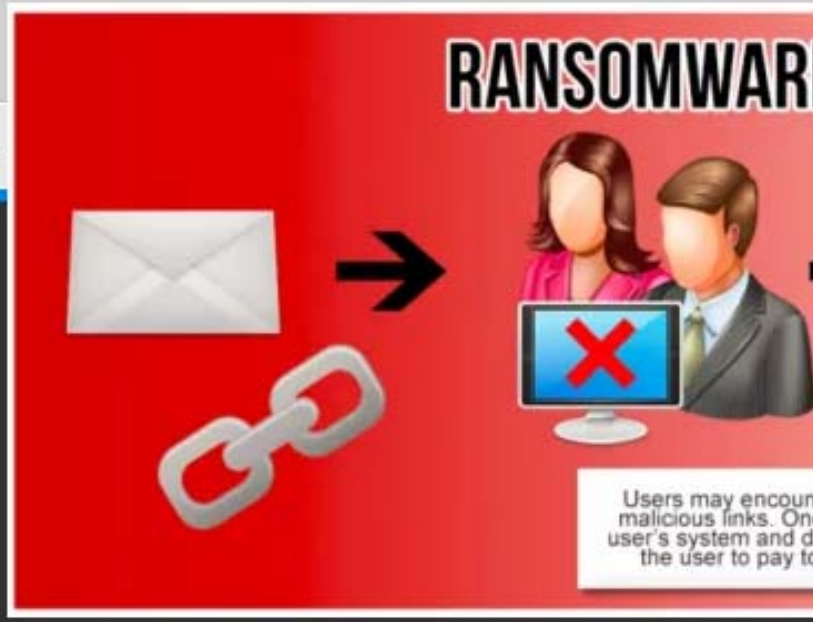
2016-04-19

AiTLE 資訊科技教育領袖協會
Association of I.T. Leaders in Education

首頁 | 最新消息 | 本會資料 | 本會項目 (Projects) | 會員專區 | 常用連結 | 「IT in Ed

AiTLE 合辦活動：「學校資訊保安講座：加密勒索軟件～防範、數據保障與解決方案」

Dates: 04/19/2016 Times: 14:30 - 17:30 Location: 九龍九龍塘「教育局九龍塘教育服務中心」西座 4 樓演講廳



https://www.aitle.org.hk/?p=3243

2016-04-30

AiTLE 資訊科技教育領袖協會
Association of I.T. Leaders in Education

首頁 | 最新消息 | 本會資料 | 本會項目 (Projects) | 會員專區 | 常用連結 | 「IT in E

AiTLE 合辦活動：Email [Server] Migration to Cloud Seminar

Dates: 04/30/2016 Times: 09:30 - 12:30 Location: Room 201-202, 2/F, HkedCity, Sha Kok Estate, Shatin Wai, Shatin

https://www.aitle.org.hk/?p=3252

2016-09-07

AiTLE 資訊科技教育領袖協會
Association of I.T. Leaders in Education

首頁 | 最新消息 | 本會資料 | 本會項目 (Projects) | 會員專區 | 常用連結 | 「IT in Ed、e

AiTLE + HKUEdAA + EDB Seminar : Security Threats in Schools (physical and social)

Dates: 07/09/2016 Times: 09:30 - 12:29 Location: W404, EDB KTESC, Kowloon Tong, Kowloon

https://www.aitle.org.hk/?p=3446

2017-05-17

AiTLE 資訊科技教育領袖協會
Association of I.T. Leaders in Education

首頁 | 最新消息 | 本會資料 | 本會項目 (Projects) | 會員專區 | 常用連結 | 「IT in Ed、eLearning、STEM」活動時間表 | Subscribe for updates

AiTLE Seminar : Briefing Seminar re Defense Against the Ransomware "WannaCry"

Dates: 05/17/2017 Times: 17:00 - 19:00 Location: Lecture Theatre, 4/F, West Block, Kowloon Tong Education Services Centre, 19 Suffolk Road, Kowloon Tong, Kowloon

https://www.aitle.org.hk/?p=3937

2017-11-28

AiTLE 資訊科技教育領袖協會
Association of I.T. Leaders in Education

首頁 | 最新消息 | 本會資料 | 本會項目 (Projects) | 會員專區 | 常用連結 | 「IT in Ed、

AiTLE 簡介會：加強學校資訊保安與數據保護簡介會

Dates: 11/28/2017 Times: 09:30 - 12:30 Location: 九龍九龍塘「教育局九龍塘教育服務中心」西座四樓演講廳

https://www.aitle.org.hk/?p=4365

2018-04-30

AiTLE 資訊科技教育領袖協會
Association of I.T. Leaders in Education

首頁 | 最新消息 | 本會資料 | 本會項目 (Projects) | 會員專區 | 常用連結 | 「IT in Ed

「資訊科技教育領袖協會（AiTLE）」
全港學校網站安全普查發布會

Dates: 04/30/2018 Times: 10:00 - 11:00 Location: 觀塘鴻圖道 52 號 2 樓

https://www.aitle.org.hk/?p=4656

2018-06-13

AiTLE 資訊科技教育領袖協會
Association of I.T. Leaders in Education

首頁 | 最新消息 | 本會資料 | 本會項目 (Projects) | 會員專區 | 常用連結 | 「IT in E

AiTLE Event : Seminar on SSL & DNSSEC for School Websites

Dates: 06/13/2018 Times: 15:00 - 17:30 Location: 新界沙田博康邨「基督書院」

https://www.aitle.org.hk/?p=3177

AiTLE Community of Practices on Info Sec

AiTLE Sch Info Security 1

Created 3/31/2016 at 10:37

AiTLE Sch Info Security 2

Created 7/31/2017 at 23:01

Another AiTLE Whatsapp group

With expert from

- **AiTLE**
- **HKCERT**
- **HKIRC / HKDNR**
- **HKCERT**
- **Hong Kong Police Force**
- **PISA**
- **Cisco**
- **Microsoft**
- **Speedy**
- **UDomain**
- **EDB**
- **HkedCity**

你與 Info Sec

一間學校的 IT 工作

- 班房電腦，咪箱，實物投影機
- 教員室電腦
- 電腦室電腦
- 影印機
- 廣播系統
- 校園電視台
- 閉路電視
- 禮堂音響、燈光
- 學校網頁
- 學校伺服器（維護、備份、冗餘）
- 無線網絡
- 軟件版權
- 電子學習
- BYOD
- 內聯網
- 拍卡點名
- 電子通告
- 家長 App
- 防火牆
- 資訊素養
- 技術員管理
- .....

一間學校的 IT 工作

- 班房電腦，咪箱，實物投影機
- 教員室電腦
- 電腦室電腦
- 禮堂音響、燈光
- 學校網頁
- 學校伺服器（維護、備份、冗餘）
- 無線網絡
- 軟件版權
- 電子學習
- BYOD
- 防火牆
- 資訊素養
- 技術員管理
- .....

哪一項工作最重要？

一間學校的 IT 工作

- 班房電腦，咪箱，實物投影機
- 教員室電腦
- 電腦室電腦
- 禮堂音響、燈光
- 學校網頁
- 學校伺服器（維護、備份、冗餘）
- 無線網絡
- 軟件版權
- 電子學習
- BYOD
- 防火牆
- 資訊素養
- 技術員管理
- .....

其實：每一門也是一門學問

一間學校的 IT 工作

- 班房電腦，咪箱，實物投影機
- 教員室電腦
- 禮堂音響、燈光
- 學校網頁
- 學校伺服器（維護、備份、冗餘）
- 無線網絡
- 軟件版權
- 電子學習
- 防火牆
- 資訊素養
- 技術員管理
- .....

但變化得最快，可令你「一舖清袋」的，是..

中咗

當你（學校）中咗

Image Source :
https://cdn.hk01.com/di/media/images/378041/org/960c58864092edf3b0c40c3b31eb8171.jpg/VYZZY-6xlEPB_0P9Gi-0MwodOvEfV4zHZT_sXmU_7F4?v=w1920

當你（學校）中咗

你會問：「點解會係我呀！」

回顧 AiTLE Activities on Info Sec

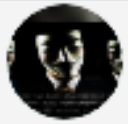
2016 > 2017 > 2018

代表「靜」咗？

分享（一）

AiTLE Sch Info Security 1
12/5/2018
近日收到兩三個學校求救，中了 Ransomware ... 有學校 File Server & Backup Server 都中咗。提提大家做 backup & remind 同事
14:11
記緊唔好將remote desktop 直接放出街. 同埋Backup server 有留一set offline
14:13
14:35
You
近日收到兩三個學校求救，中了 Ransomware ... 有學校 File Server & Backup Server 都中咗。提提大家做 backup & remind 同事
如有多些資料，例如：怎樣中？源頭？請告知，謝謝!!
14:45

分享（一）



AiTLE Sch Info Security 1

一些建議：

如果要用Remote desktop, 請先用VPN.
如果是一般操作，請不要用Domain Administrator Password.
一定要有一份offline backup.

16:53

用teamviewer 會唔會較安全？

16:57

分享（二）

Alert For [redacted] - albertwong

Terence Reardon <foflorentinozq... 2018年7月28日 週六 上午6:59

寄給 albertwong@aitle.org.hk

I will cut to the chase. I'm aware [redacted] is your pass word. Moreover, I am aware about your secret and I have proof of it. You do not know me and no one employed me to check out you.

