USE MULTIPLE ROUTERS TO PROTECT AGAINST "IoT" INSECURITY

by Francis Chao
fchao2@yahoo.com

Web Location for Presentations:

http://aztcs.org

Click on “Meeting Notes”

SUMMARY

- "Internet of Things" (IoT) devices come with a proprietary Internet access methodology that is controlled by their manufacturers. Having IoT devices share the same router as a computer or tablet is not recommended. We recommend a 2 (or more) router solution for connecting "IoT" devices your home or small business network.

TOPICS

- Basic Advice About Routers
- Basic Assumptions
- Two Router Configuration
- Three Router Configuration
- Activate "Access Point" Isolation on More Expensive Routers

BASIC ADVICE ABOUT ROUTERS

- One of the best descriptions of securing local networks for insecure "Internet of Things" devices can be found at https://shkspr.mobi/blog/2016/03/designing-a-home-network-for-hostile-devices/

BASIC ADVICE ABOUT ROUTERS (continued)

- See also https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/protect-home-network-securing-router

BASIC ADVICE ABOUT ROUTERS (continued)

- See also https://www.welivesecurity.com/2017/10/26/secure-your-router-prevent-iot-threats/

2 Divide and triumph: separate devices

Most of the modern Internet Routers of Things allow you to create different networks for different purposes. A good practice is to take advantage of this function and create separate networks, so as to expose as little as possible when using the most sensitive devices.

BASIC ADVICE ABOUT ROUTERS (continued)

- See also
- https://www.csoonline.com/article/3085607/internet-of-things/8-tips-to-secure-those-iot-devices.html

2. Create a separate network

Many Wi-Fi routers support guest networking so that visitors can connect to your network without gaining access to shared files or networked devices. This kind of separation also works well for IoT devices that have questionable security.

BASIC ADVICE ABOUT ROUTERS (continued)

- We agree with the general concept of using a "guest Wi-Fi network" inside an existing router but having multiple virtual routers inside a single router is usually a lot more susceptible to malware relative to having separate routers with uniquely different usernames and passwords.

BASIC ADVICE ABOUT ROUTERS (continued)

- See
- https://www.tomsguide.com/us/secure-smart-home-how-to,news-19380.html

So what can someone who's already bought one of these devices do? When it comes to the so-called Internet of Things and the connected home, it's best to proactively secure the home network. There is no antivirus software for a smart TV, but you can protect your Wi-Fi network so hacking the TV doesn't become a backdoor into your home.

BASIC ASSUMPTIONS

- Assumption One:
  We are using "dumb routers" that generate and assign "private IP addresses" for their local network-attached computers and devices.
- Assumption Two:
  These "dumb routers" do not communicate and coordinate with each other.

MULTIPLE ROUTER CONCEPT

- In the large networks of governments, large businesses, and educational institutions, multiple tree-like levels of routers (both actual and virtual) have been the normal mode of operation for about 40 years

MULTIPLE ROUTER CONCEPT (continued)

- Because of the security risks of using "Internet of Things" (IoT) devices such as Internet-connected home appliances, security cameras, alarm systems, environmental sensors, etc., the multiple router method of protecting computer assets will move into the home and small business.

MULTIPLE ROUTER CONCEPT (continued)

- There are two main versions of the "Multiple Router Concept:
  - Two Router Configuration
  - Three Router Configuration

TWO ROUTER CONFIGURATION

- "Main router" is usually provided by our "Internet Service Provider" as part of their "broadband modem"

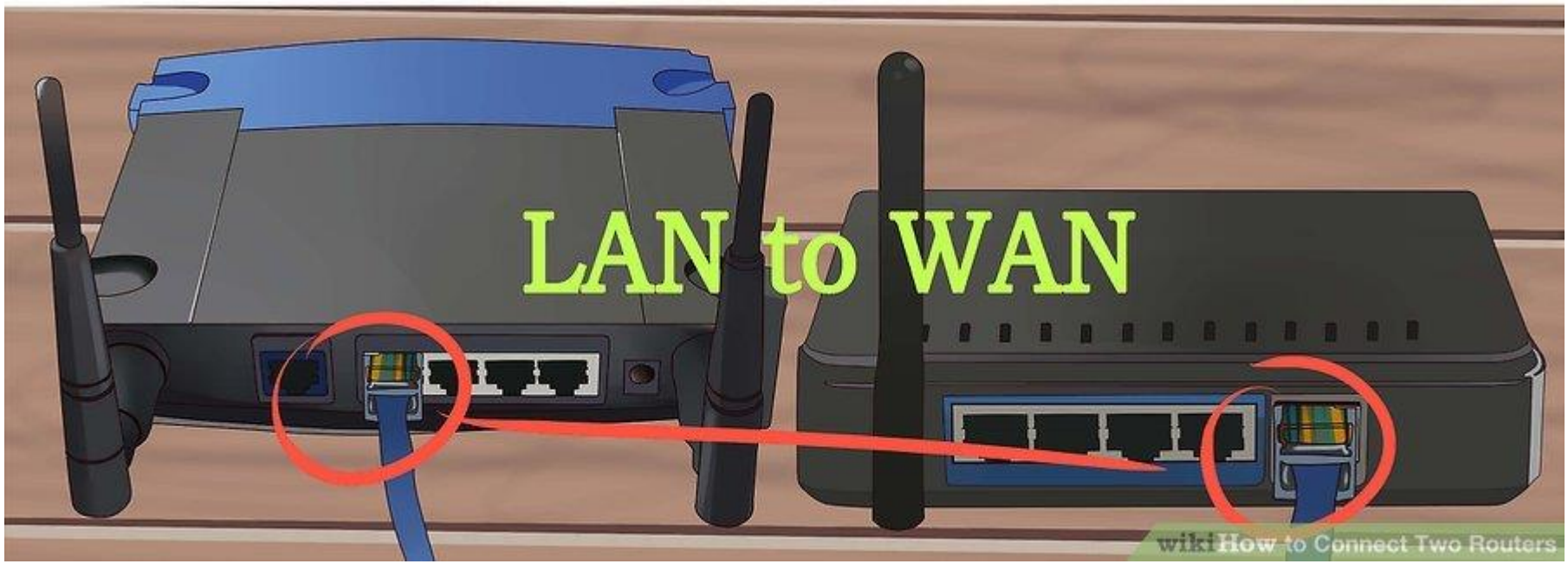

Internet
Border
IOT

TWO ROUTER CONFIGURATION (continued)

