# Episode Book

EPISODE #5831

# Managed vs Layer 3: Two Switch Axes, One Empty Box

| | |
|---|---|
| PUBLISHED | 10 October 2026 at 10:28 UTC |
| DURATION | 23:17 |
| LISTEN | myweirdprompts.com/episode/managed-vs-layer3-switches/ |
| HOSTS | Corn, Herman, Hilbert |
| SCRIPT MODEL | deepseek-flash |
| VOICES | chatterbox-regular (chatterbox-local) |
| PIPELINE | V5.2 |
| SOURCES | 10 cited by the research (listed at the end) |
| BOOK GENERATED | 19 October 2026 at 17:40 UTC |

## SYNOPSIS

When you go shopping for a switch, the shelves hand you two vocabularies at once: managed versus unmanaged, and Layer 2 versus Layer 3. They sound related. They aren't. Managed describes whether you can configure the box; Layer 2 versus Layer 3 describes what the box is allowed to decide. Build the four-quadrant matrix and something surprising falls out — one of the four combinations is essentially a ghost. This episode walks the axes, populates all four boxes, explains why a Layer 3 unmanaged switch is close to self-contradictory, and then applies the whole framework to a real two-switch fiber link running across an apartment. Along the way: what the 802.1Q tag actually is, why MAC learning is the baseline rather than an upgrade, and why fiber doesn't promote your switch to anything.

# TRANSCRIPT



**Corn**

Daniel's got two switches at opposite ends of his apartment and a fiber line between them, and somehow that turned into a question about the entire OSI model.



**Herman**

Which is the correct amount of question, honestly.



**Corn**

It is. He upgraded to fiber and 2.5 gigabit, and now he's sitting on what he calls a rather illogical collection of daisy-chained switches. So he went shopping, and noticed the shelves are organized by two labels that don't obviously talk to each other. Managed versus unmanaged. Layer 2 versus Layer 3.



**Herman**

Everybody hits this. You go looking for a switch and you get handed two vocabularies at once.



**Corn**

Right. And he wants to know how those two classifications actually relate. Whether all four combinations are real and useful or whether some of them are nonsense, which one fits his two-switch fiber link, and why Layer 3 switches exist at all when we already have routers doing routing. He wants the concepts, not the product recommendations.



**Herman**

Good, because the matrix is where it gets fun. And one of those quadrants is basically empty.



**Corn**

The cleanest way to hold all of that at once is a four-quadrant matrix, so let's build it.



**Herman**

Start with the axes themselves, because the single most common mistake is treating managed and Layer 3 as the same thing. They are completely orthogonal. Managed versus unmanaged describes control. Does the box have a management interface, web, command line, a controller, that lets you configure it, monitor it, secure it.



**Corn**

And Layer 2 versus Layer 3 describes what the box is allowed to decide.



**Herman**

Exactly right. A Layer 2 switch forwards frames by MAC address inside one broadcast domain. A Layer 3 switch also routes packets by IP address between subnets. One is about whether you can talk to the device. The other is about what the device understands.



**Corn**

So managed does not mean Layer 3, and Layer 3 does not mean managed.



**Herman**

Neither direction. You can buy a managed Layer 2 switch and it's probably the most common switch in small business.



**Corn**

And the stacking principle that organizes the rest of this.



**Herman**

A Layer 3 switch is a Layer 2 switch that also routes. Nothing is taken away as you climb. Only added. And only paid for. That's the thing to hold onto. It isn't a ladder where each rung replaces the last one. It's a stack.



**Corn**

So let's populate the matrix. Four boxes. Layer 2 unmanaged, Layer 2 managed, Layer 3 unmanaged, Layer 3 managed. And one of them is going to turn out to be a ghost.



**Herman**

Let's start with the box everyone already owns. Layer 2 unmanaged. The dumb switch. No configuration, no management address, no logs, plug it in and it works.



**Corn**

And I want to defend the dumb switch here, because people talk about it like it's a toy.



