Použité zariadenia

* 1 Router-PT
* 1 Switch-PT
* 2 AccessPoint-PT
* 1 PC-PT
* 1 Laptop-PT
* 1 GarageDoor
* 1 Webcam
* 1 Smartphone-PT
* 1 TabletPC-PT

Pracovný postup

1. Pridal som si dané zariadenia na plochu
2. Pospájal som zariadenia automatickým spojením
3. Spustil som router a spojil ho so switchom v CLI nasledujúcimi príkazmi: configure terminal, interface (názov portu na ktorom je switch zapojený do routeru), no shutdown
4. Na access pointoch som nastavil SSID s WPA2-PSK zabezpecenim jedno pre hosti: hostia s heslom: Hostia123, a jedno pre IoT zariadenia: IoT s heslom: IoT12345
5. Rovnaké údaje som nastavil aj na zariadeniach ktoré som chcel k daným access pointom pripojiť
6. Na Switchi som si vytvoril tri Vlany: Vlan 10 pre Domacnost, Vlan 20 pre IoT, Vlan 30 pre Hosti. Priradil som jednotlive Vlany k spravnym portom na ktorych boli zapojene jednotlive časti siete
7. Na routeri som ako default Gateaway nastavil 192.168.1.1

Obrázok, na ktorom je diagram, text, snímka obrazovky

Automaticky generovaný popis

Nastavovanie IP adries

1. Pre Vlan 10:

* Určená pre domáce zariadenia
* Nastavil som DHCP s rozsahom IP adries:192.168.10.0/24
* Ako default gateaway som nastavil 192.168.1.1

1. Pre Vlan 20:

* Určená pre IoT zariadenia
* Podľa zadania som nastavil IP adresy manualne
* IP adresy som nastavil: 192.168.20.2 a 192.168.20.3
* Ako default gateaway som nastavil 192.168.1.1

1. Pre Vlan 30:

* Určená pre zariadenia hostí
* Nastavil som DHCP s rozsahom IP adries: 192.168.30.0/24
* Ako default gateaway som nastavil 192.168.1.1

Nastavenie obmedzenia pre sieť hostia

Pre sieť hostia som nastavil aby z nej nebolo možne komunikovať do ostatných sieti pomocou týchto príkazov

Router(config)# access-list 100 deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255

Router(config)# access-list 100 deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255

Router(config)# access-list 100 permit ip any any

Router(config)# interface vlan 30

Router(config-if)# ip access-group 100 in

Zabezpečenie a zraniteľnosť siete

Na access pointoch som pridal WPA2-PSK šifrovanie a nastavil heslo aby sa bez hesla nevedeli pripojiť k sieti. Nastavil som access listy aby hostia nevedeli komunikovať do iných sieti.

Komplikácie

Keďže som SSID robil cez access point tak som nenašiel možnosť skryť SSID pre sieť IoT. Skúšal som pripojiť SSID IoT k wireless routeru ale potom som nenašiel spôsob ako zakázať sieti hostia komunikovať s inými sieťami.

Keď som chcel nastaviť pre sieť domacnosť a hostia DHCP vypisalo ze DHCP zlyhalo ze sa pouziva APIPA. Skušal som resetovať router ale chyba stale pretrvavala.