- Reference for the previous illustration: https://www.pcper.com/reviews/General-Tech/Steve-Gibsons-Three-Router-Solution-IOT-Insecurity However this article criticizes the two-router configuration as follows:

TWO ROUTER CONFIGURATION (continued)

- "Border router" on the left
  and
  "IOT router" on the right:


LAN to WAN
wikiHow to Connect Two Routers

TWO ROUTER CONFIGURATION (continued)

- If the "border router" is not part of a "broadband modem", then the WAN jack or Internet jack connect here: ("WAN" stands for "Wide Area Network"):


LAN to WAN
wikiHow to Connect Two Routers

TWO ROUTER CONFIGURATION (continued)

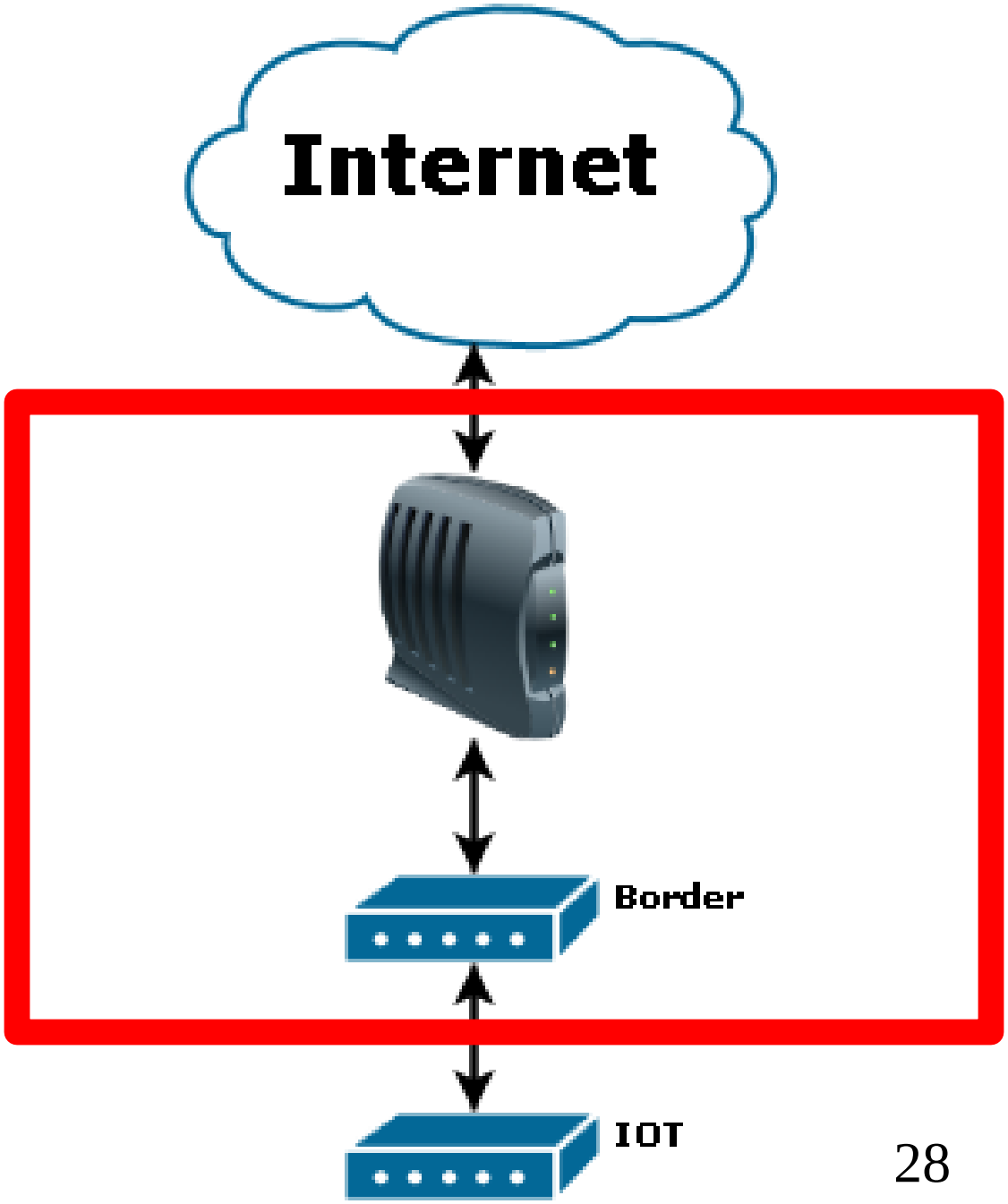
- Reference for the previous two illustrations: https://www.wikihow.com/Connect-Two-Routers

TWO ROUTER CONFIGURATION (continued)

- "LAN to WAN" means that one of the "LAN" jacks of the (left) "border router" is connected to the the "WAN" jack of the (right) "IOT router":

