

The Fortinet logo, featuring the word "FORTINET" in a bold, black, sans-serif font. The letter "O" is stylized with a red square containing a white grid pattern.

FORTINET

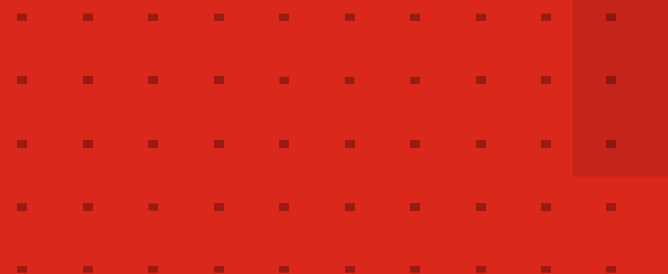
The text "XPERTS26 FortiSwitch" in a bold, black, sans-serif font. The background features a large, faint, light gray grid pattern with some cells containing red and gray geometric shapes, including squares and semi-circles.

XPERTS26 FortiSwitch



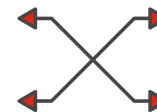
FortiSwitch

Secure Simplified Scalable Ethernet



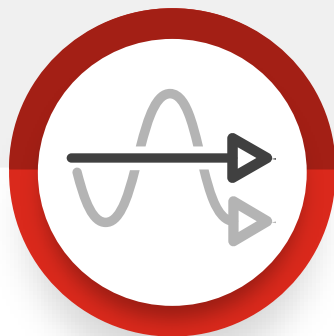
FortiSwitch Secure Ethernet Switching

A secure approach to Ethernet



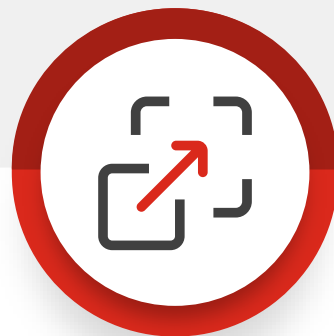
Secure

NGFW security
visibility and
control to Ethernet
networking



Simple

Zero touch
deployment
Easy to manage
whether integrated
or standalone



Scalable

Deployments from
the smallest branch
to largest campus



Secure LAN Use Cases

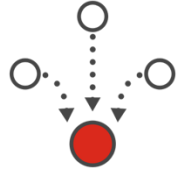
Solutions across deployment types

Campus



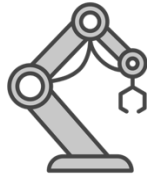
Security, visibility, and control at scale for large deployments.

SD-Branch



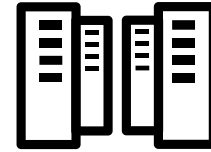
Reduce Complexity, Standardize Security Through convergence of wireless, switching, 5G gateway and SD-WAN

OT



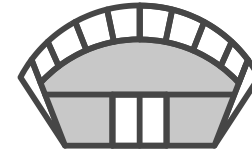
Provides visibility and protection, enhanced efficiency and improved safety to OT networks

Data Center



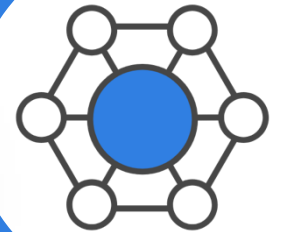
Provide the performance and security necessary for today's and tomorrow's datacenter

HD Wireless



Provide Reliable High Performance Wireless for large public venues

Micro Branch



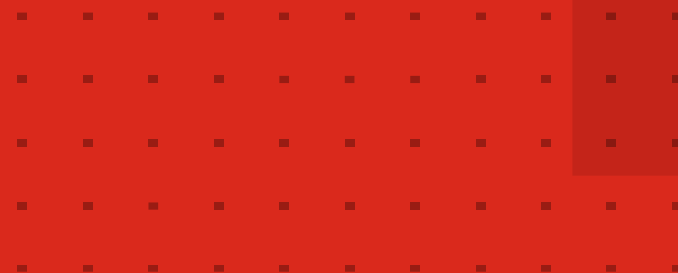
Simplify network and security via integration. Get unified policies, high performance, and central management