It is just your misfortune that I stumbled across your blunder. In fact, I actually setup a malware on the adult vids (sex sites) and you visited this site to experience fun (you know what I mean). While you were watching videos, your internet browser started operating as a Rdp (Remote desktop) with a keylogger which provided me with accessibility to your display as well as web camera. Just after that, my software

分享（二）

And I am about to offer you two options which will achieve that. Those two choices to either ignore this letter, or perhaps pay me $3200. Let's investigate these 2 options in details.

First Option is to ignore this e-mail. Let's see what will happen if you select this path. I will definitely send out your video recording to all of your contacts including family members, colleagues, and so on. It will not save you from the humiliation you and your family will face when family and friends learn your unpleasant details from me.

Option 2 is to send me $3200. We will name it my "privacy charges". Now lets see what will happen if you pick this option. Your secret will remain your secret. I'll destroy the recording immediately. You continue on with your daily life as though none of this ever happened.

Now you may be thinking, "I will call the cops". Let me tell you, I have covered my steps to make sure that this message cannot be linked to me plus it won't stop the evidence from destroying your life. I am not planning to steal all your savings. I just want to get

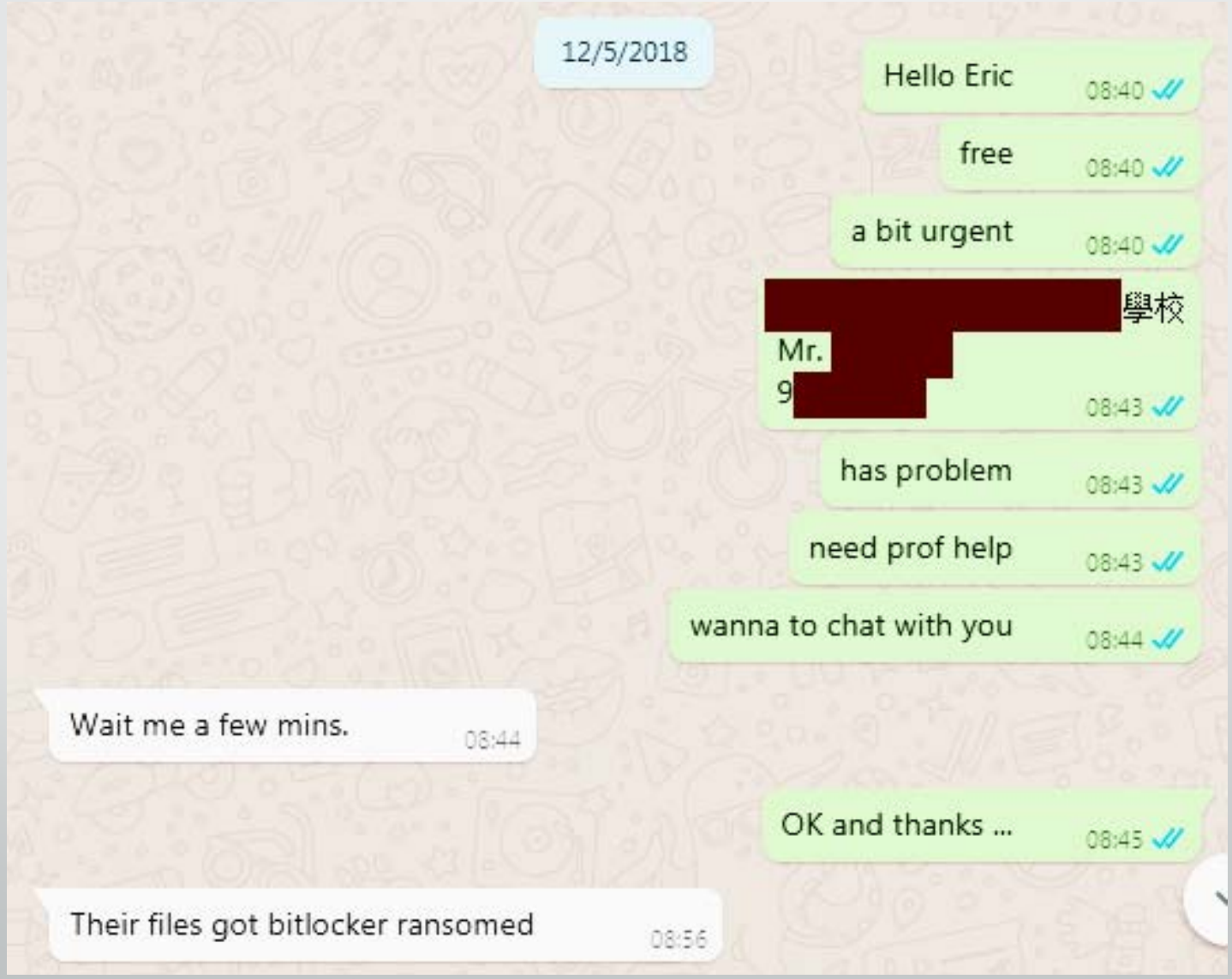
分享（二）

pretty much everything disappear and pay me my confidentiality fee. You'll make the payment via Bitcoin (if you do not know this, type "how to buy bitcoins" on google)

Amount to be sent: $3200
Bitcoin Address to Send to: 17G46bmya24bMEzvbYmvUrGLtgAEdDW45M
(It is CASE sensitive, so copy and paste it)

Share with no one what will you be utilizing the bitcoin for or they may not offer it to you. The process to have bitcoins may take a day or two so do not delay.
I've a unique pixel within this e-mail, and now I know that you have read through this email message. You now have 2 days in order to make the payment. If I do not get the BitCoin, I will definitely send your video recording to all of your contacts including friends and family, colleagues, and so forth. You better come up with an excuse for friends and family before they find out. Nonetheless, if I receive the payment, I'll destroy the video and all other proofs immediately. It's a non negotiable offer, so don't waste my time and yours. Time is running out. You should know that my software will still be sharing what action you adopt when you are done looking over this email. Let me assure you that If I see any bad activity from your web history then let me send

分享（二）


12/5/2018
Hello Eric 08:40
free 08:40
a bit urgent 08:40
[redacted]學校
Mr.
9[redacted] 08:43
has problem 08:43
need prof help 08:43
wanna to chat with you 08:44
Wait me a few mins. 08:44
OK and thanks ... 08:45
Their files got bitlocker ransomed 08:56

分享（二）

12/5/2018
OK and thanks ... 08:45
Their files got bitlocker ransomed 08:56
Oooooo 08:57
又黎 08:57
有無得救？ 08:57
嗯，要度度 08:58
Thanks ... 08:58
Total lost 16:14
無得救？ 16:14

分享（三）

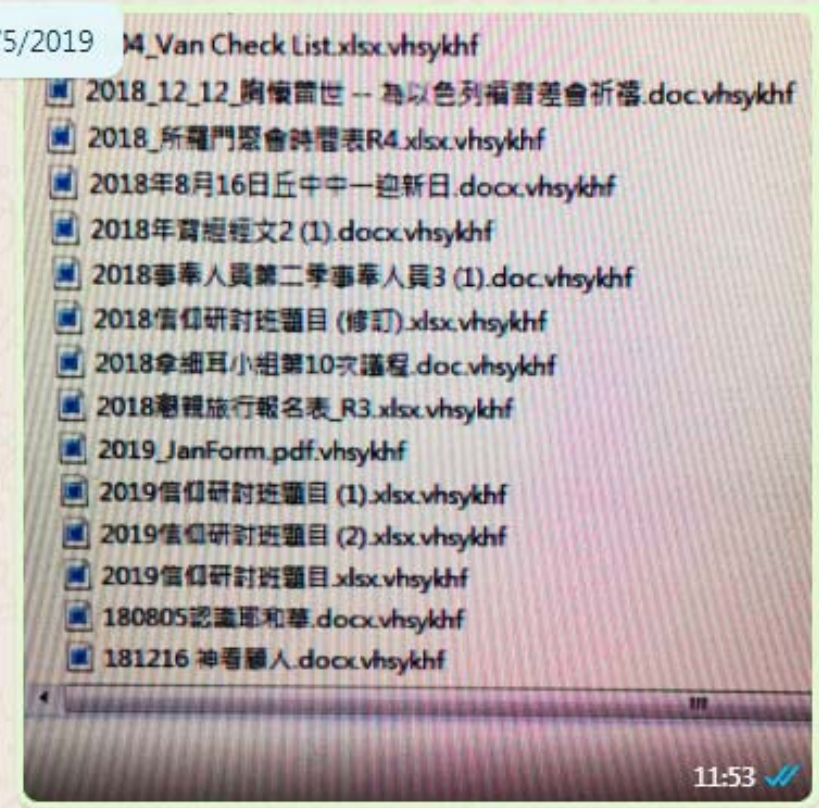
12/5/2018
無得救？ 16:14
佢好似話[redacted]黎幫手 16:15
無 16:15
都救唔到？ 16:15
無啦 16:15
差做data recovery 16:15
差 ransom 係 encrypt 啲 file 定係 deleted 晒啲 file ??? 16:15
Bitlocker encrypt file server 16:18
Format backup server 16:18
AD create 一個user 16:18
feel to chat through phone ??? 16:18

分享（二）

12/6/2018
Do you know the update of the school case yesterday ?!?
15:38
Yes, they whatsapp me this morning
15:56
Eric Fan
Yes, they whatsapp me this morning
An unexpected result
16:16
haha, which mean they have luck
16:16
你估，佢地會唔會有follow up action?
16:17
Eric Fan
haha, which mean they have luck
Yes
18:18
Eric Fan
你估，佢地會唔會有follow up action?
佢地 = school or hacker
18:19

