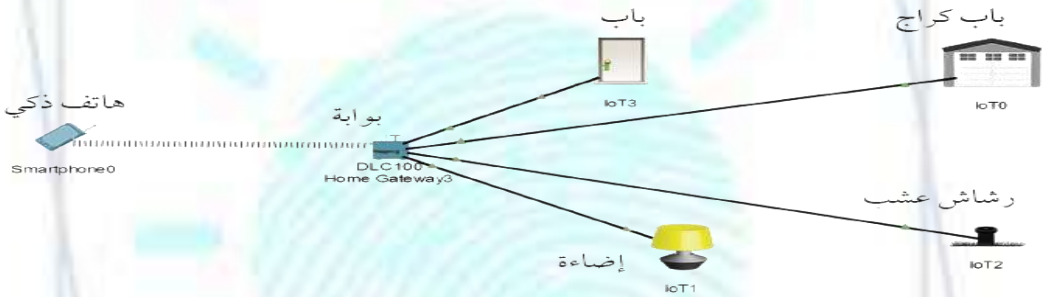
تلخيص الدرس الرابع: تطبيقات عملية لتصميم شبكة إنترنت الأشياء

- ✓ شبكة إنترنت الأشياء (IoT) ليست مجرد امتداد لشبكات الحاسوب السلكية أو شبكات الإنترنت؛ فهي نموذج فريد يعتمد على الربط المباشر بين الأجهزة والأشياء المادية لجمع البيانات ومعالجتها واتخاذ القرارات تلقائياً.
- ✓ يُعد برنامج (Packet Tracer) واحداً من البرامج المناسبة لمحاكاة شبكات إنترنت الأشياء.

➢ أولاً: التحكم في الأجهزة عبر البوابة المنزلية:

- ✓ سيتم تطبيق سيناريو أول لشبكة إنترنت أشياء تتكون من بوابة منزلية، وأربعة أجهزة، وهاتف ذكي واحد.



- ✓ تُضاف الأجهزة إلى الشبكة في منطقة العمل، وتوصل على النحو الآتي:
- ✓ شرح تفصيلي لتطبيق هذا السيناريو في (Cisco Packet Tracer):

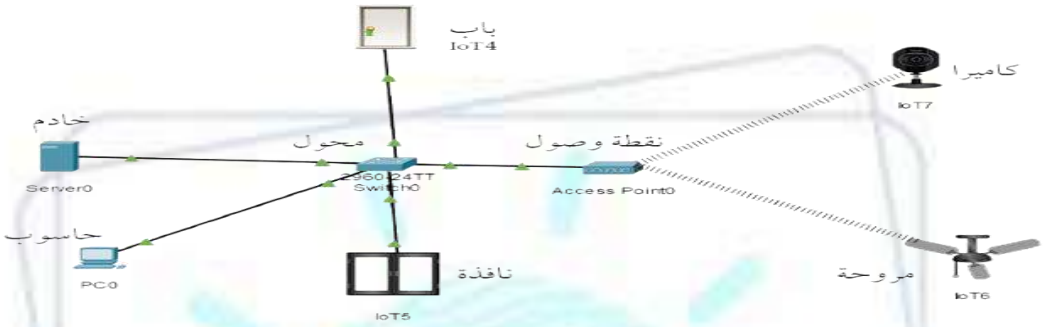
1- إضافة أجهزة الشبكة ووصلها: تُضاف الأجهزة إلى الشبكة في منطقة العمل، وتوصل على النحو الآتي:

- إضافة بوابة منزلية (Home Gateway) وأربعة أجهزة (Light, Lawn Sprinkler, Garage Door, Door) بسحبها من قسم (IoT Devices) إلى منطقة العمل.
- إضافة هاتف ذكي (Smartphone) من قسم (End Devices).
- وصلُ كل جهاز بالبوابة (Home Gateway) بواسطة كبل (FastEthernet).
- وصل الهاتف لاسلكياً باختيار (Wireless) من (Config)، ثم إدخال مُعرّف مجموعة الخدمة (SSID) الظاهر على البوابة.
- تفعيل بروتوكول إعدادات الشبكة والبوابة (DHCP) في كل جهاز باتباع ما يأتي:
  - ✓ Config > Settings > Enable DHCP
  - ✓ Config > Settings > Enable HomeGateway
- وصل الهاتف بالبوابة المنزلية عن طريق نسخ مُعرّف مجموعة الخدمة (SSID) من قسم اللاسلكي:
  - ✓ Config > Wireless –> SSID

2- التحقق من صحة الاتصال:

- يُمكن التحقق من فعالية الاتصال وصحته باستخدام (IoT Monitor) في الهاتف.