FortiSwitch

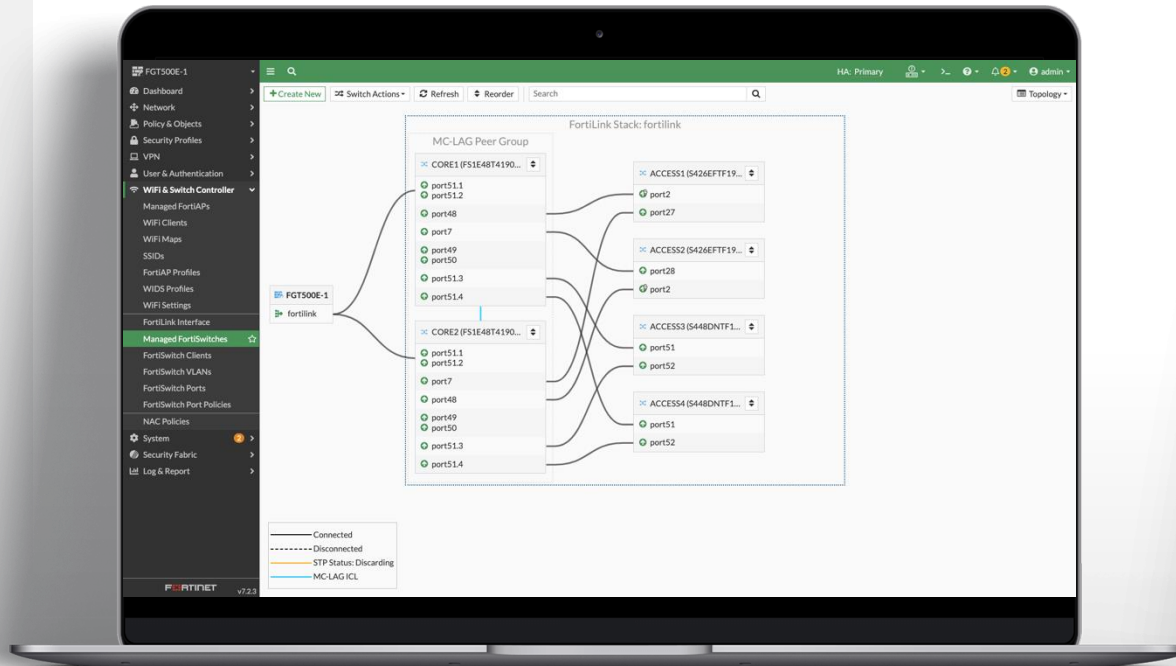
Deployment and Management



FortiSwitch Deployment Options

FortiLink

FortiGate Managed. Security Fabric Enabled.
Most common deployment model



Stand Alone

Industry Standard Deployment Model
Common in non-FortiGate environments



Fortinet Secure LAN Management Options



FortiGate

Manage FortiSwitch & FortiAP in the FortiGate UI



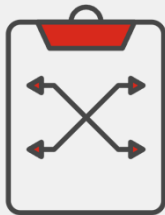
FortiManager

Single point of management for the Security Fabric



FortiEdge Cloud

Cloud management for standalone (Non FortiGate managed) FortiSwitch and FortiAP



FortiSwitch Manager

On premise management of standalone FortiSwitch



FortiLink Plane Architecture

Control Plane



FortiGate as Switch and wireless
Controller



FortiLink

Management Plane



FortiGate Managing FortiLink
Fabrics

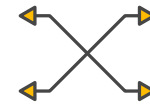


FortiEdge Cloud



FortiManager and
FortiAnalyzer

Data Plane



FortiSwitch



FortiAP



FortiExtender

Fabric Integrations



AI for Networking (AIOPS)



FortiMonitor



FortiNAC

FortiLink Plane Architecture

Control Plane

Who controls the fabric

- FortiGate discovers and authorizes FortiSwitch
- FortiLink control communication and topology view
- VLAN / interface orchestration from the controller
- Policy enforcement anchored at FortiGate

Management Plane

Who operates it

- FortiManager templates and configuration lifecycle
- Firmware, backup, revision control, and change process
- FortiAnalyzer logs, reports, and operational visibility
- FortiEdge Cloud option where cloud-managed LAN is used