分享（四）

1/5/2019



中咗？ 11:53

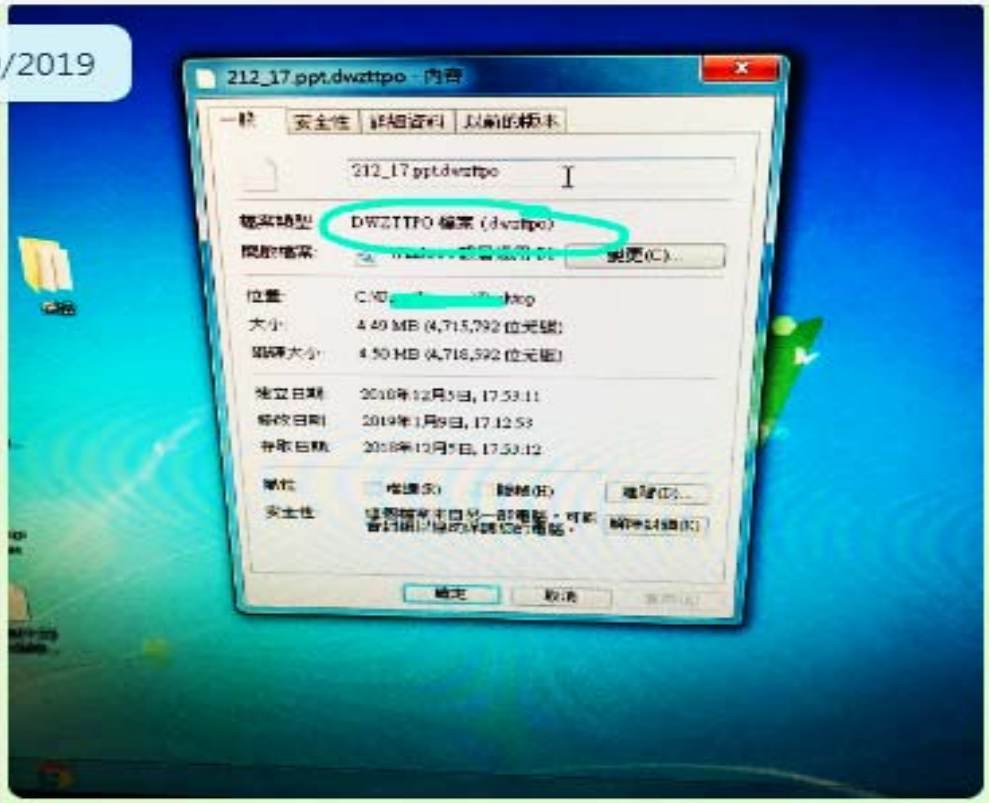
From a friend 11:53

中左啦 12:04

用邊隻Ant Virus. 12:05

分享（五）

1/9/2019



A teacher ask whether is infected by virus / ransomeware ?!?

18:17

個老師話個同事上網去一個把影片轉格式既網址，Click 咗入去就中咗

19:00

跟住而家部機啲 file encrypted .. Server files also encrypting ... 但暫時發現只係果位中咗同事既權限去到既檔案被加密

19:01

分享（六）

同事？

學生？

TSS？

一切從設計開始

基本學校網絡佈局

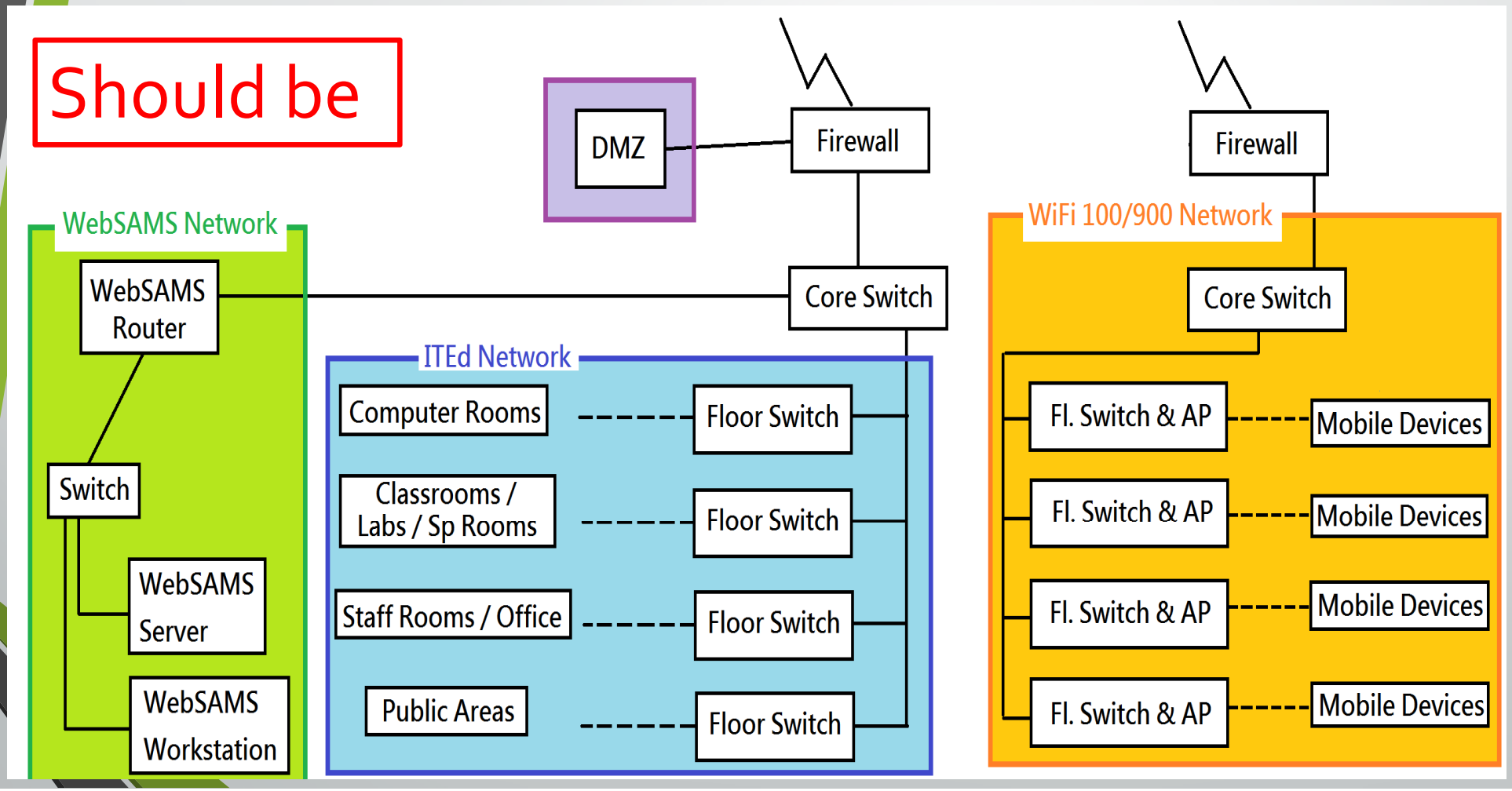

Should be
DMZ
Firewall
Firewall
WebSAMS Network
WebSAMS Router
Core Switch
Core Switch
WiFi 100/900 Network
ITEd Network
Switch
WebSAMS Server
WebSAMS Workstation
Computer Rooms
Classrooms / Labs / Sp Rooms
Staff Rooms / Office
Public Areas
Floor Switch
Floor Switch
Floor Switch
Floor Switch
Fl. Switch & AP
Fl. Switch & AP
Fl. Switch & AP
Fl. Switch & AP
Mobile Devices
Mobile Devices
Mobile Devices
Mobile Devices

Image Source :
https://i.pinimg.com/originals/17/ce/c9/17cec9b145684a57d96142522769c178.jpg