➢ ثانياً: التحكم في الأجهزة عبر الخادم والمحوّل ونقطة الوصول (AP):



✓ سننفذ في هذا السيناريو شبكة إنترنت أشياء داخلية باستخدام: جهاز خادم (Server)، ومحوّل (Switch)، ونقطة وصول (Access Point)، أجهزة (IoT) متنوعة (باب، نافذة، كاميرا، مروحة).

✓ شرح تفصيلي لتطبيق هذا السيناريو في (Cisco Packet Tracer):

1- إضافة الأجهزة إلى المشروع:

- أسحب جهاز (Server-PT) من قائمة (End Devices) في قسم (Server).
- أسحب جهاز (PC-PT) من قسم (End Devices).
- أسحب جهاز (Switch-PT) من أجهزة الشبكة (Network Devices) في قسم المحولات (Switches).
- أسحب جهاز (Access Point-PT) من قسم (Wireless Devices).
- أضيف الأجهزة الآتية من قسم (IoT Devices) :

✓ Door (IoT2)

✓ Window (IoT3)

✓ Webcam (IoT4)

✓ Fan (IoT5)

2- وصل الأجهزة:

- أصل بين كل جهازين من الأجهزة الآتية باستخدامِ كبل (FastEthernet):

✓ (Server) مع (Switch).

✓ (PC) مع (Switch).

✓ (Door) و(Window) مع (Switch).

تلخيص الدرس الرابع: تطبيقات عملية لتصميم شبكة إنترنت الأشياء

- أصل بين كل جهازين من الأجهزة الآتية عبر الاتصال اللاسلكي (Wireless):
  - ✓ نقطةُ الوصولِ (Access Point) مع المُحول (Switch).
  - ✓ الكاميرا (Webcam) والمروحة (Fan) مع نقطة الاتصال (Access Point) عن طريق الإعدادات (SSID).

3- إعداد الخادم (Server1):

- اختيار (FastEthernet) من (Config) ثم تعيين الإعدادين الآتيين:
  - ✓ IP Address: 192.168.1.1
  - ✓ Subnet Mask: 255.255.255.0
- تفعيل بوابة (DHCP) من جزء (Services) ثم تعيين الإعدادات الآتية:
  - ✓ Service: ON
  - ✓ Gateway: 192.168.1.1
  - ✓ Starting IP Address: 192.168.1.10
  - ✓ Maximum Users: 20
  - ✓ اختيار (IoT) من (Config) ثم تفعيل الخادم (IoT Server).
- اختيارُ (IoT Monitor) من سطح المكتب (Desktop) ثم إضافة مستخدم على النحو الآتي:
  - ✓ Add User → username: admin | password: 123

4- إعداد أجهزة IoT:

- إعداد الأجهزة المتصلة بالكابل (Door) و(Window):
  - ✓ من Config > Settings أفعل بوابة (DHCP) و(Remote Server).
- إعداد الأجهزة اللاسلكية (Webcam) و(Fan):
  - ✓ أختار Config > Wireless ثم أدخل اسم (SSID) الموجود في (Access Point).
  - ✓ أفعّل بوابة (DHCP) و(Remote Server).

5- إعداد الحاسوب (PC0) على النحو الآتي:

- أختار Config > FastEthernet، ثم أتأكد من الحصول على (IP) تلقائيًا من بوابة (DHCP).
- أختار (IoT Monitor) من سطح المكتب (Desktop)، ثم أسجل عملية الدخول باستخدام:
  - ✓ username: admin | password: 123
- أتأكد من ظهور الأجهزة جميعها.