Data Plane

Where traffic flows

- Endpoint traffic forwarding through FortiSwitch ports
- VLANs, trunks, LACP, STP, and MC-LAG operations
- FortiAP and FortiExtender access traffic
- Inter-VLAN / north-south traffic inspected by FortiGate

Fabric Integrations

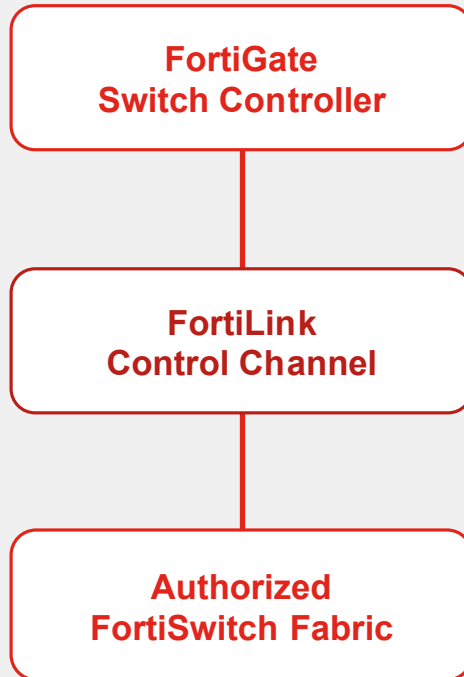
Who enriches security

- FortiNAC: identity, profiling, posture, dynamic VLAN
- FortiAnalyzer: logging, analytics, and reports
- AIOps / FortiMonitor: health and anomaly detection
- APIs and telemetry for automation and visibility