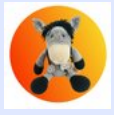
**Herman**

It isn't. It does the baseline job, and the baseline job is real. It learns MAC addresses and forwards frames out the correct port. That's the whole function of a switch. A hub used to shout every frame out every port. A switch builds a table, learns which MAC lives on which port, and sends traffic only where it needs to go.



**Corn**

And the point I keep wanting to make is that learning is the baseline, not the upgrade.



**Herman**

That's the line. The cheapest unmanaged switch you can buy does it. There's no tier of switch that doesn't do MAC learning, because MAC learning is what makes it a switch. It's like saying the cheap car still has wheels.



**Corn**

How long does it hold that table?



**Herman**

Default aging is three hundred seconds on Cisco gear. Entry goes stale, gets flushed, gets relearned next time traffic shows up. That's the standard behavior and it's fine.



**Corn**

So where does it fall apart?



**Herman**

VLANs. There are none. One flat broadcast domain, everything hears everything's broadcast traffic. No quality of service, so no priority for voice or video. No loop protection on most models, so if you accidentally cable a loop back into the same unmanaged switch you can melt the network. And no visibility at all.



**Corn**

Meaning when something breaks you find out by walking around unplugging things.



**Herman**

One at a time. It's a genuine diagnostic technique and I hate it. The correct home for an unmanaged switch is far-end fan-out in a single trusted location. The desk. The media wall. The workbench. Somewhere you need four more ports and you trust everything plugged into it. Modern ones are gigabit or 2.5 gigabit, so they aren't slow either.



**Corn**

Box one is real, it's everywhere, it's cheap. Box two. Layer 2 managed. This is the good stuff.



**Herman**

This is the tier most homes and small businesses land on and never leave. Everything unmanaged does, plus VLANs via 802.1Q tagging. Plus QoS. Per-port power over Ethernet control. Link aggregation. Spanning tree and storm control. SNMP, logs, port mirroring. Port security, 802.1X. And remote management, so you can sit at your desk and see what the switch thinks.



**Corn**

Give me the tag, because the tag is where VLANs stop being a word and become a thing.



**Herman**

Four bytes. The 802.1Q tag is four bytes inserted between the source MAC and the EtherType field. Which pushes the maximum frame size from fifteen eighteen to fifteen twenty-two bytes. That's it. That's the entire mechanism. Four bytes inside the frame that says which VLAN this belongs to.



**Corn**

And the VLAN ID lives in there.



**Herman**

Twelve bits. So zero to four thousand ninety-five theoretically, except zero and four thousand ninety-five are reserved, which leaves one to four thousand ninety-four usable. Four thousand and ninety-two VLANs, give or take, and I have never once seen a home network come close.



**Corn**

Now the crucial limitation of box two, and this is the sentence that unlocks the whole episode.



**Herman**

A Layer 2 managed switch can separate VLANs but it cannot connect them.



**Corn**

Say more, because people hear "managed" and assume it does everything.



**Herman**

It doesn't. The switch can put your cameras on VLAN twenty and your laptops on VLAN thirty and they will be perfectly isolated. But if a laptop needs to reach a camera, that traffic has to leave the switch, go up to a router, get routed, and come back down the same cable. The switch cannot do that step itself. It has no concept of IP. It doesn't know what a subnet is.



**Corn**

So VLANs are walls and the switch can build walls but not doors.



**Herman**

It can build walls. Doors are somebody else's job. And that's fine, that's most networks. This is where the vast majority of people should stop and buy nothing else.



**Corn**

Box three. Layer 3 unmanaged.



**Herman**

And here's where we find the ghost.



**Corn**

I want to be precise about this, because it's the most interesting thing in the matrix. Routing is inherently a configured act. You have to define subnets. You have to define switched virtual interfaces. Gateways. Routes. Somebody has to sit down and decide.



**Herman**

There's nothing automatic about it. A switch can learn a MAC address by watching traffic. It cannot learn your intent about which subnet should talk to which.



**Corn**

So a switch that routes but has no management interface is close to self-contradictory.