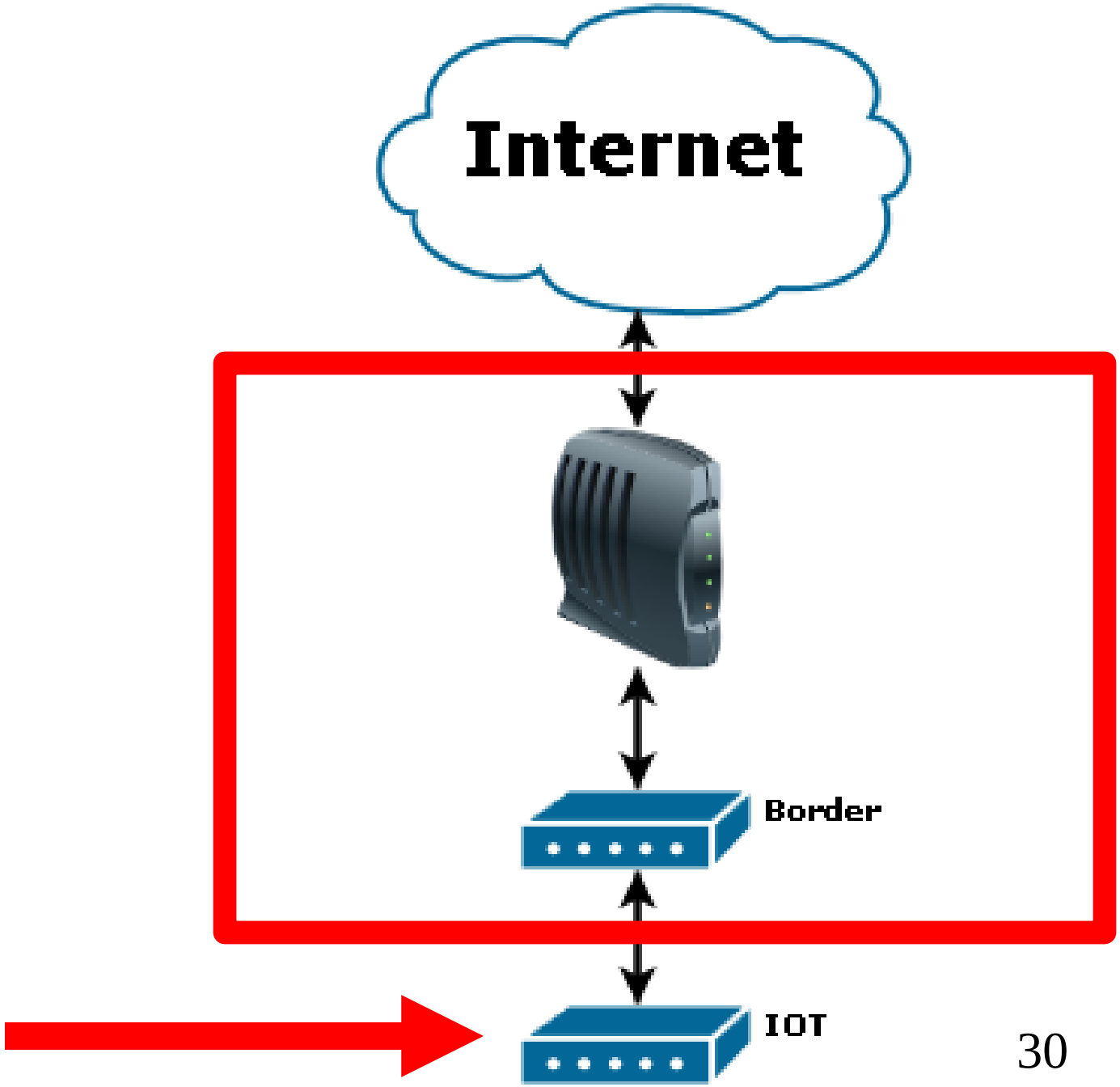
TWO ROUTER CONFIGURATION (continued)

- For most of us, the broadband modem that we rent from our "Internet Services Provider" actually has both a broadband modem and a "border router" inside it:


Internet
Border
IOT

TWO ROUTER CONFIGURATION (continued)

- Therefore, for most of us, adding one additional router brings us to the "two router" configuration:


Internet
Border
IOT

TWO ROUTER CONFIGURATION (continued)

- The article at https://www.pcper.com/reviews/General-Tech/Steve-Gibsons-Three-Router-Solution-IOT-Insecurity criticizes the two-router configuration as follows:

TWO ROUTER CONFIGURATION (continued)

- <Start of quote:>
  In this arrangement, only IOT/Smart devices are connected to the internal (or IOT-purposed) router. The idea was to isolate insecure or poorly implemented devices from the more valuable personal local data devices such as a NAS with important files and or backups.

TWO ROUTER CONFIGURATION (continued)

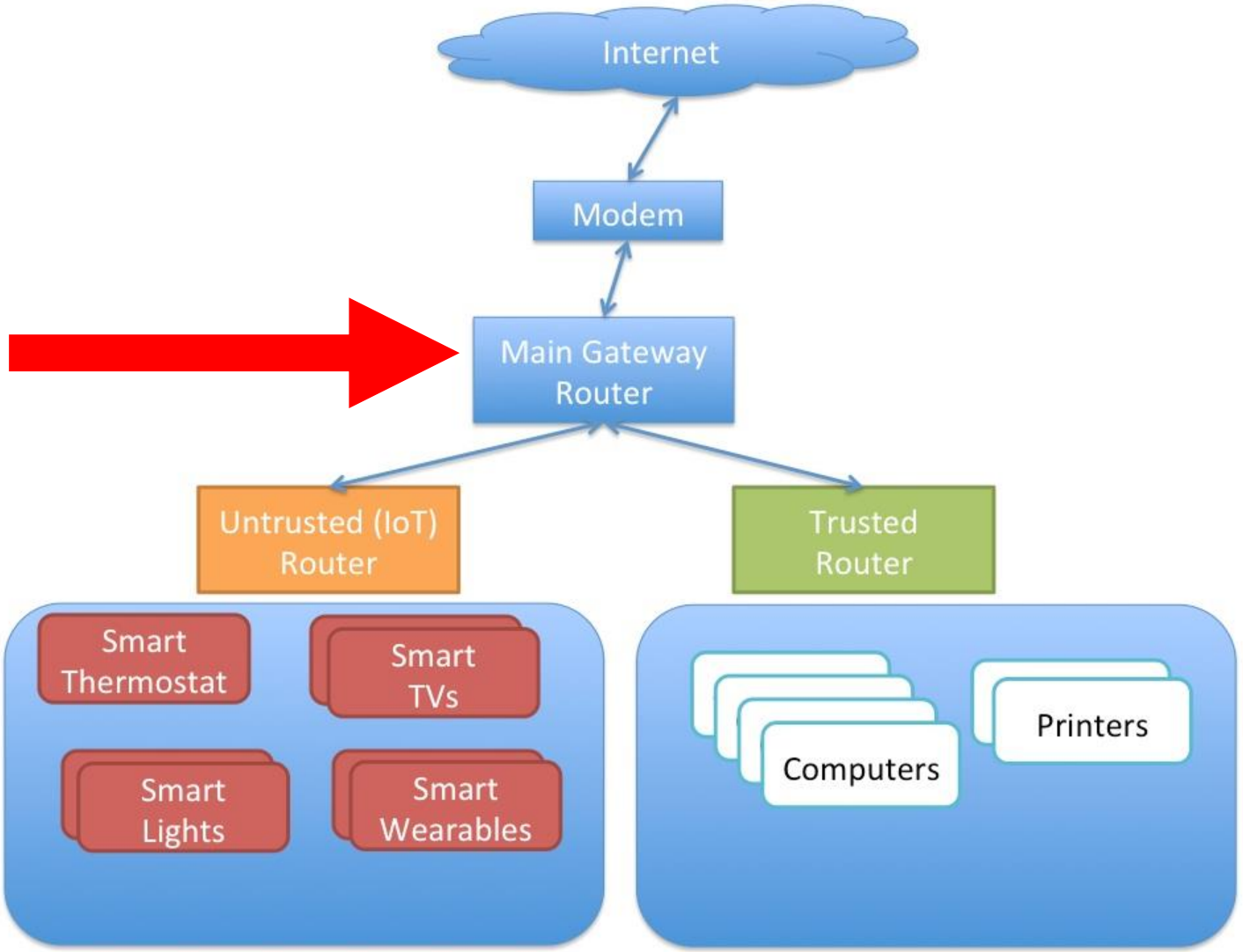
- Unfortunately this clever arrangement leaves any device directly connected to the “border” router open to attack by infected devices running on the internal/IOT router. Said devices could perform a simple trace-route and identify that an intermediate network exists between it and the public Internet.