تلخيص الدرس الرابع: تطبيقات عملية لتصميم شبكة إنترنت الأشياء

6- اختبار الشبكة:

- أتحقق من اتصالات الأجهزة عن طريق (IoT Monitor).
- أضبط شروط تشغيل الأجهزة كما يأتي:
  - ✓ Desktop > IoT Monitor > Conditions
  - ✓ أكتب الشروط المناسبة، مثالًا: إذا انفتح الباب، فإنه يتم تشغيل المروحة أو الكاميرا

➢ إضاءة:

- ✓ عند إعداد شبكة إنترنت الأشياء، يجب التحقق من تفعيل بوابة (DHCP) و(Remote Server) في كل جهاز من أجهزة IoT.
- ✓ يمكن اختبار الاتصالات بالضغط على Alt + Click في الأجهزة.

➢ أسئلة مناقشة:

1- ماذا يحدث إذا لم تفعل بوابة DHCP في أحد الأجهزة؟

- ✓ الحل: إذا لم يتم تفعيل بروتوكول DHCP (بروتوكول تهيئة المضيف الديناميكي)، فلن يتمكن الجهاز من الحصول على عنوان IP تلقائياً من الراوتر، هذا سيؤدي إلى:
  - فشل الاتصال بالشبكة: لن يستطيع الجهاز التواصل مع الأجهزة الأخرى أو الوصول إلى الإنترنت.
  - الحاجة للضبط اليدوي: سيتعين عليك إدخال عنوان IP، وقناع الشبكة (Subnet Mask)، والبوابة الافتراضية (Gateway) يدوياً وبدقة لتجنب تعارض العناوين.

2- إذا أردنا إضافة جهاز إنذار إلى الباب، فكيف يمكن ضبط شرط تشغيله عند الفتح؟

- ✓ الحل: لضبط هذا الشرط، نستخدم عادةً مستشعر تلامس (Magnetic Door Sensor) وبرمجة تعتمد على الحالات المنطقية:
  - المبدأ الفيزيائي: المستشعر يعطي قيمة (1 أو True) عندما يكون الباب مغلقاً (التماس موجود)، وقيمة (0 أو False) عند فتحه.
  - الشرط البرمجي: نضع جملة شرطية في الكود تكون كالتالي:

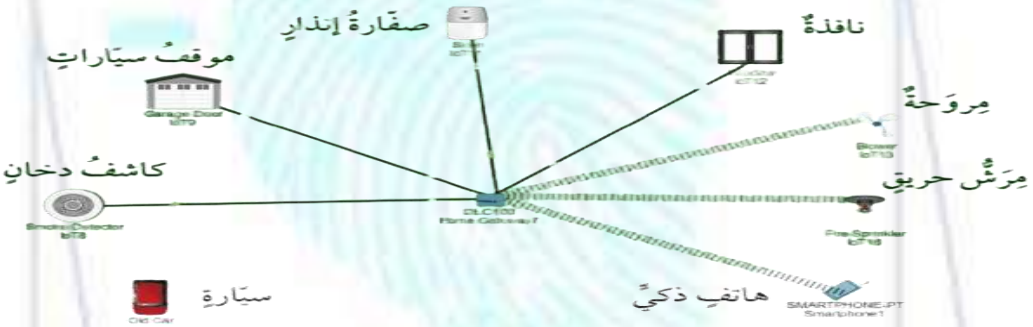
(If (Door_Sensor == 0) then (Turn on Alarm) "إذا كانت قيمة مستشعر الباب تساوي 0 (أي تم قطع التلامس)، قم بتفعيل جرس الإنذار".

3- لماذا تفعل بوابة DHCP في الأجهزة الذكية؟

✓ الحل: يتم تفعيل الـ DHCP في الأجهزة الذكية (مثل المصابيح، الكاميرات، والمستشعرات) للأسباب التالية:

- سهولة الإعداد: تتيح للمستخدم تشغيل الجهاز وربطه بالشبكة فوراً دون الحاجة لخبرة تقنية في تكنولوجيا المعلومات.
- تجنب تعارض العناوين: يقوم الراوتر بتوزيع عناوين فريدة لكل جهاز تلقائياً، مما يمنع حدوث تصادم بين جهازين بنفس العنوان.
- الإدارة المركزية: تسهل على الراوتر إدارة مئات الأجهزة الذكية في وقت واحد وتحديث بيانات الاتصال الخاصة بها تلقائياً عند إعادة تشغيل الشبكة.