**Herman**

It's a device whose defining feature requires configuration, shipped with no way to configure it. That's not a product, that's a riddle.



**Corn**

And the market agrees with us. Search for an unmanaged Layer 3 switch and tell me what comes back.



**Herman**

Unmanaged Layer 2 devices on one side, managed Layer 3 devices on the other. Nothing in between. I could not find a standalone product that combines routing with zero management. It doesn't appear to exist as a category.



**Corn**

Which is a real finding and not a search failure.



**Herman**

I think it's structural. There's no version of this that makes sense to build.



**Corn**

Now the adjacent category that gets mistaken for it, because somebody's going to email about this.



**Herman**

Smart switches. Easy-smart. Web-managed. These sit between tiers. They've got a basic web page, VLAN tagging, simple priority settings. No command line. And no routing.



**Corn**

So they are managed-lite Layer 2.



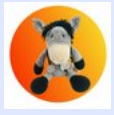
**Herman**

Managed-lite Layer 2. They are not unmanaged, and they do not route. If you've seen a cheap eight-port switch with a clunky web interface and VLAN checkboxes, that's what you're holding. It's a perfectly good box. It's just not the ghost.



**Corn**

Box four. Layer 3 managed.



**Herman**

Everything Layer 2 managed does, plus hardware IP routing between VLANs via switched virtual interfaces and routed ports. Static routing, and often dynamic routing, OSPF or BGP. DHCP relay. Access control lists.



**Corn**

And the routing happens where?



**Herman**

In the ASICs and the TCAM. At wire speed. Not on a general-purpose CPU grinding through a routing table in software.



**Corn**

So the L2 managed switch builds walls but can't build doors. The L3 managed switch builds the doors too, and builds them at line rate.



**Herman**

And I want to frame Layer 3 properly, because it gets sold as an upgrade. It isn't. It's a traffic answer, not a status symbol. It earns its place when a lot of traffic crosses between VLANs inside the building. If almost nothing crosses, you've bought a router you didn't need and a configuration surface you now have to maintain.



**Corn**

And there's a price signal for all of this. Same shelf, same port count, wildly different prices.



**Herman**

Ten times is the spread you can see. An eight-port L2 smart-managed PoE+ switch at a hundred and forty-nine dollars, the FS S2805S, and then an industrial L3 managed eight-port at a thousand and forty-nine. Same shelf, same rough port count, seven times the money.



**Corn**

Which buys you routing, and hardening, and industrial temperature ratings, but the routing is the part we care about.



**Herman**

Three of those four quadrants are real, shipping product categories. The fourth is a category error. And the emptiness is itself the finding.



**Corn**

So three quadrants are real products and one is a category error. Now let's put that matrix to work on Daniel's actual apartment.



**Herman**

Two switches, opposite ends of an apartment, joined by an SFP+ fiber link. Single flat network. No routing required.



**Corn**

Because it's one subnet. Everything can talk to everything, and nothing needs to be decided.



**Herman**

Nothing needs to be decided. Which means box one, Layer 2 unmanaged, is entirely sufficient if everything on that network is equally trusted. You want ports at both ends. You have ports at both ends. Done.



**Corn**

And if Daniel wants to separate things?



**Herman**

Then it's Layer 2 managed. VLANs for the IoT devices, the cameras, the guests, the work laptop. Link aggregation if he wants two links between the switches instead of one. Remote visibility, so he can see port counters without walking to the far end.



**Corn**

And it only becomes Layer 3 managed if he introduces multiple VLANs and a lot of traffic crossing between them inside the apartment.



**Herman**

Concrete case. An NVR on the camera VLAN, a NAS on the storage VLAN, and the NVR is pulling camera streams across that boundary all day. That's a lot of east-west traffic. That's the case where routing internally saves you a trip up to the router and back.



**Corn**

And the thing I want to nail down here, because it comes up every time somebody mentions fiber.



**Herman**

Go ahead.



**Corn**

The fiber link is just a physical medium.