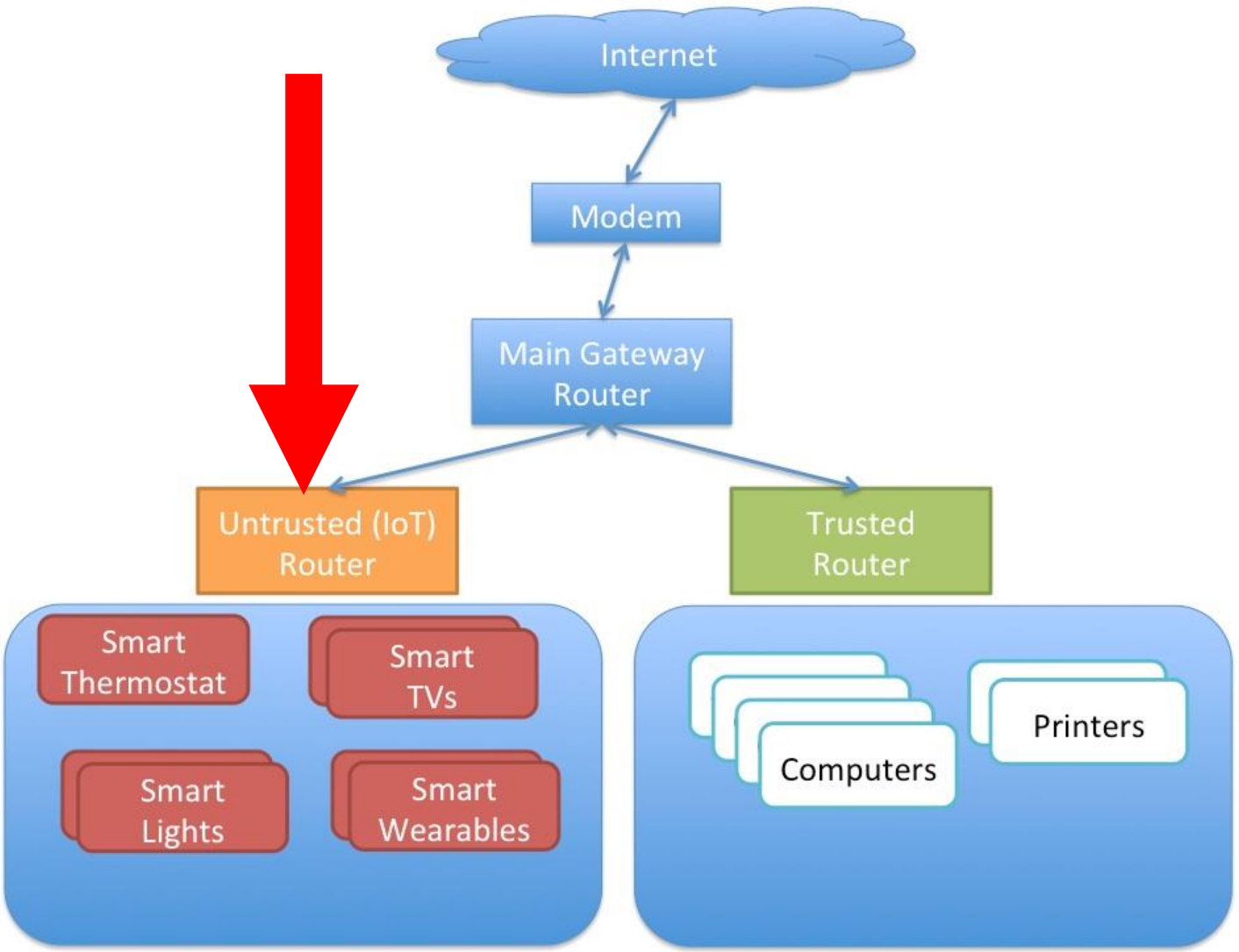
TWO ROUTER CONFIGURATION (continued)

- Any device running under the border router with known (or worse - unknown!) vulnerabilities can be immediately exploited.
<End of quote>