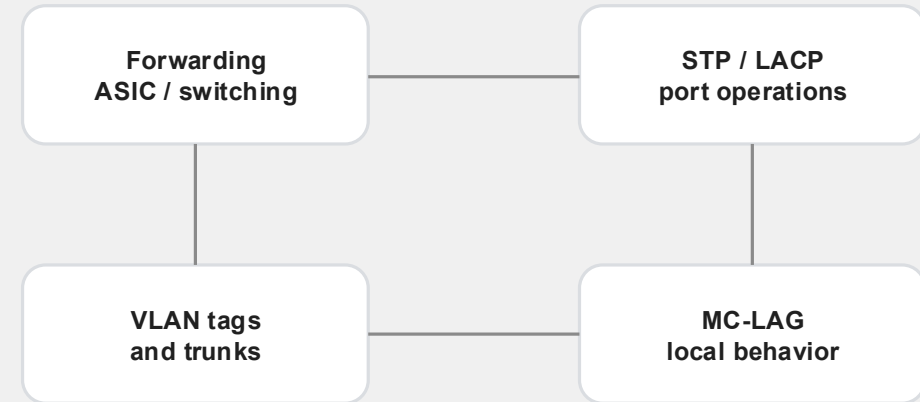


Control Plane: Orchestration, Authorization, and Policy Anchor

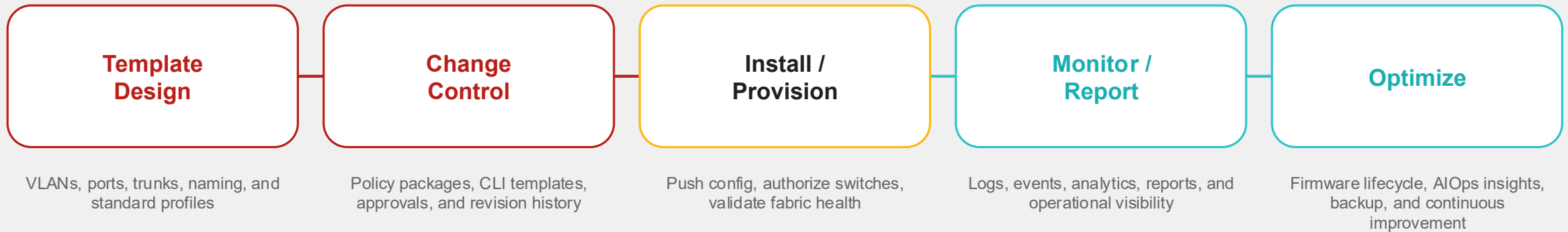
Centralized by FortiGate / FortiLink



Still local on FortiSwitch



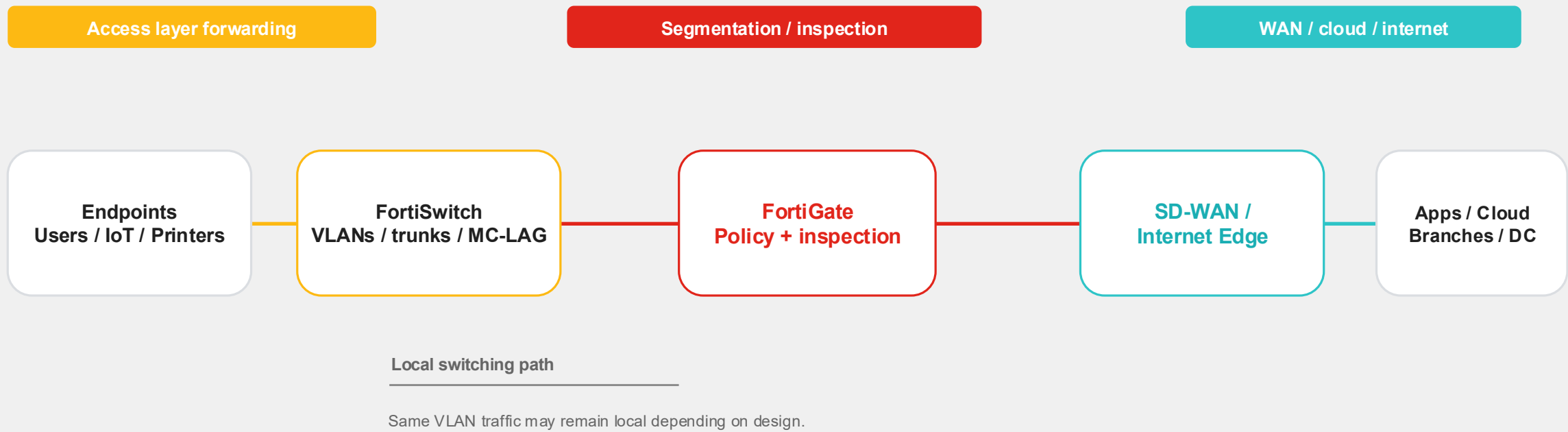
Management Plane: Lifecycle, Visibility, and Change Control