基本學校網絡佈局

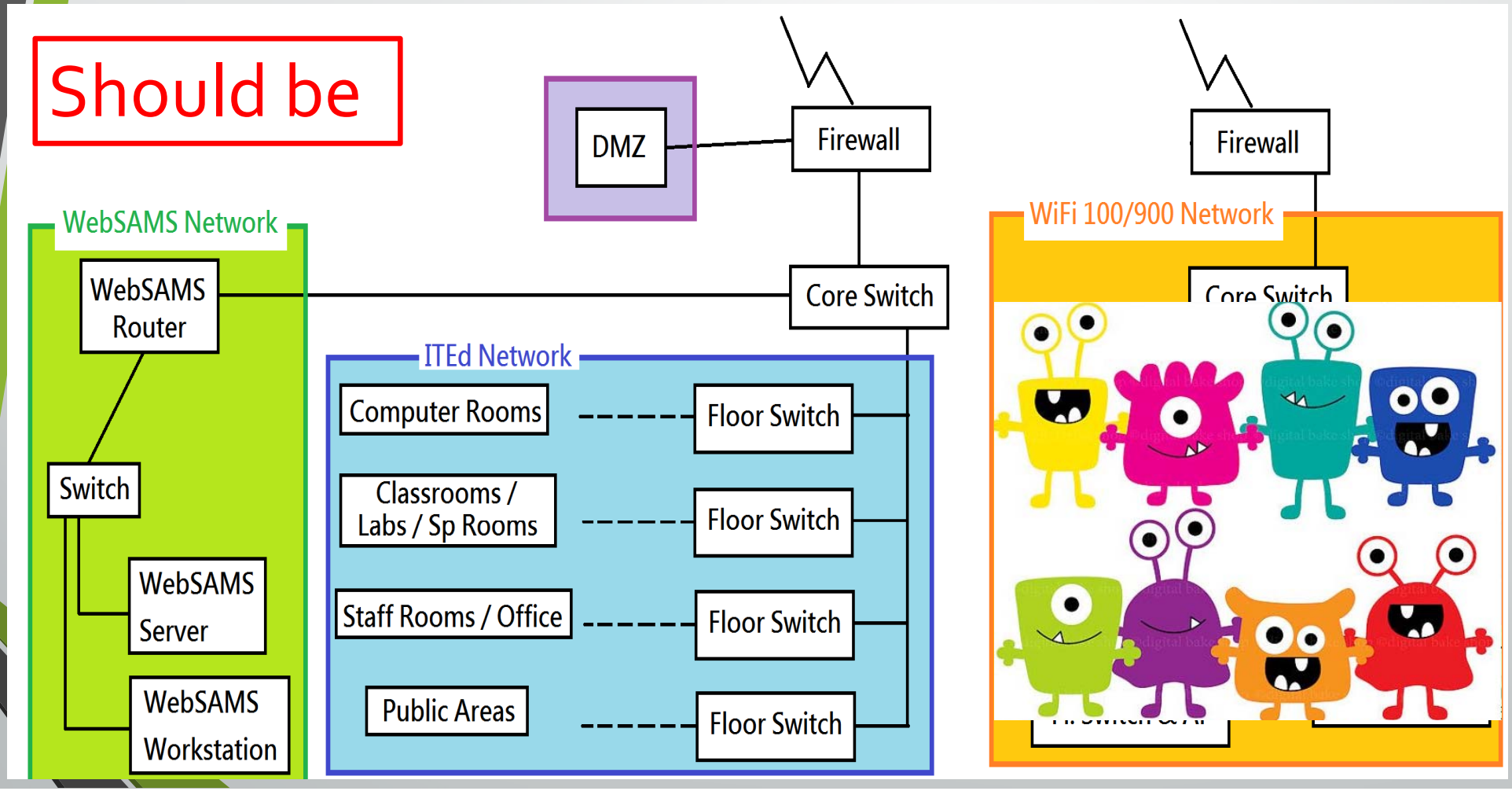
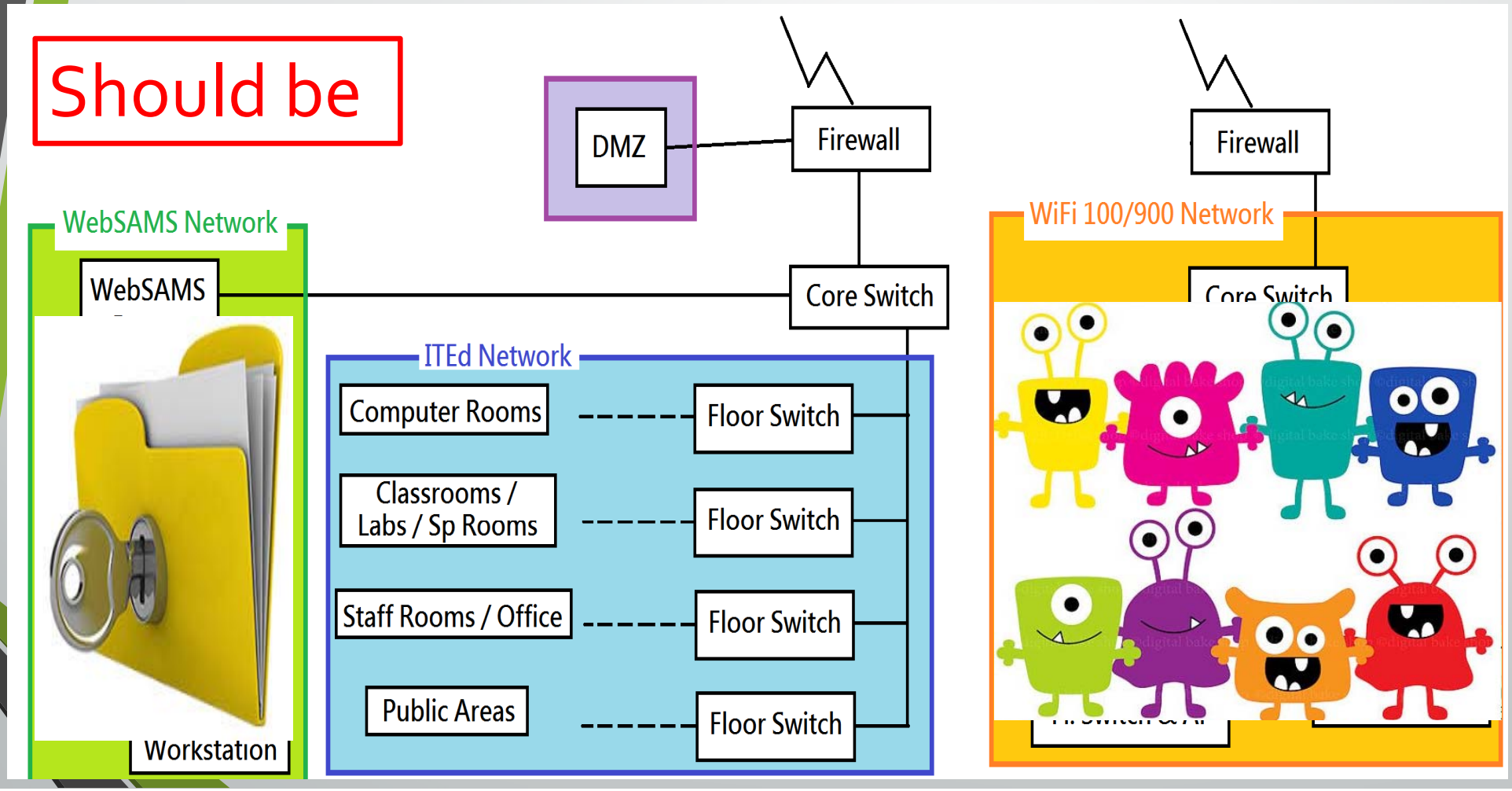
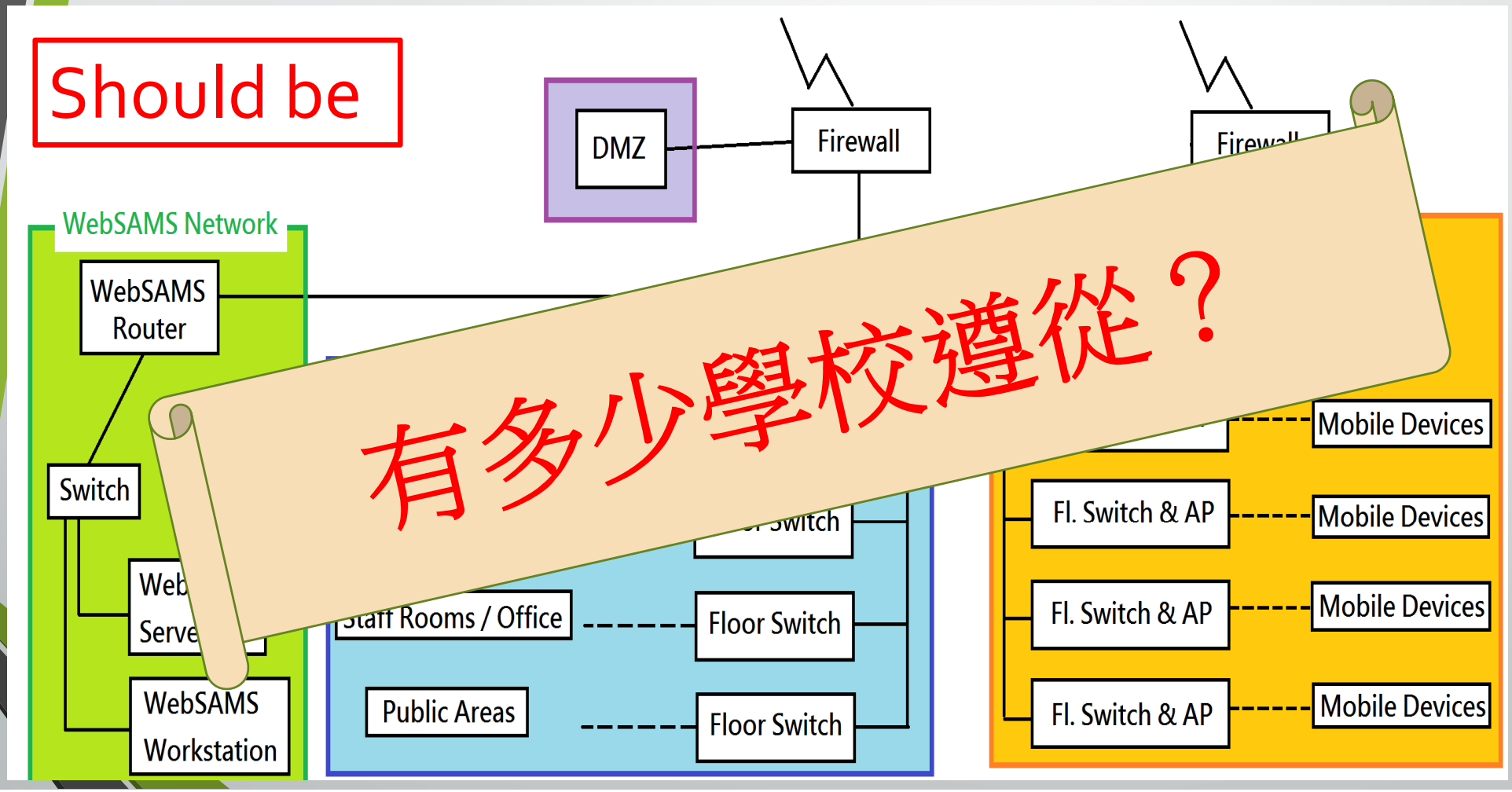