**Herman**

It is. SFP+ carries the same Ethernet frames. Copper carries them too. The transceiver changes the physics of the signal, not the logic of the network. A Layer 2 switch with a fiber port is still a Layer 2 switch. Fiber does not promote anything. It's a longer cable that doesn't pick up noise.



**Corn**

People see the SFP+ and assume they've crossed into enterprise territory.



**Herman**

Fiber is just the cabling decision. What you plug it into is still the layer decision. They're independent, same as managed and Layer 3 are independent. The whole episode is about two axes not being one axis.



**Corn**

Now the daisy-chain caveat, because this speaks directly to Daniel's pile.



**Herman**

This is the one that actually bites him. An unmanaged switch must sit at the edge of one VLAN.



**Corn**

Never in the middle of a path carrying tagged traffic for several VLANs.



**Herman**

Never in the middle. And here's why it's nasty. Some unmanaged switches pass tagged frames through intact. Some strip the tag. Some do something stranger. And none of them report which one they're doing. There's no log, no counter, no notification. The switch is silent about it.



**Corn**

So you have a managed switch at one end, a managed switch at the other, VLANs configured correctly on both, and a dumb switch in the middle quietly eating tags.



**Herman**

And the result is faults that work on one floor and fail on another. The camera on VLAN twenty reaches the NVR when it's plugged into the near switch and doesn't when it's plugged into the far one, because that path crosses the dumb switch and the tags didn't survive the trip.



**Corn**

And that is exactly the kind of intermittent problem that makes people replace hardware at random.



**Herman**

They swap the managed switch because it's the expensive one and it must be the problem. It isn't. The fifty-dollar box in the middle with no logs is the problem, and it has no way of telling you so.



**Corn**

Which is worth saying plainly to Daniel. The pile, if there are VLANs anywhere in it, may not be a performance problem. It may be a correctness problem.



**Herman**

Right. And the diagnostic move is to find every unmanaged switch on the path between two points that are supposed to talk and pull it out of the middle.



**Corn**

So to Daniel's apartment specifically, the answer is box one or box two, and probably box two if he's got cameras and guests on the same wire.



**Herman**

And he almost certainly doesn't need box four. Very few apartments generate the kind of east-west inter-VLAN traffic an L3 switch is built for.



**Corn**

Which brings the router question, and I want the real answer here, not the marketing one. Why do Layer 3 switches exist when routers already route?



**Herman**

History is the honest answer. Inter-VLAN traffic used to go host to switch to router to switch to host. Everybody calls it router-on-a-stick, because the router is hanging off one link, and every packet crossing between VLANs has to go up that stick and come back down.



**Corn**

One physical link carrying all the inter-VLAN traffic in the building.



**Herman**

One link, and a general-purpose CPU forwarding in software. So you had a bottleneck and a ceiling at the same time. An L3 switch routes internally. Host to switch, routed inside the switch, to host. One fewer hop, no trunk bottleneck, and the routing is happening in hardware.



**Corn**

The L3 switch exists because the router-on-a-stick topology didn't scale.



**Herman**

That's why the category was invented. Take the routing function and put it where the traffic already is.



**Corn**

Now the part where the distinction gets blurry.



**Herman**

The classic framing is routers route in software, switches route in hardware. That's increasingly legacy. Modern enterprise routers, the Cisco ASR line, the Juniper MX line, they use ASICs too. Hardware forwarding isn't a switch thing anymore. It's a both thing.



**Corn**

If that line is gone, what actually separates them?



**Herman**

What remains true is where each is optimized. L3 switches are built for high-port-density inter-VLAN routing. Forty-eight ports, a bunch of VLANs, lots of traffic crossing between them, all inside one building. Routers are built for WAN connectivity, NAT, VPN termination, complex policy routing, and protocol support that switches don't have.



**Corn**

There's a media difference that doesn't get mentioned enough.



**Herman**

There is. Most switches support one physical network type. Ethernet. That's the whole menu. A router may support different kinds of physical networks on different ports. A serial link here, a fiber uplink there, an Ethernet handoff to the carrier. That flexibility is part of what you're paying for.