➢ ثالثًا: إعداد مطفأة حريق ذكية:



✓ سأنفذ في هذا السيناريو شبكة إنترنت أشياء داخلية تتكون من بوابة منزلية، وستة أجهزة (صفارة إنذار، كاشف دخان، موقف سيارات، نافذة، مرش حريق، مروحة)، وسيارة، وهاتف ذكي.

✓ شرح تفصيلي لتطبيق هذا السيناريو في (Cisco Packet Tracer):

1- سحب الأجهزة (صفارة الإنذار، كاشف الدخان، موقف السيارات، النافذة، مرش الحريق، المروحة، السيارة، الهاتف الذكي) إلى منطقة العمل.

2- وصل الأجهزة باستخدام (FastEthernet) أو الاتصال اللاسلكي.

3- تفعيل بوابة (DHCP) في كل جهاز.

4- تفعيل خيار (HomeGateway).

5- وصل الهاتف بالبوابة المنزلية بنسخ (SSID).

6- ضبط شروط كاشف الدخان بتنفيذ الإجراء الآتي:

✓ SmartPhone > IoT Monitor > Conditions > Add

7- ثم كتابة الشروط:

- ✓ إذا كان مستوى الدخان > 0.1، فإن المروحة تضبط على المستوى المنخفض.
- ✓ إذا كان مستوى الدخان > 0.15، فإن جميع الأجهزة تشغل وتدار وفق الحد الأقصى.
- ✓ إذا كان مستوى الدخان > 0.05، فيجب إيقاف عمل جميع الأجهزة، وضبطها وفق الحد الأدنى.

8- التحقق من صحة الاتصال بطريقتين:

- ✓ الطريقة الأولى: SmartPhone > IoT Monitor
- ✓ الطريقة الثانية: SmartPhone > web browser

9- اختبار كاشف الدخان بالضغط على Alt + Click في السيارة.

تلخيص الدرس الرابع: تطبيقات عملية لتصميم شبكة إنترنت الأشياء

➢ أقيّم تعلّمي:

- المعرفة: أستخدم ما تعلمته من معارف في هذا الدرس للإجابة عن الأسئلة الآتية:

- السؤال الأول: أذكر القائمة في برنامج (Packet Tracer) التي أتوصل بها إلى كل جهاز من الأجهزة الآتية: صفارة الإنذار، الهاتف الذكي، المحول، البوابة، الخادم.

✓ الحل: - صفارة الإنذار: قسم (IoT Devices) أو (End Devices) حسب التصنيف في البرنامج.

- الهاتف الذكي: قسم (End Devices).

- المحول: قسم أجهزة الشبكة (Network Devices) ← قسم المحولات (Switches).

- البوابة: قسم (Wireless Devices) أو (Network Devices).

- الخادم: قسم (End Devices).

- السؤال الثاني: فيم يستفاد من تفعيل بوابة (DHCP) في كل جهاز من أجهزة الشبكة؟

✓ الحل: يستفاد من تفعيل بوابة (DHCP) في توزيع عناوين IP تلقائياً على الأجهزة المتصلة بالشبكة، مما يسهل عملية الاتصال ويجنب المستخدم عناء تعيين العناوين يدوياً لكل جهاز، ويضمن عدم وجود تعارض في العناوين.

- السؤال الثالث: أوضح طريقة تعيين عنوان (IP Address) لأجهزة شبكة إنترنت الأشياء.

✓ الحل: 1- الدخول إلى إعدادات الجهاز (Config).

2- اختيار واجهة الاتصال المناسبة (FastEthernet أو Wireless).

3- تفعيل خيار DHCP للحصول على عنوان IP تلقائياً من البوابة.

4- أو تعيين العنوان يدوياً عن طريق إدخال:

✓ IP Address (مثل: 192.168.1.x).

✓ Subnet Mask (مثل: 255.255.255.0).

✓ Default Gateway (عنوان البوابة).