Core management tools



Data Plane: Traffic Paths and Enforcement Points



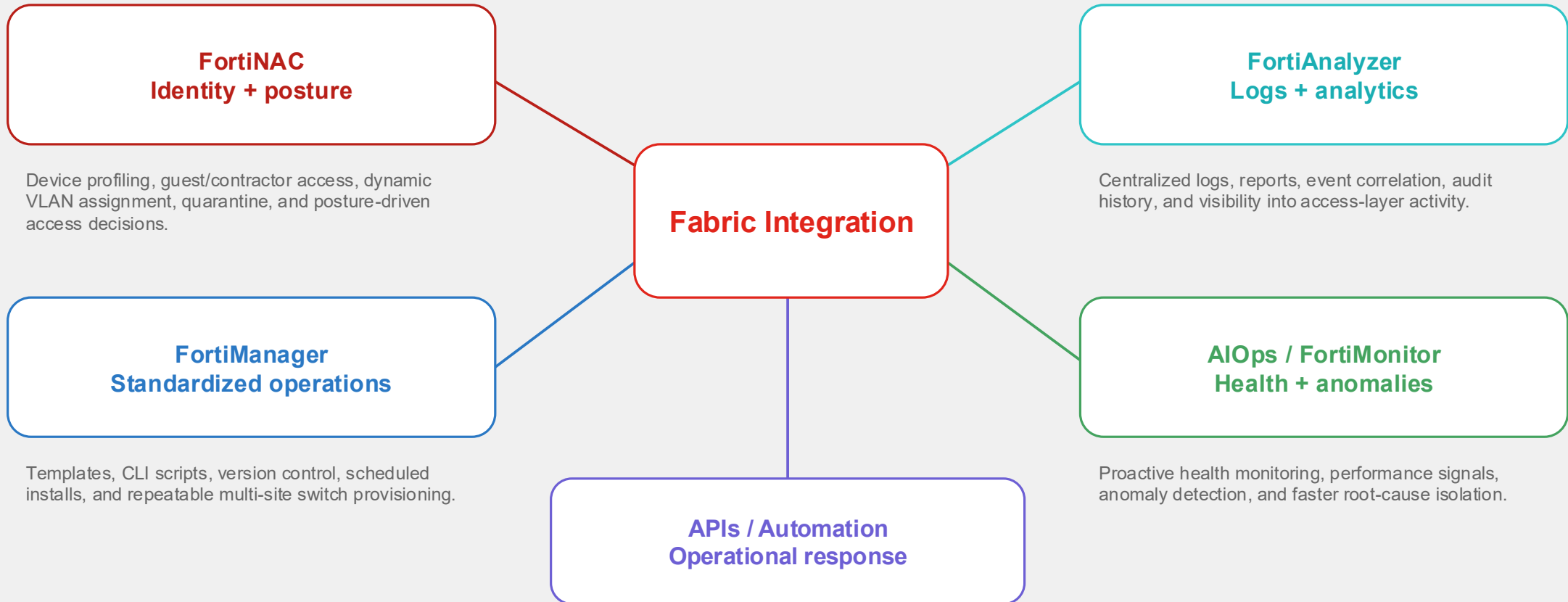
Traffic path matrix

Traffic type	Primary data path	Architectural point
Same VLAN endpoint traffic	FortiSwitch	Local forwarding where allowed by design
Inter-VLAN / east-west traffic	FortiGate	Security policy, segmentation, inspection
North-south traffic	FortiGate / SD-WAN edge	Firewall, IPS, app control, web filtering, routing
Wireless / LTE traffic	FortiAP / FortiExtender	Access traffic enters the same policy model



Fabric Integrations: Security Fabric Outcomes

The value is not only centralized switch management; it is context, control, visibility, and response.



Outcome: the access fabric becomes measurable, enforceable, and automatable.





