Prepping Your Network for

The Internet of Things

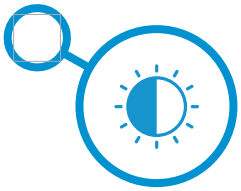
A CHECKLIST OF QUESTIONS FOR OWNERS AND DESIGN PROVIDERS

Part I: Design Considerations

Networks must be appropriately designed to support connectivity within a room, building, or campus. Owners and architects should include design considerations such as the following:

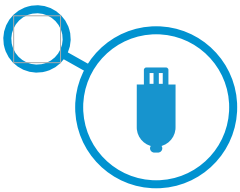
1. Connectivity

Is the cabling or wireless appropriately designed to support all anticipated end device connectivity?



2. Aesthetics

Many of today's technologies can be transparent. Will the connectivity be visibly acceptable?

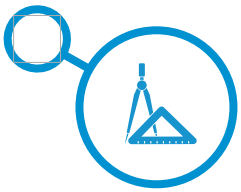


3. Power

Does the end device need to be powered (PoE) from the wired Ethernet network cable?

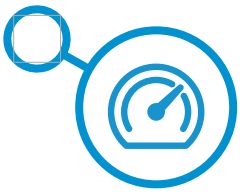
Are the telecom rooms powered and cooled to support the full PoE load?

Is there a need for a UPS?



4. Placement

Clearance requirements, building codes, and cable distances impact telecom room design. Are the telecom rooms appropriately sized and placed?



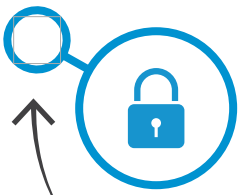
5. Capacity

Is there enough connectivity and bandwidth to support the individual and aggregation device connectivity?

6. Availability

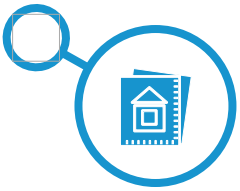
How tolerant is the technology to failures such as power or connectivity loss?

What happens if there is a sub-second, second, minute, hour or day connectivity loss?



7. Security

How will you protect your devices from hacking? Employ frequent infrastructure audits.



8. Physical Attributes

What is the facility size, layout, and materials? These can all affect systems design.

CHECK IT OFF THE LIST

TEECOM

Part II: Technical Considerations

To develop a network design that addresses the questions on the previous page, your design provider will need to ask facility, business, and the operational manager the following questions:

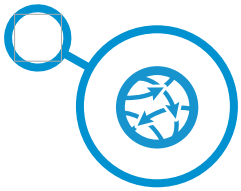
1. Devices

How many devices (servers, desktops, laptops, tablets, phones, etc.) will the network need to support?

2. Connectivity

What types of connectivity are needed - wired, Wi-Fi and cellular?

What amount of connectivity is needed to the internet or other locations?



3. Protocols

Which network protocols will your devices use to identify each other?

Will they be proprietary or open?

4. Architecture

Are there architectural or aesthetic considerations for technology deployment?

5. Network

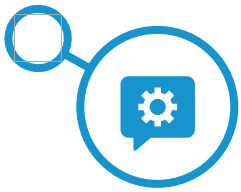
How tolerant will occupants and equipment be to network disruptions?

6. Standards

What standards must the network design adhere to?

Part III: Best Practices

A sustainable long-term IoT strategy must address questions of operation and maintenance. This may involve incorporating new mechanisms and processes. Owners and administrators should consider the following:



1. Support

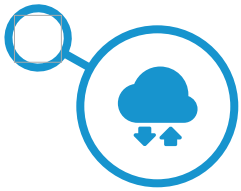
How will the network be supported?

Is the proposed network aligned with an existing support team?

Will the network require automated or external support?

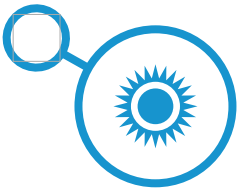
2. Security, Again

Are you regularly introducing new consumer devices connected to your IoT? Plan how you will track them and maintain their security profiles.



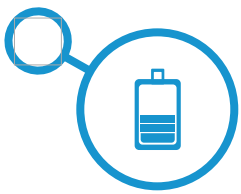
3. Data Aggregation

Which tools will you use to collect, control, and parse the data that will be produced by the devices on your IoT?



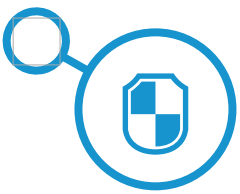
4. Environment

How will physical operating conditions affect your devices and sensors (temperature, moisture, vibration, etc.)?



5. Energy

Devices connected to a network require power, either through in-line connection or batteries. Consider power-aware routing and sleep-scheduling protocols.



6. Access

Is physical security of your hardware an issue? Tampering alerts may be incorporated into the data stream to alert operators or administrators.

Have more questions to check off your list? Contact us!

Bob Fluegge, CCNA
Director of Network Engineering at TEECOM
bob.fluegge@teecom.com

teecom.com