THREE ROUTER CONFIGURATION

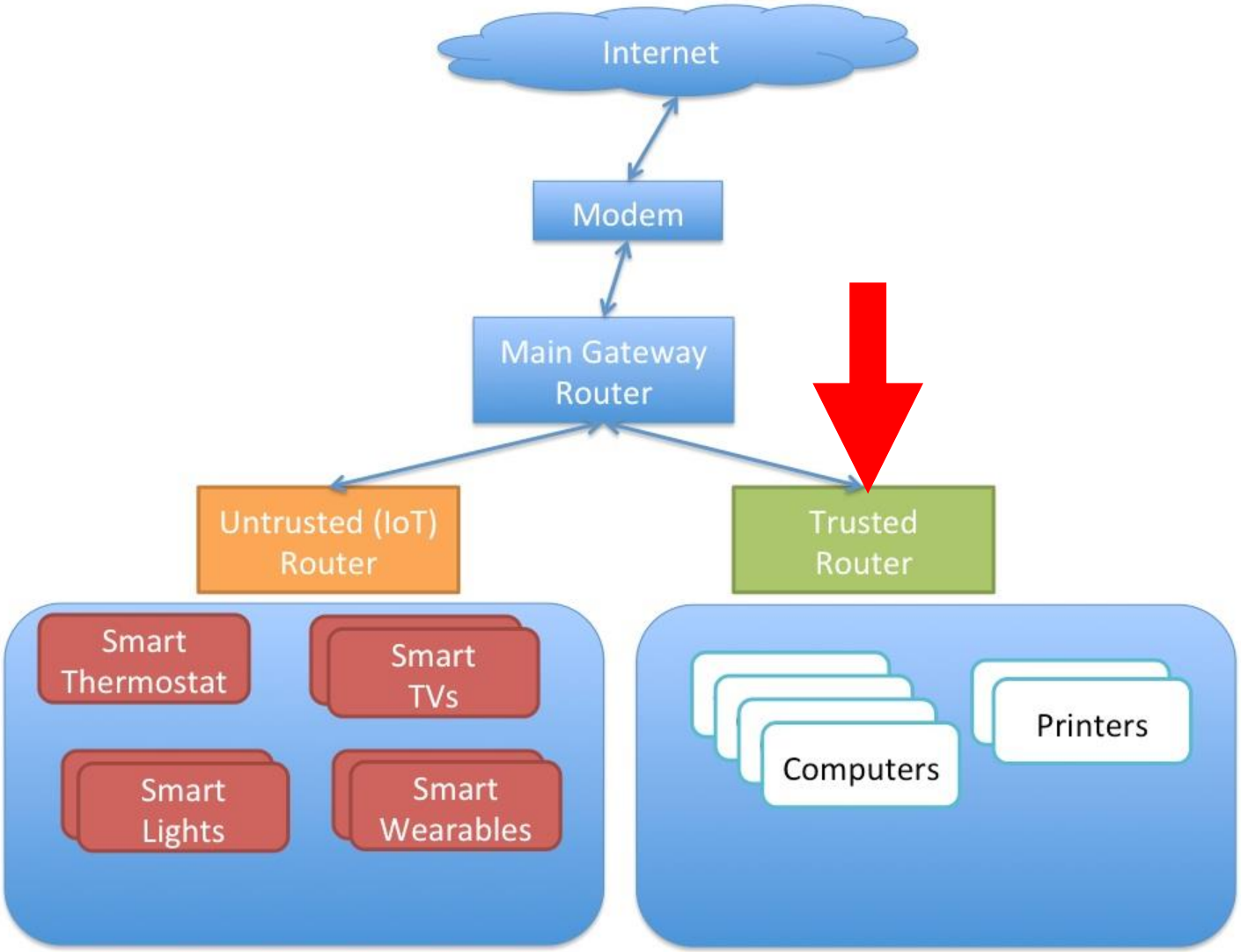
- Untrusted IoT Router:


Internet
Modem
Main Gateway Router
Untrusted (IoT) Router
Trusted Router
Smart Thermostat
Smart TVs
Smart Lights
Smart Wearables
Computers
Printers


Internet
Modem
Main Gateway Router
Untrusted (IoT) Router
Trusted Router
Smart Thermostat
Smart TVs
Smart Lights
Smart Wearables
Computers
Printers