FortiLink Deep Dive

Deployment and Management

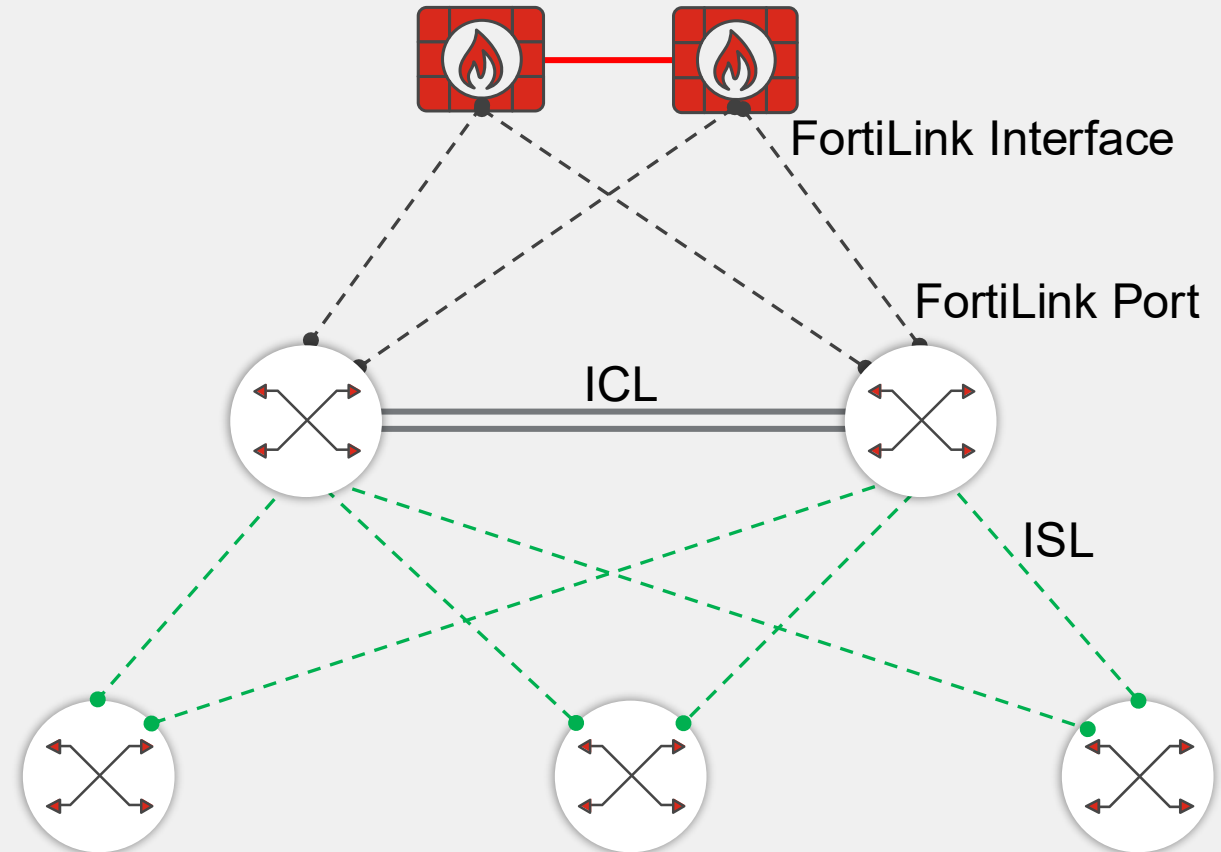


FortiLink Concepts

- Terminology

- **FortiLink Interface**. The interface in FGT dedicated to manage switches.
 - There can be more than one Fortilink interface in a FGT since version 6.4.
- **Fortilink Port**: The port on the switch that connects directly to FGT
- **ISL**: Inter Switch Link. Direct connection between two switches in FGT managed mode. Could be single or LACP
- **ICL or MCLAG-ICL**: The inter switch link between two switches in the same MCLAG Tier (Intern Chassis Link)

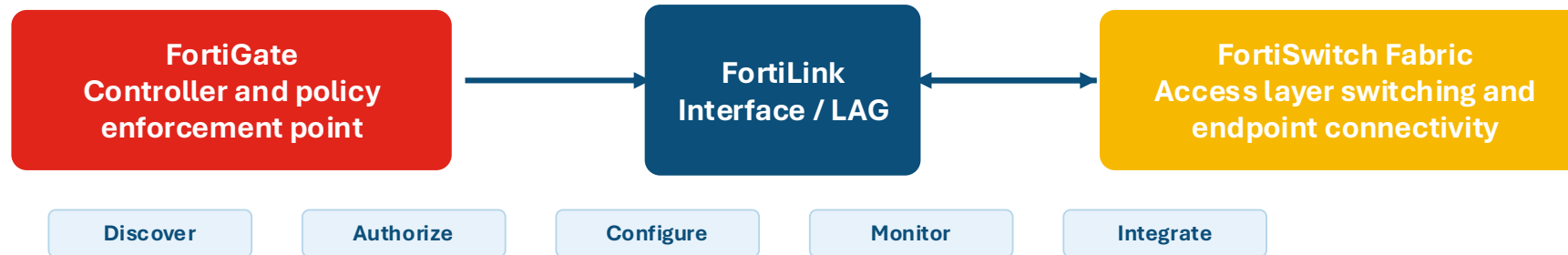
Physical Interface
802.3ad Aggregate
EMAC VLAN
FortiExtender WAN Extension
Hardware Switch
Loopback Interface
PPPoE Interface
Redundant Interface
Software Switch
SSL-VPN Tunnel
VLAN
WiFi SSID



What Is FortiLink?