Image Source :
http://www.aptusinfotech.com/sites/default/files/Data%20Loss%20Prevention%20-%20DLP%20%282%29.png

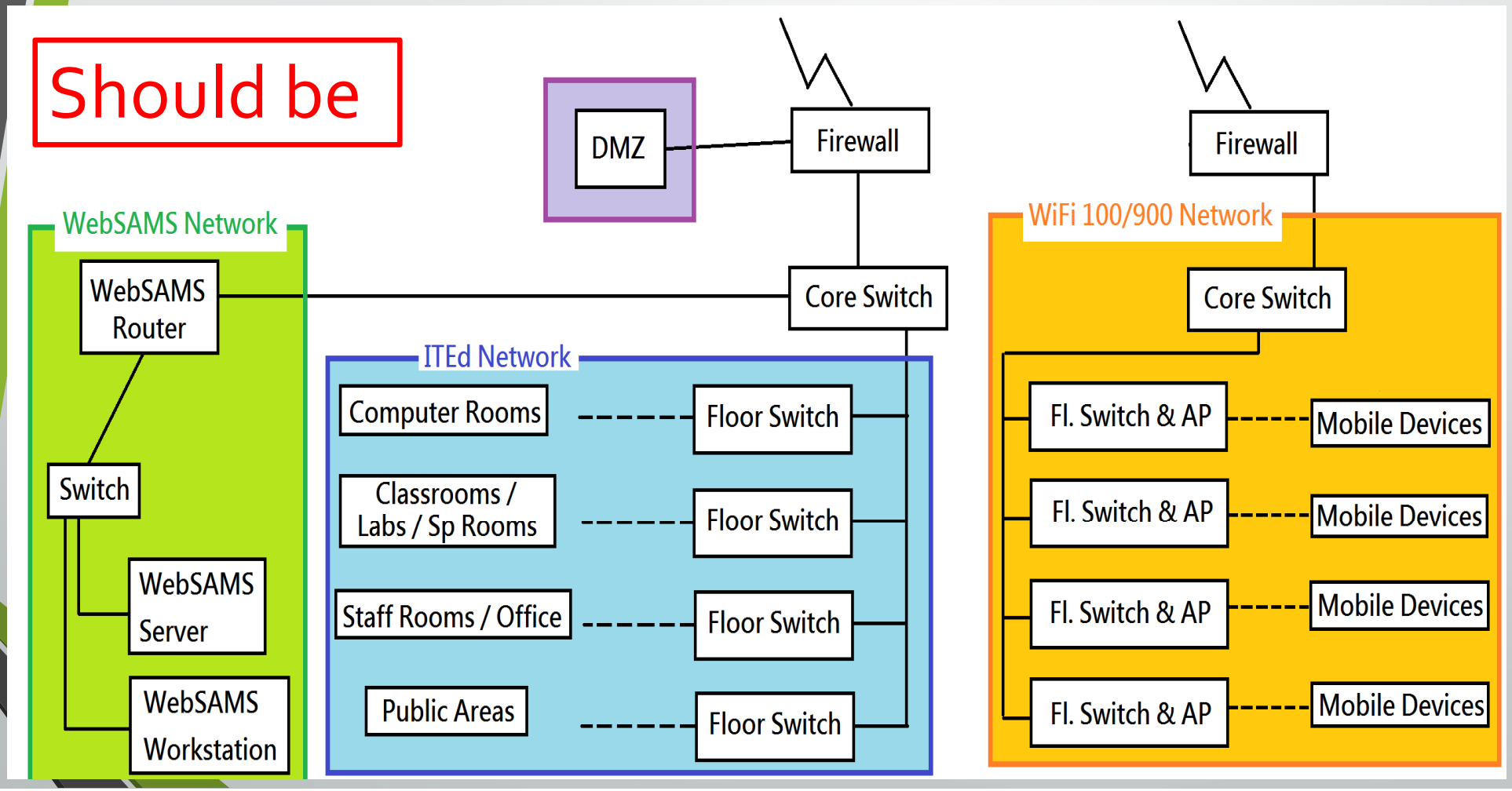
基本學校網絡佈局



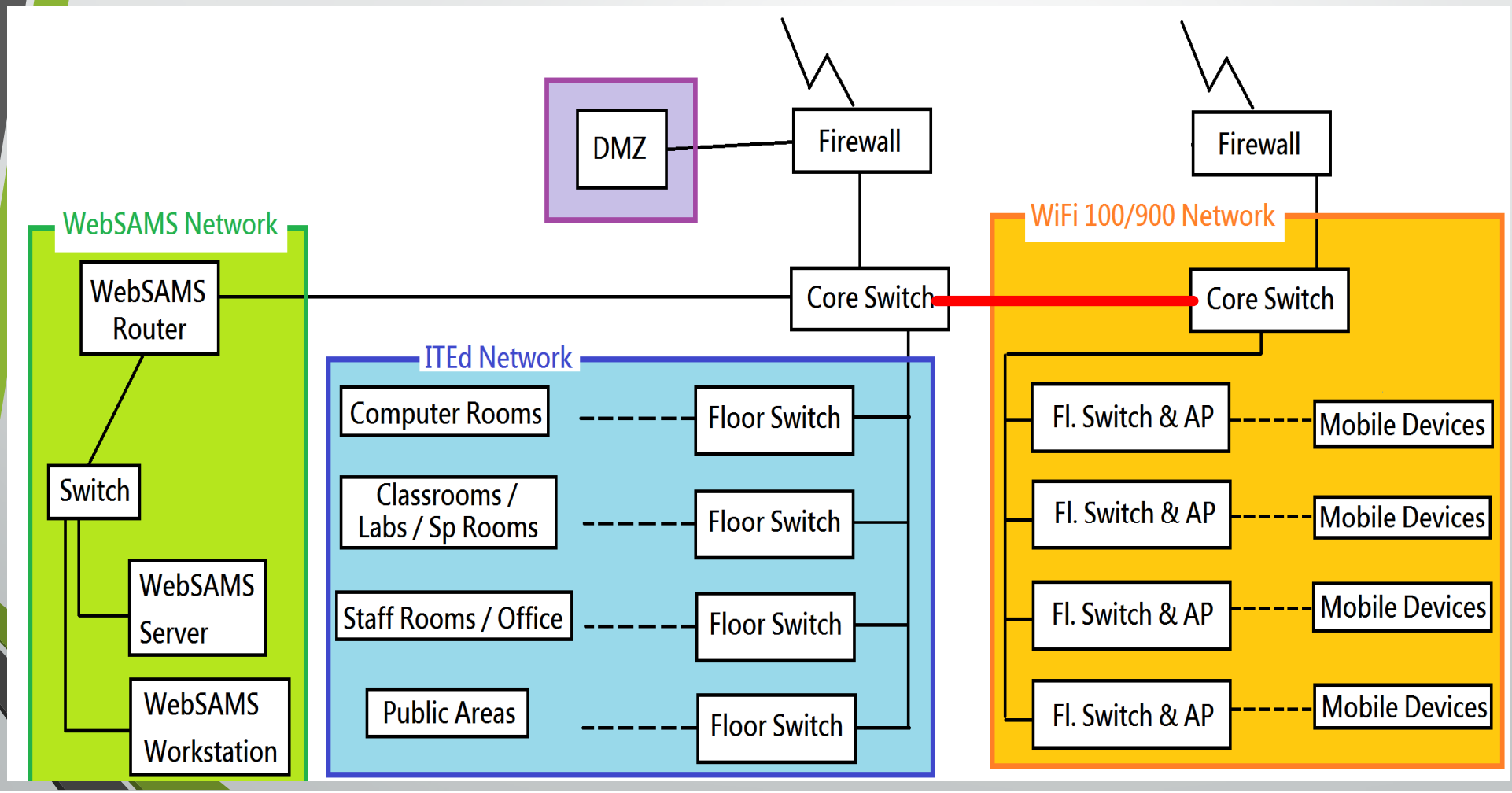
基本學校網絡佈局


Should be
DMZ
Firewall
WebSAMS Network
WebSAMS Router
Switch
WebSAMS Workstation
Staff Rooms / Office
Public Areas
Floor Switch
Floor Switch
Fl. Switch & AP
Fl. Switch & AP
Fl. Switch & AP
Mobile Devices
Mobile Devices
Mobile Devices
Mobile Devices
有多少學校遵從？