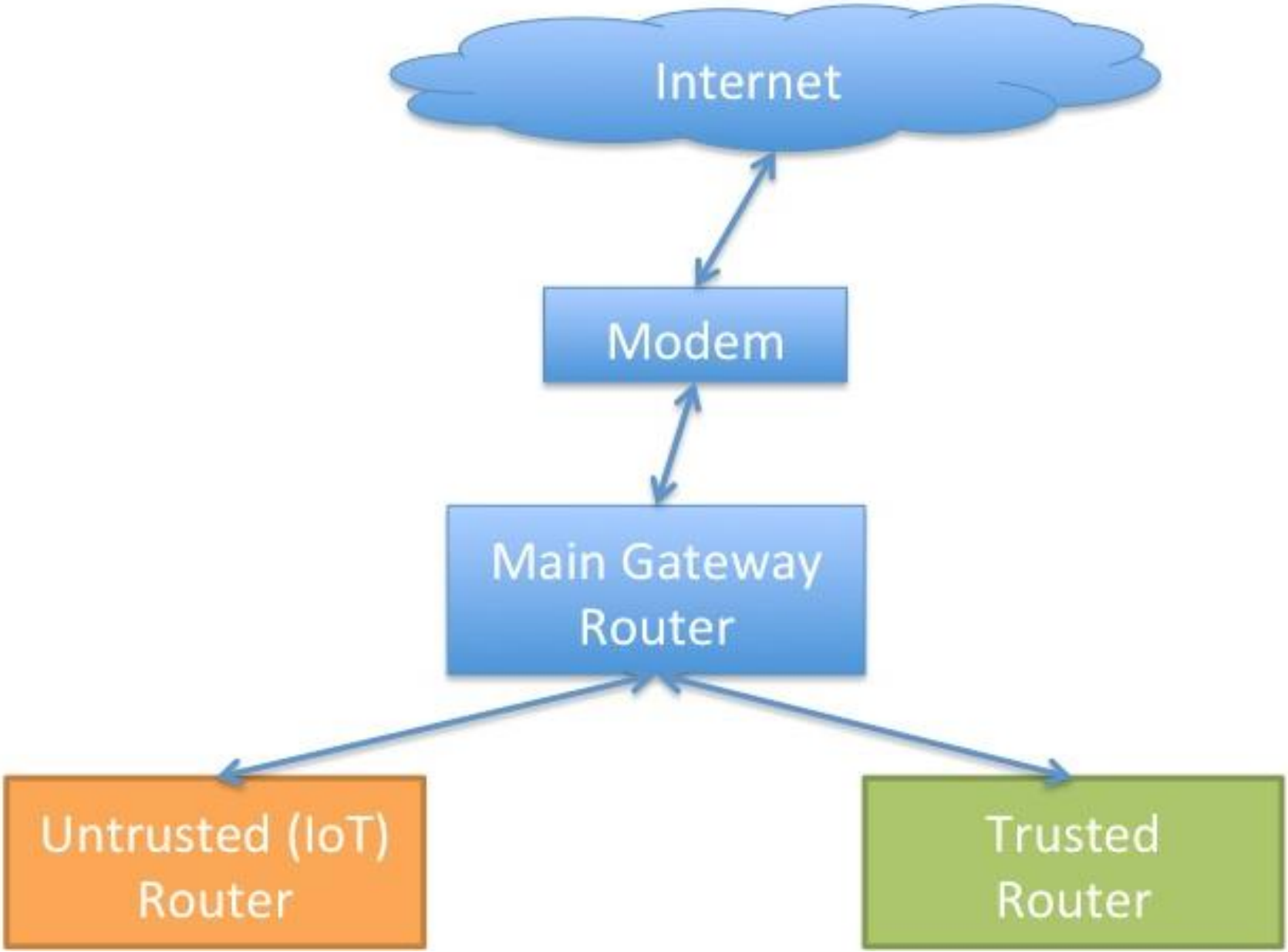
BASIC THREE ROUTER CONCEPT (continued)

- Trusted Router:


Internet
Modem
Main Gateway Router
Untrusted (IoT) Router
Trusted Router
Smart Thermostat
Smart TVs
Smart Lights
Smart Wearables
Computers
Printers

BASIC THREE ROUTER CONCEPT (continued)

- Basic Concept:
  Internet providers modem or router connects to
  Main Gateway Router
  which has a LAN side that connects to Untrusted (IoT) Router
  and
  to Trusted router


Internet
Modem
Main Gateway Router
Untrusted (IoT) Router
Trusted Router

BASIC THREE ROUTER CONCEPT (continued)

- Reference for the previous diagram: http://www.securityperspectives.com/three-dumb-routers-are-coming-to-a-home-network-near-you/

BASIC THREE ROUTER CONCEPT (continued)

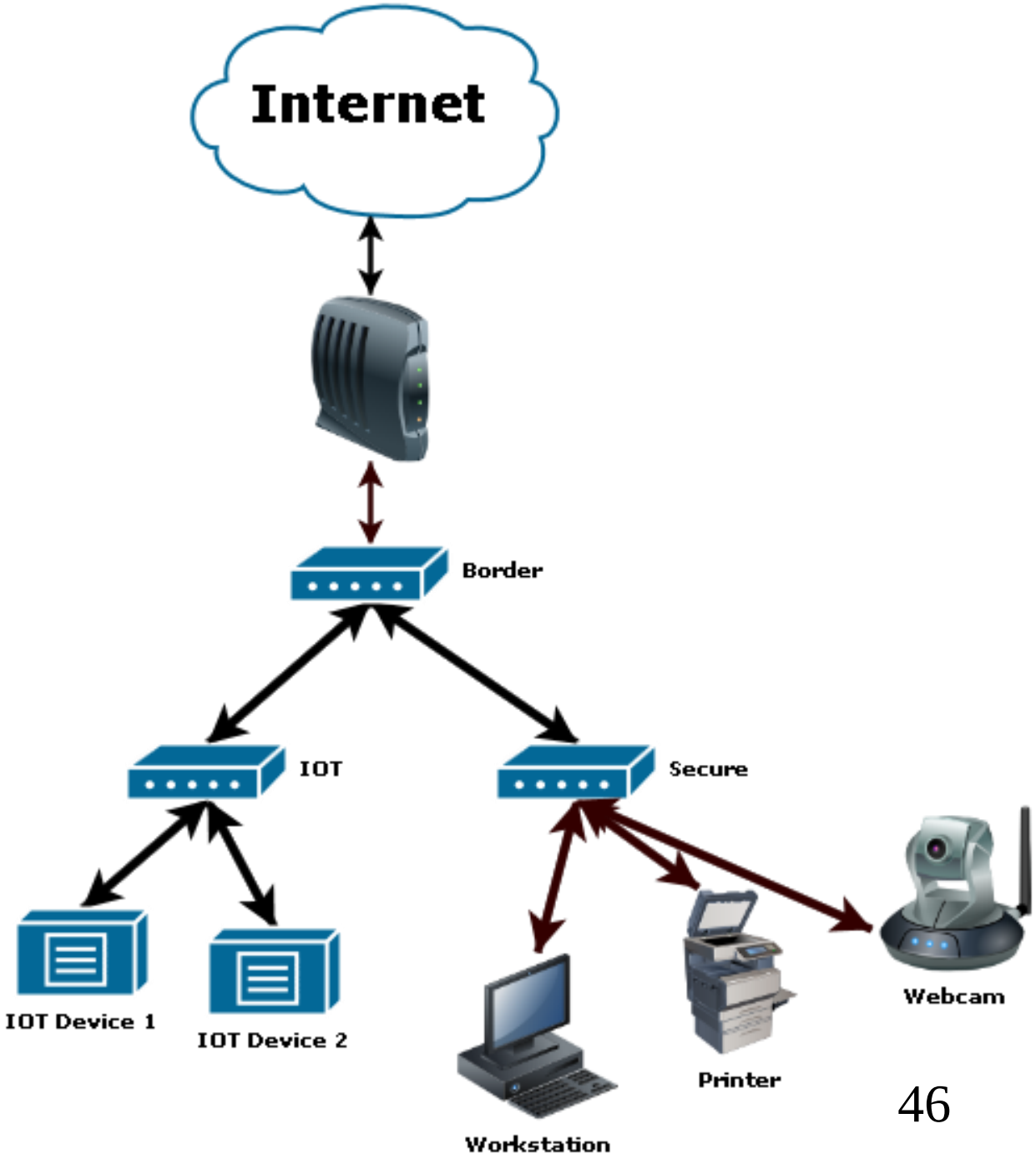
- Also known as "3 dumb routers" as coined by Steve Gibson because the routers that are purchased for homes and small business are much dumber than that ones that larger businesses and organizations use, which, for a home or small business network, may be a good thing.