**Corn**

Wikipedia's framing on this is useful. Because many Layer 3 switches offer the same functionality as conventional routers, they can be cheaper, lower-latency replacements in some networks.



**Herman**

Cheaper and lower latency, in some networks. The qualifier is doing real work there. In a building where everything is Ethernet and traffic is mostly east-west, an L3 switch replaces a router and does it better. Point it at a carrier handoff with a bunch of policy you need to enforce and it's the wrong tool.



**Corn**

Now the firewall trap, because this is the second-order consequence I most want on the record.



**Herman**

Once the switch routes between VLANs locally, that traffic no longer passes the firewall.



**Corn**

It just doesn't go there anymore.



**Herman**

It doesn't go there anymore. That's the entire trick. You configured the switch, the routing works, everything is faster, and quietly every inter-VLAN rule you had on the firewall is now being bypassed by design. The traffic isn't being blocked. It isn't being inspected. It simply isn't in the firewall's path.



**Corn**

The rule is still sitting in the firewall, looking like it's protecting something.



**Herman**

It's protecting nothing, because nothing reaches it. Any policy you relied on there has to be rebuilt as ACLs on the switch. That's the single most common Layer 3 mistake. People enable routing, feel the speed, and never think about where the packets stopped going.



**Corn**

To say the obvious thing directly. Replacing a firewall with a Layer 3 switch is a security downgrade, not a consolidation.



**Herman**

It is not a consolidation. A switch with ACLs is not a firewall. It doesn't do stateful inspection, it doesn't do application awareness, it doesn't do the things you bought a firewall to do. You've moved the routing and dropped the policy.



**Corn**

There's a second consequence too, the hardware one.



**Herman**

TCAM. The routing table lives in ternary content-addressable memory, and TCAM lookups are O of one. Constant time regardless of route count. That's why L3 switching is fast. It doesn't matter whether there are ten routes or ten thousand, the lookup takes the same time.



**Corn**

Until it doesn't.



**Herman**

Until the TCAM overflows. And when it overflows, the switch falls back to software forwarding via the CPU. Performance drops off a cliff. Not a slope. A cliff. Hardware routing is fast right up until the moment it isn't, and then it's dramatically slower than the thing it replaced.



**Corn**

Which is a failure mode you find by accident.



**Herman**

Which is a breaking point you find by adding routes. There's no warning. You cross the line and the network gets worse.



**Hilbert**

The facility had eleven of them. Eleven switches, and the network dropped every Tuesday.



**Corn**

The facility.



**Hilbert**

Locked room, no computers, one switch. It had a routing table. It had no management interface. Most honest piece of equipment I ever owned. It never pretended to be configurable.



**Herman**

How did you configure the routes on a switch with no interface?



**Hilbert**

You didn't. One port. I plugged it into itself. Only way to keep it from routing.



**Corn**

You plugged the switch into itself.



**Hilbert**

Ran a cable from port one to port one. It would sit there, tables full, routing to itself, perfectly content. I checked the lights every month. Herman, the frames don't drop on the far side, they drop on the near side. That's your problem with Daniel's pile, and it was mine.



**Herman**

That would have been the useful thing to know three minutes ago.



**Hilbert**

I still have the key. Never told anyone where the room is. Anyway, your levels are drifting, cut that cough in the second segment.



**Corn**

What does the switch in Daniel's apartment actually need to be, given that the fault is probably at the near end?



**Herman**

Given that the fault is probably at the near end, it needs to be a managed Layer 2 switch, and he needs to be able to see what the near end thinks. Which is the whole case for the tier. Not speed, visibility.



**Corn**

Let's pull back to the matrix one last time.



**Herman**

Three quadrants real, one empty, and the empty one is empty for a reason that generalizes. Routing is an intention, and intentions have to be expressed somewhere. Any box that routes has to have a surface for you to express them.



**Corn**

Which raises the question of whether the smart tier eventually eats that space. Managed-lite Layer 2 keeps getting more capable as the silicon gets cheaper. Does it eventually grow routing and swallow the concept?