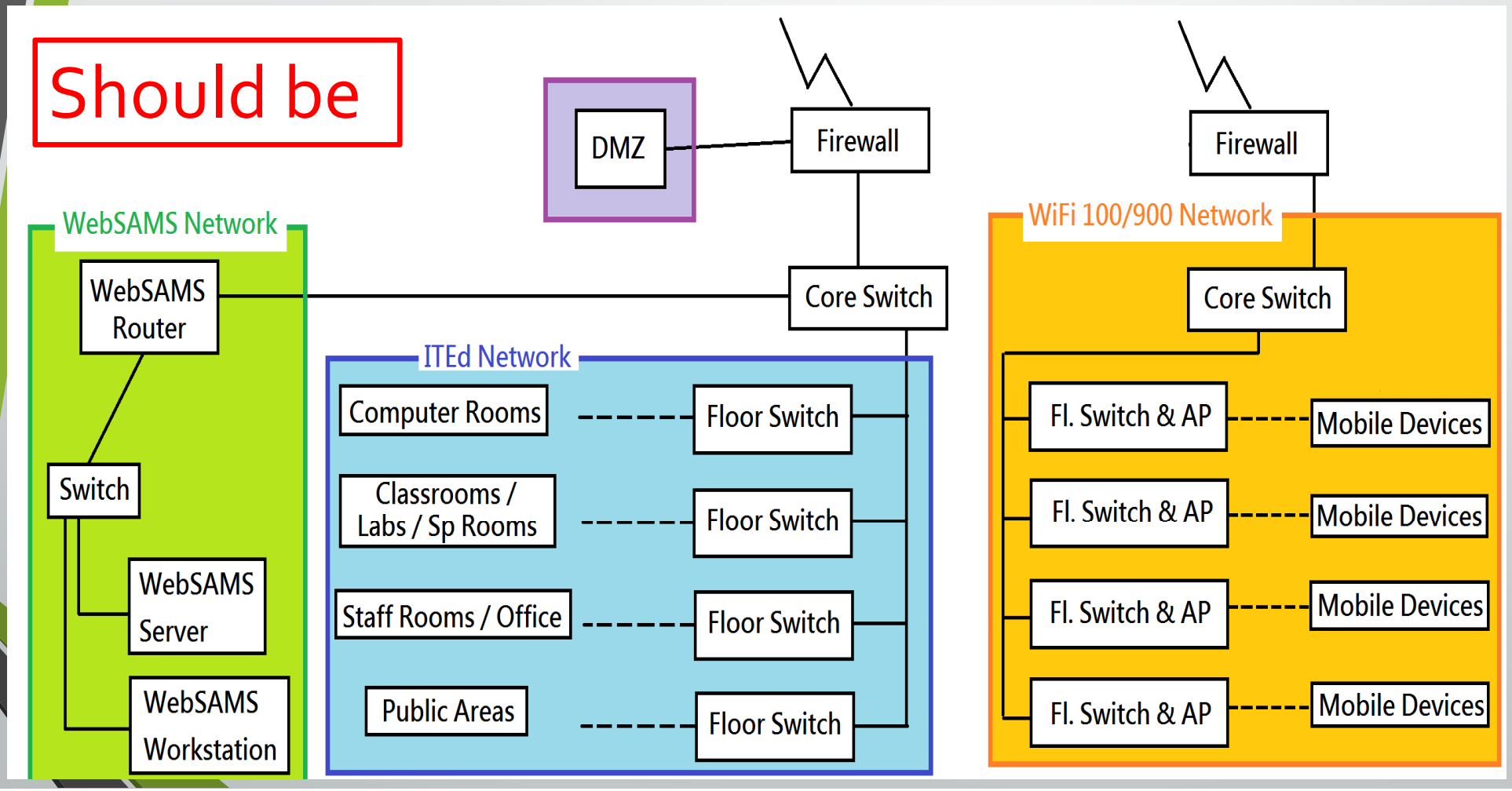
基本學校網絡佈局


Should be
DMZ
Firewall
Firewall
WebSAMS Network
WebSAMS Router
Core Switch
Core Switch
WiFi 100/900 Network
ITEd Network
Switch
WebSAMS Server
WebSAMS Workstation
Computer Rooms
Classrooms / Labs / Sp Rooms
Staff Rooms / Office
Public Areas
Floor Switch
Floor Switch
Floor Switch
Floor Switch
Fl. Switch & AP
Fl. Switch & AP
Fl. Switch & AP
Fl. Switch & AP
Mobile Devices
Mobile Devices
Mobile Devices
Mobile Devices

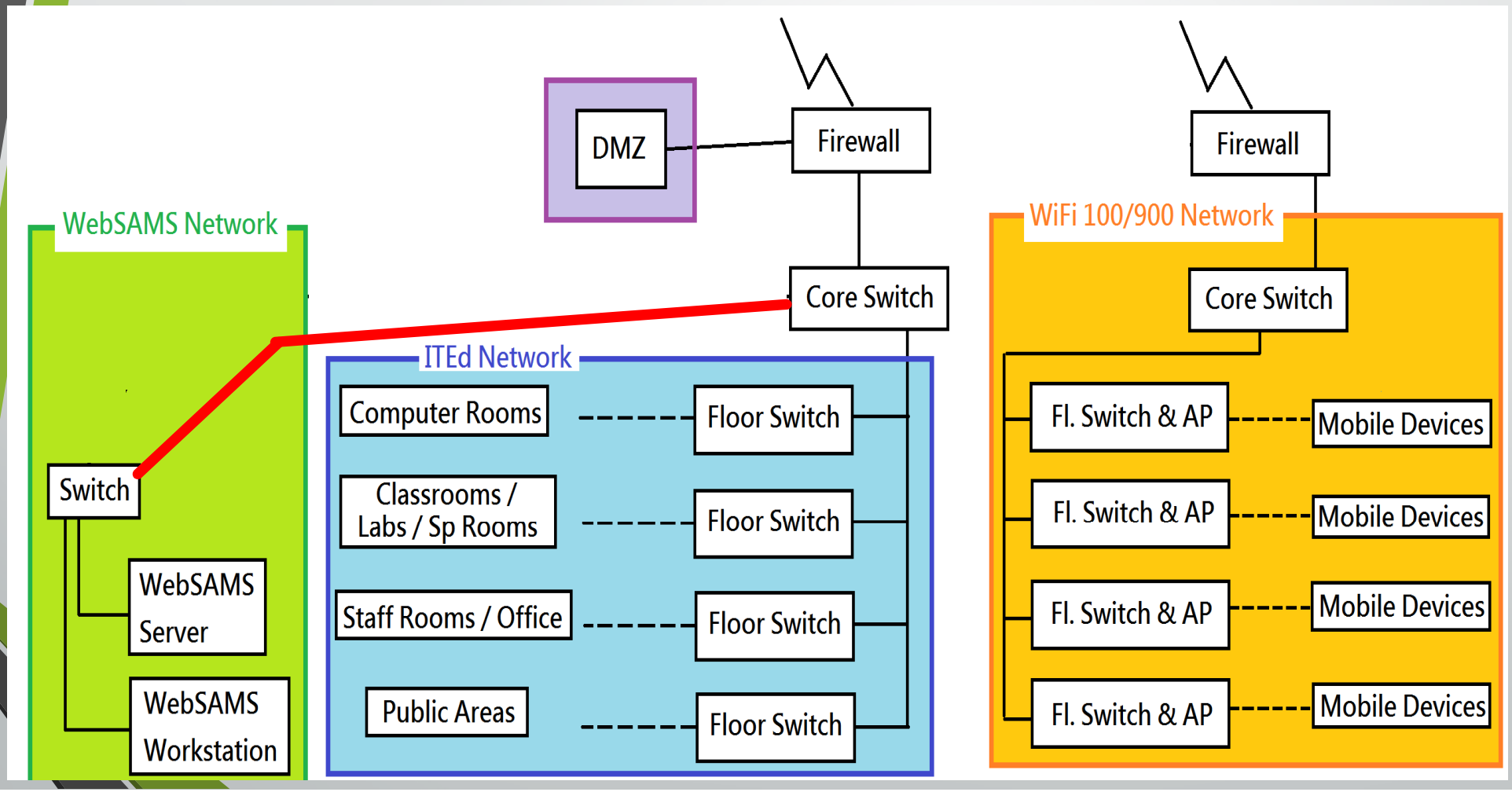
？？學校網絡佈局


DMZ
Firewall
Firewall
WebSAMS Network
WebSAMS Router
Core Switch
Core Switch
WiFi 100/900 Network
ITEd Network
Switch
WebSAMS Server
WebSAMS Workstation
Computer Rooms
Classrooms / Labs / Sp Rooms
Staff Rooms / Office
Public Areas
Floor Switch
Floor Switch
Floor Switch
Floor Switch
Fl. Switch & AP
Fl. Switch & AP
Fl. Switch & AP
Fl. Switch & AP
Mobile Devices
Mobile Devices
Mobile Devices
Mobile Devices