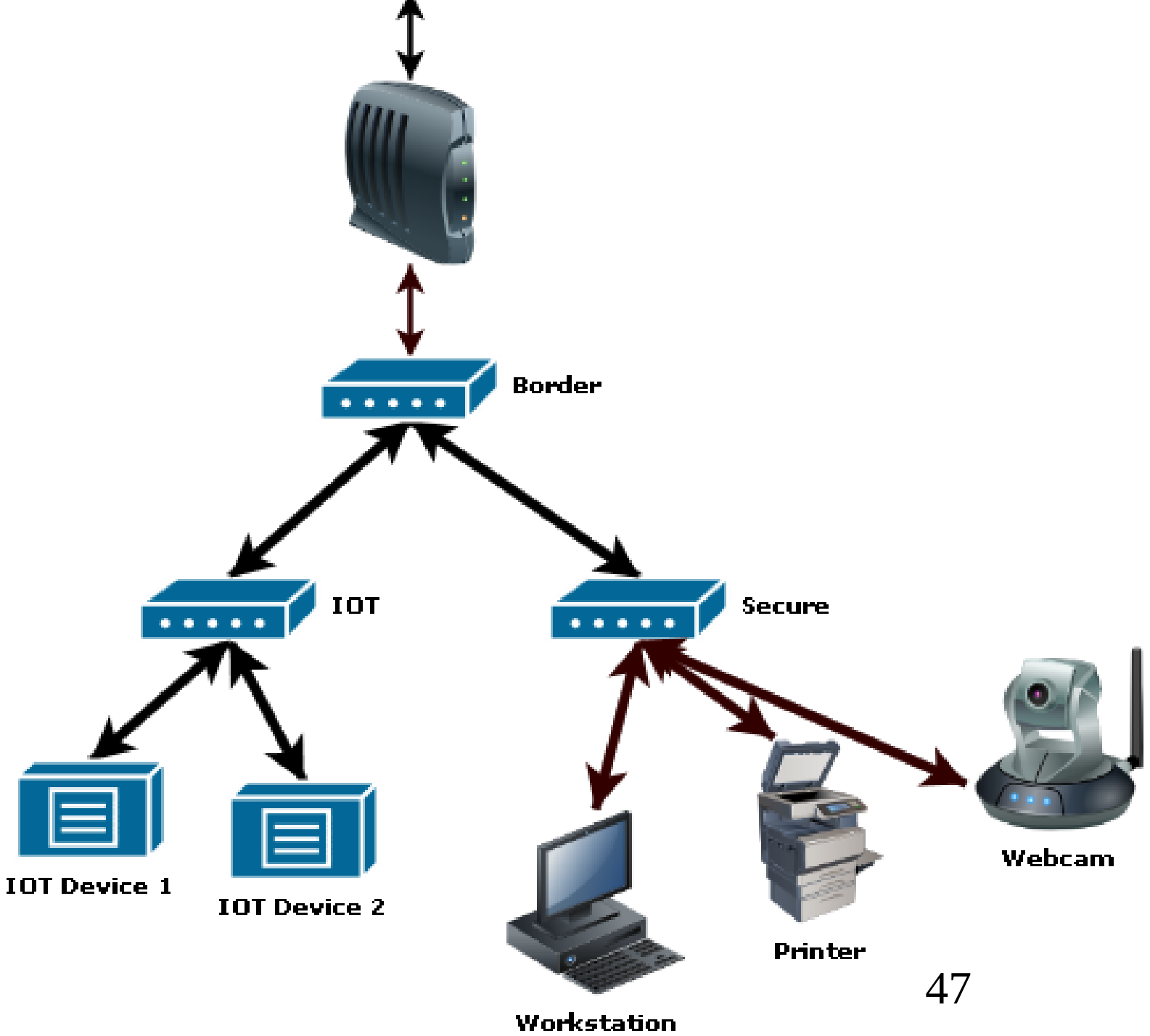
A MORE PROFESSIONAL DESCRIPTION OF THE THREE ROUTER CONCEPT

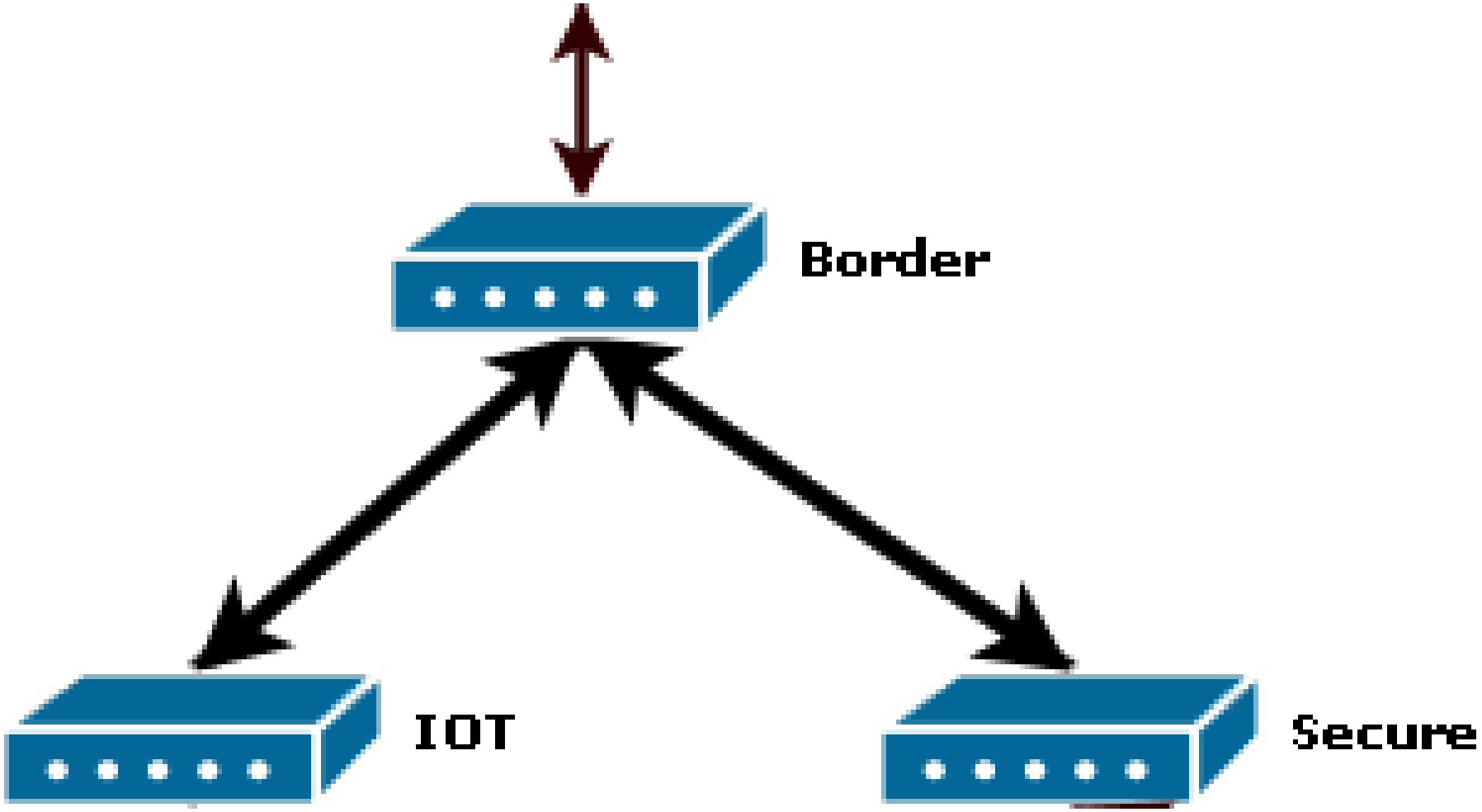
- A more professional description of the 3 router concept along with a more critical view of the details can be found at https://www.pcper.com/reviews/General-Tech/Steve-Gibsons-Three-Router-Solution-IOT-Insecurity

A MORE PROFESSIONAL DESCRIPTION OF THE THREE ROUTER CONCEPT (continued)

- "Main Gateway Router" is usually called "Border Router" by computer and network professionals.
- "Untrusted Router" is now usually called "IoT Router" since "Untrusted.." has a bad connotation.


Internet
Border
IOT
Secure
IOT Device 1
IOT Device 2
Workstation
Printer
Webcam


Border
IOT
Secure
IOT Device 1
IOT Device 2
Workstation
Printer
Webcam


Border
IOT
Secure

A MORE PROFESSIONAL DESCRIPTION OF THE THREE ROUTER CONCEPT (continued)

- For most of us, the "border router" is part of the broadband modem that is provided by our broadband "Internet Service Provider"

ACTIVATE "ACCESS POINT ISOLATION" ON MORE EXPENSIVE ROUTERS

- On more expensive routers, you might be able to activate "wireless isolation" so that each Wi-Fi-connected "Internet of Things" device is isolated from each other and from wired computers on the local network.

ACTIVATE "WIRELESS ISOLATION" ON MORE EXPENSIVE ROUTERS (continued)

- "wireless isolation"
  = "AP isolation"
  = "Access Point isolation"
  = "client isolation"
  = "station isolation"
  = "wireless client isolation"

ACTIVATE "WIRELESS ISOLATION" ON MORE EXPENSIVE ROUTERS (continued)