**Herman**

Or whether routing will always require a management surface of some kind, which would mean the ghost stays a ghost forever. I don't know. I lean toward the ghost staying, because routing without configuration isn't routing.



**Corn**

In the home, the point at which an L3 switch starts to make sense keeps moving closer to the living room. Every year there are more VLANs. IoT, cameras, guests, work devices. And the firewall trap moves with it.



**Herman**

It moves with it. More VLANs, more routing, more traffic that quietly stops passing your firewall on the way.



**Corn**

The cutting-room floor. One thing from the reading that didn't fit. The cheap web-managed switches that people mistake for the ghost.



**Herman**

They're managed-lite Layer 2. Web page, VLAN tagging, simple priority, no command line, no routing. Every time somebody says they found an unmanaged Layer 3 switch, they're holding one of these. It's a good box. It just isn't a ghost.



**Corn**

The difference between these boxes is not speed. It's how much the box is allowed to think.



**Herman**

A box with no way to tell it what to think can't route. That's the whole quadrant.



**Corn**

Thanks to Hilbert Flumingtop, our producer, who has been at the desk this whole time, quietly holding a key.



**Herman**

If this was your kind of episode, go back for episode two forty-six, Fiber vs. Copper; episode forty-one fifty-nine, Managed vs Unmanaged Switches; and episode thirty-five, The Privacy Gap. This has been My Weird Prompts.



**Corn**

If you've got a prompt of your own, send it to us on Telegram at t dot me slash MWP listener bot.



**Herman**

We'll be back soon.

# SOURCES

What the research for this episode read before the script was written. Primary sources first.

1. **QuickSurfNetwork**
   Unmanaged vs L2 vs L3 Switches, Plain English Guide (undated)
   https://quicksurfnetwork.com/unmanaged-vs-l2-vs-l3-switches/

2. **blog.gtfo.dev**
   Layer 2 vs. Layer 3 Switches: SVIs, TCAM, and VLAN Routing, published Apr 8, 2026
   https://blog.gtfo.dev/blog/layer-2-vs-layer-3-switches/

3. **NetworkAcademy.IO**
   Routers and L3 Switches (CCNA)
   https://www.networkacademy.io/ccna/network-fundamentals/routers-layer3-switches

4. **Wikipedia**
   Multilayer switch (Layer 3 switching)
   https://en.wikipedia.org/wiki/Layer_3_switching

5. **FS.com**
   Layer 2 Switches vs Layer 3 Switches: Which One Fits Your Network?
   https://www.fs.com/blog/layer-2-switches-vs-layer-3-switches-which-one-fits-your-network-13397.html

6. **Planet Technology USA**
   IGS-6325-8T8S4X Industrial L3 Managed Switch product page ($1,049.69)
   https://planetechusa.com/product/igs-6325-8t8s4x-industrial-l3-8-port-10-100-1000t-8-port-100-1000x-sfp-4-port-10g-sfp-managed-ethernet-switch/

7. **Planet Technology USA**
   IGS-6325-20T4C4X Industrial L3 Managed Switch product page ($1,289.20)
   https://planetechusa.com/product/igs-6325-20t4c4x-industrial-l3-20-port-10-100-1000t-4-port-gigabit-tp-sfp-4-port-10g-sfp-managed-ethernet-switch/

8. **Benchu Group**
   8-Port 10G Unmanaged PoE++ Switch, June 29, 2026 (example of unmanaged L2, no routing)
   https://www.benchu-group.com/8-port-10g-unmanaged-poe-switch

9. **Tom's Hardware Forum**
   Can an unmanaged switch route different IPs (unmanaged = L2, no IP awareness)
   https://forums.tomshardware.com/threads/can-a-unmanaged-switch-route-different-ips.2513249/

10. **Grandstream**
    Layer 3 Network Switches (GWN7810/7820 series)
    https://www.grandstream.com/products/networking-solutions/layer-3-network-switches