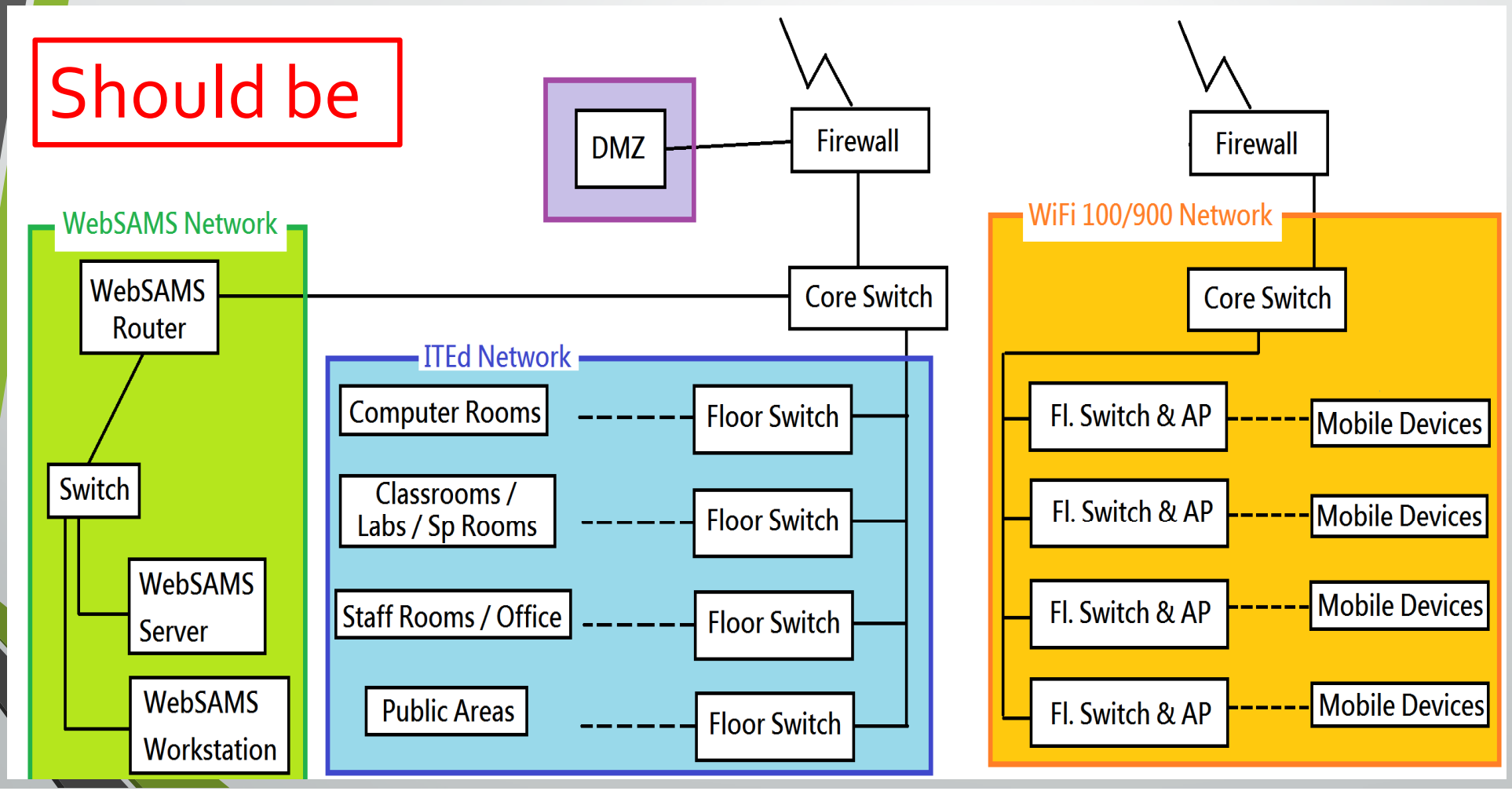
基本學校網絡佈局


Should be
DMZ
Firewall
Firewall
WebSAMS Network
WebSAMS Router
Core Switch
Core Switch
WiFi 100/900 Network
ITEd Network
Switch
WebSAMS Server
WebSAMS Workstation
Computer Rooms
Classrooms / Labs / Sp Rooms
Staff Rooms / Office
Public Areas
Floor Switch
Floor Switch
Floor Switch
Floor Switch
Fl. Switch & AP
Fl. Switch & AP
Fl. Switch & AP
Fl. Switch & AP
Mobile Devices
Mobile Devices
Mobile Devices
Mobile Devices

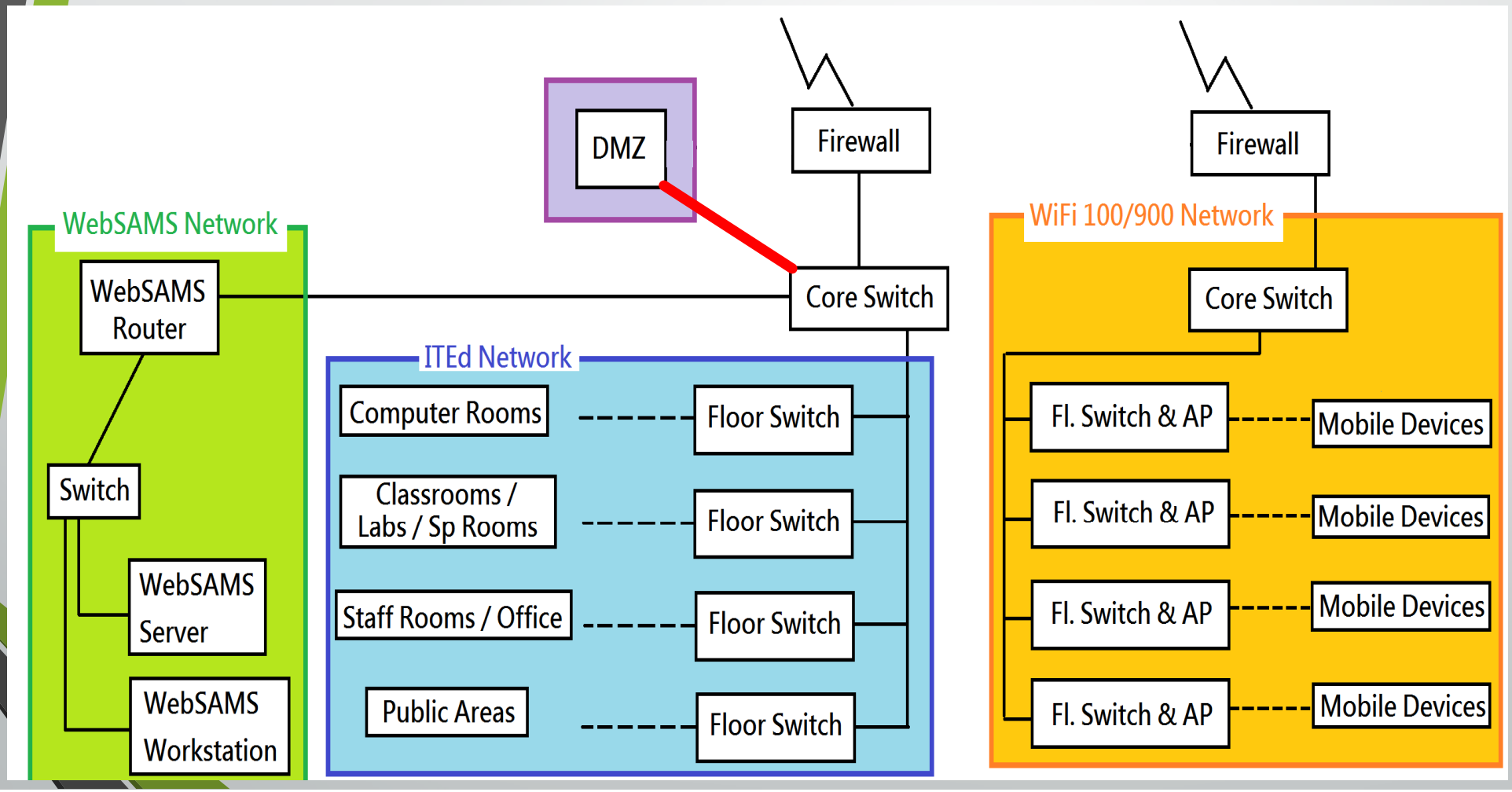
？？學校網絡佈局


DMZ
Firewall
Firewall
WebSAMS Network
Core Switch
Core Switch
WiFi 100/900 Network
ITEd Network
Computer Rooms
Floor Switch
Fl. Switch & AP
Mobile Devices
Switch
Classrooms / Labs / Sp Rooms
Floor Switch
Fl. Switch & AP
Mobile Devices
WebSAMS Server
Staff Rooms / Office
Floor Switch
Fl. Switch & AP
Mobile Devices
WebSAMS Workstation
Public Areas
Floor Switch
Fl. Switch & AP
Mobile Devices