- "Wireless isolation" means that each Wi-Fi-connected "Internet of Things" device cannot access shared files on any other Wi-Fi-connected or Ethernet-connected device that is connected to the router.

ACTIVATE "WIRELESS ISOLATION" ON MORE EXPENSIVE ROUTERS (continued)

- When you activate "access point isolation", you end up with a separate virtual router for each individual "Internet of Things" device, as described at https://dazeend.org/2017/03/segregating-iot-devices-on-an-isolated-network/

ACTIVATE "WIRELESS ISOLATION" ON MORE EXPENSIVE ROUTERS (continued)

- However, "wireless isolation" is implemented differently in different models of routers, as described at https://jervis.ws/implementing-security-zones-with-home-routers-for-the-iot-early-years/ as follows:

ACTIVATE "WIRELESS ISOLATION" ON MORE EXPENSIVE ROUTERS (continued)

- <Start of quote:>
  Some routers provide ‘Wireless isolation’ which is designed to block inter-device access on the same wireless network. In some cases this blocks access to wired devices and all other wireless devices,

ACTIVATE "WIRELESS ISOLATION" ON MORE EXPENSIVE ROUTERS (continued)

- in others access to wired devices is ALLOWED however access to other wireless devices is blocked. If you wish to utilise wireless isolation on a wireless network,

ACTIVATE "WIRELESS ISOLATION" ON MORE EXPENSIVE ROUTERS (continued)

- check the manufacture's manual and perform some tests to ensure you’re familiar with the implementation.
  <End of quote>

ACTIVATE "WIRELESS ISOLATION" ON MORE EXPENSIVE ROUTERS (continued)

- In other words, "wireless isolation" is useful as a way to isolate "Internet of Things" devices from other computers in some models of routers and worthless in other models of routers.