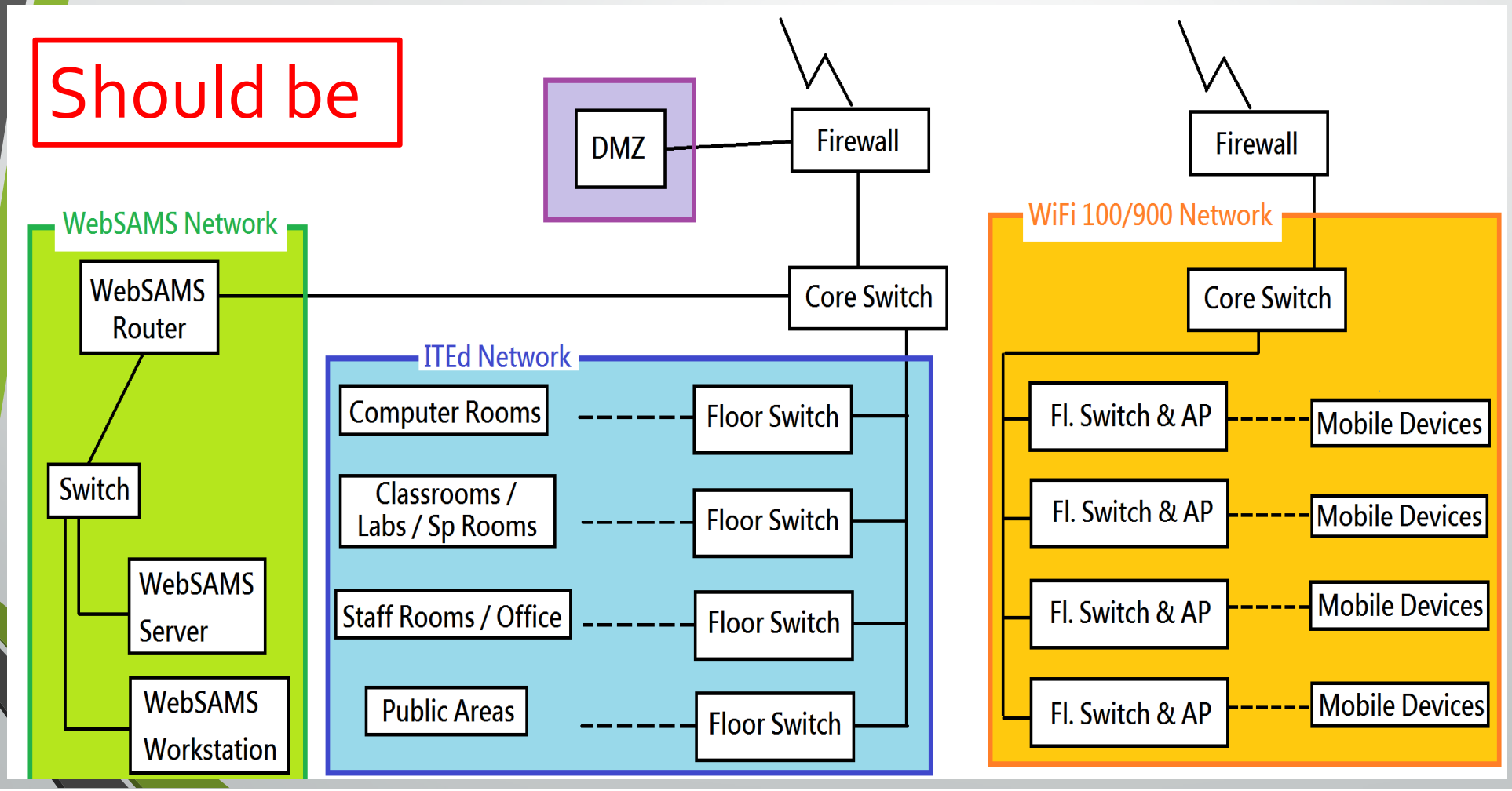
基本學校網絡佈局


Should be
DMZ
Firewall
Firewall
WebSAMS Network
WebSAMS Router
Core Switch
Core Switch
WiFi 100/900 Network
ITEd Network
Switch
WebSAMS Server
WebSAMS Workstation
Computer Rooms
Classrooms / Labs / Sp Rooms
Staff Rooms / Office
Public Areas
Floor Switch
Floor Switch
Floor Switch
Floor Switch
Fl. Switch & AP
Fl. Switch & AP
Fl. Switch & AP
Fl. Switch & AP
Mobile Devices
Mobile Devices
Mobile Devices
Mobile Devices

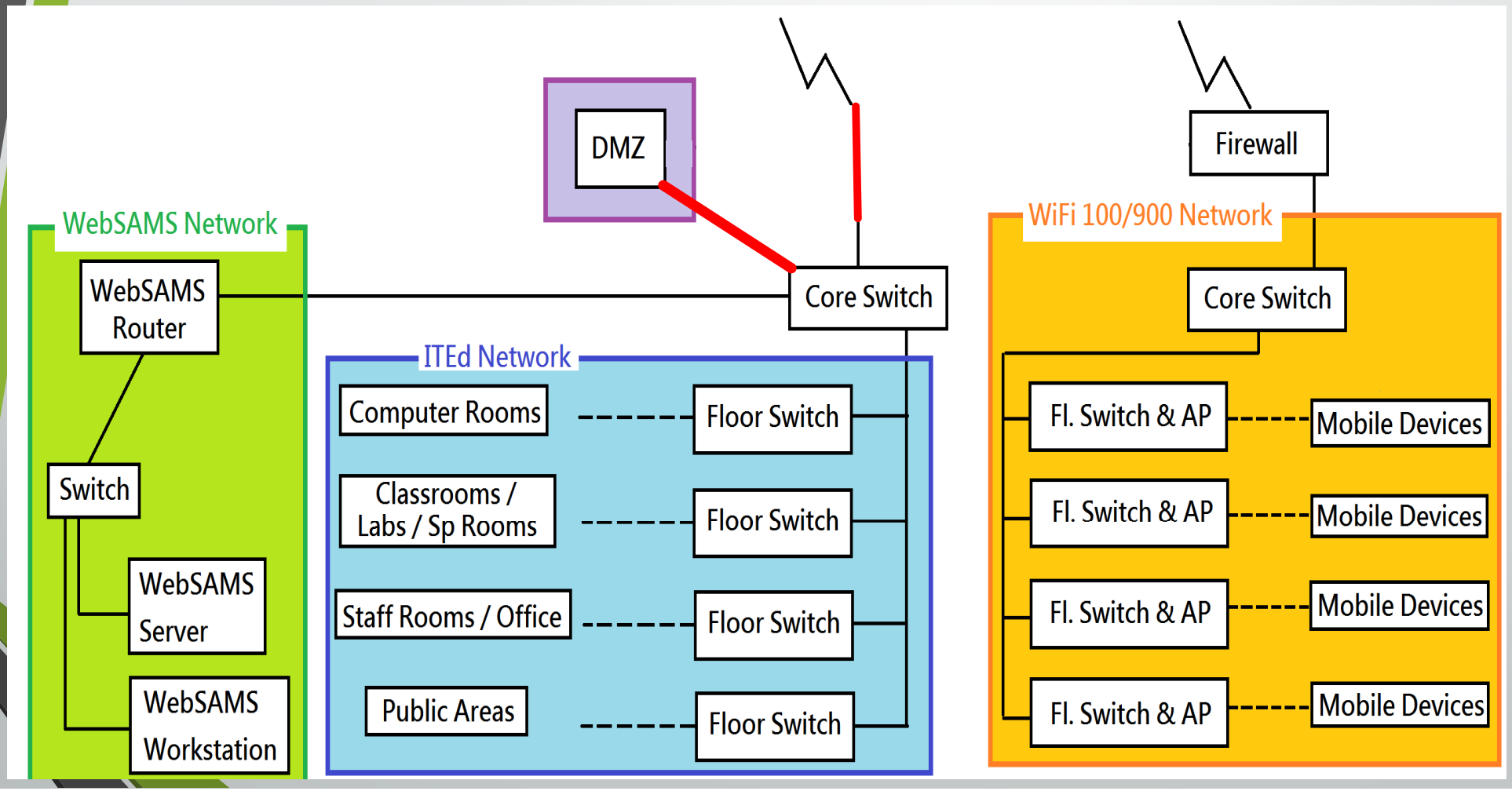
？？學校網絡佈局


DMZ
Firewall
Firewall
WebSAMS Network
WebSAMS Router
Core Switch
Core Switch
WiFi 100/900 Network
ITEd Network
Switch
WebSAMS Server
WebSAMS Workstation
Computer Rooms
Classrooms / Labs / Sp Rooms
Staff Rooms / Office
Public Areas
Floor Switch
Floor Switch
Floor Switch
Floor Switch
Fl. Switch & AP
Fl. Switch & AP
Fl. Switch & AP
Fl. Switch & AP
Mobile Devices
Mobile Devices
Mobile Devices
Mobile Devices

基本學校網絡佈局


Should be
DMZ
Firewall
Firewall
WebSAMS Network
WebSAMS Router
Core Switch
Core Switch
WiFi 100/900 Network
ITEd Network
Switch
WebSAMS Server
WebSAMS Workstation
Computer Rooms
Classrooms / Labs / Sp Rooms
Staff Rooms / Office
Public Areas
Floor Switch
Floor Switch
Floor Switch
Floor Switch
Fl. Switch & AP
Fl. Switch & AP
Fl. Switch & AP
Fl. Switch & AP
Mobile Devices
Mobile Devices
Mobile Devices
Mobile Devices

？？學校網絡佈局


DMZ
Firewall
WebSAMS Network
WebSAMS Router
Core Switch
WiFi 100/900 Network
Core Switch
ITEd Network
Switch
WebSAMS Server
WebSAMS Workstation
Computer Rooms
Floor Switch
Classrooms / Labs / Sp Rooms
Floor Switch
Staff Rooms / Office
Floor Switch
Public Areas
Floor Switch
Fl. Switch & AP
Mobile Devices
Fl. Switch & AP
Mobile Devices
Fl. Switch & AP
Mobile Devices
Fl. Switch & AP
Mobile Devices

既然中咗無得救

唯有盡量唔好中

考慮 / 可考慮

- 教職員教育（再教育）
  - 使用 **incognito browser**
  - 經常（久不久）發提示（恐嚇）電郵
    - **Sample,** 處理手法
  - 同事若不幸中了，會即找（或被找）你
  - 同事權限處理
    - 每年檢視
  - **IT** 支援（備份培訓？備份設備？）

考慮 / 可考慮

- **ITC / TSS / School 層面**
  - 將 **Info Sec** 納入每年 **year plan, budget**
  - 備份（**offline & offsite**）
  - 防毒？
  - 更新 **patch ?**
  - 使用 **well known services**
    - **Google, Microsoft**

考慮 / 可考慮

- ITC / TSS / School 層面
  - Server Migration to Cloud
  - Join Community of Practice
  - Subscribe to HKCERT news
  - Self Health-Check
  - 出席 Info Sec 活動
  - 出席 Info Sec 培訓
    - 使用 ITSSG
  - ……

AiTLE Support on Info Sec

計劃中

- Info Sec
  - Seminar
  - Workshops
- ITC 培訓課程
- TSS 培訓課程

Keep update from AiTLE by

- 參加 AiTLE Whatsapp Groups

https://www.aitle.org.hk/?p=3620

Keep update from AiTLE by

- 成為 AiTLE 會員

AiTLE Resources - 過往活動分享

AiTLE Resources - Computer & STEM Teaching

AiTLE Resources - IT in Education & Administration

AiTLE Resources : Schoolware (by Mr. Chiu KW)

Mr. Albert Wong

IT Manager & Teacher, Ying Wa College (YWC)

Chairman, Association of IT Leaders in Education (AiTLE)

Email : 9028 9443 / albertwong@aitle.org.hk

Website: https://www.aitle.org.hk