Dedicated control and management channel between FortiGate and FortiSwitch

Architecture view



What FortiLink enables

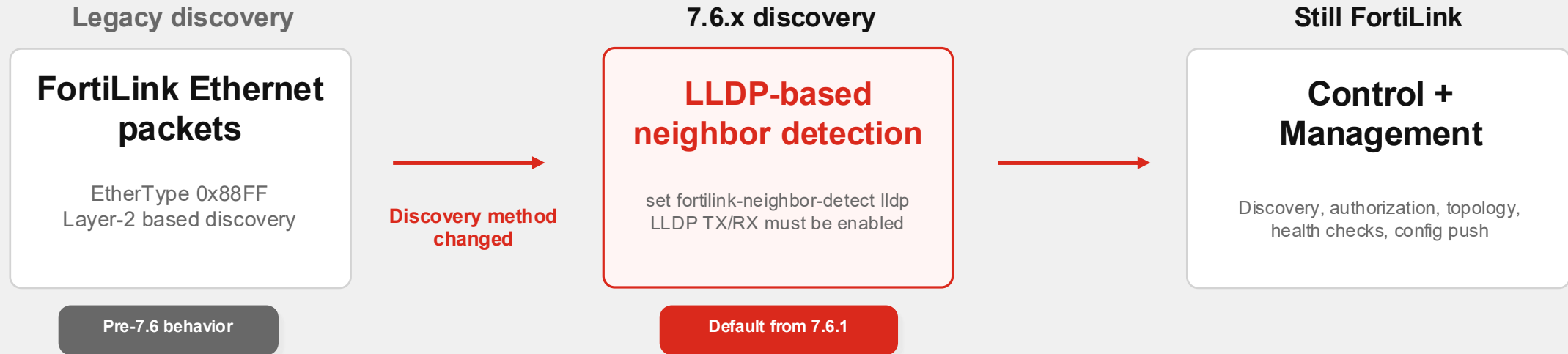
- Discover and authorize FortiSwitches from FortiGate
- Build and display the switch topology
- Push VLANs, port profiles, trunks, and switch configuration
- Monitor switch health, ports, and connected devices
- Extend access-layer visibility into the Security Fabric

Protocols and services behind FortiLink

FLP	Device discovery and capability detection
LLDP	Neighbor and topology visibility
CAPWAP	Control communication with managed Fortinet devices
REST / API	Configuration, monitoring, and operations
STP	Loop prevention and Layer 2 protection
LACP / 802.3ad	Redundant FortiLink uplinks

**Exact behavior can vary by FortiOS / FortiSwitchOS version and supported model.*

FortiLink Discovery packets



Legacy vs. LLDP-Based FortiLink Discovery

Legacy FortiLink discovery

FortiGate and FortiSwitch discovery relied on FortiLink Ethernet packets over the local Layer-2 segment.

```
diagnose sniffer packet fortilink "ether proto 0x88ff" 6
```

Legacy / older design view

LLDP-based neighbor detection

```
config system interface
edit "fortilink"
set lldp-reception enable
set lldp-transmission enable
set fortilink-neighbor-detect lldp
next
end
```

Fortilink – STP

- There is NO STP between FGT and FSW ** (Exceptions in FSW 100 series when needed)
- STP is between switches to prevent loops and provide link redundancy

- `# diagnose switch-controller get-conn-status fsw_serial`

FGT-101F-JV # execute switch-controller get-conn-status S424DF3X16000028

Get managed-switch S424DF3X16000028 connection status:

Admin Status: Authorized

Connection: Connected

Image Version: S424DF-v6.4.2-build425,200629 (GA)

Remote Address: 172.16.1.2

Join Time: Mon Feb 28 20:33:51 2022

interface	status	duplex	speed	fortilink	stacking	poe	status
port1	up	full	1000Mbps	no	no		Searching
port2	down	N/A	0	no	no		Searching

...

Aggregate Interfaces:

Interface	Status	Duplex	Speed	Type
4EPTF19004524-0(*)	up	full	1000Mbps	ISL
G101FTK20000639(*)	up	full	10000Mbps	FL

ISL: Inter-Switch-Link trunk.

FL: Fortilink Trunk connected to FGT.

(*): System auto generated trunk

← To next switch – **ISL – Inter Switch Link** (Serial of next switch)

← To FGT – Fortilink FL (Serial of FGT)

- You can get STP information on each switch from FGT
 - `# diagnose switch-controller switch-info stp fsw_serial` (this command was called before `diag switch-controller dump stp`)



Fortilink – STP

```
FGT-101F-JV # diagnose switch-controller switch-info stp S424DF3X16000028
Vdom: root

S424DF3X16000028:
MST Instance Information, primary-Channel:
Instance ID 0 (CST)
  Config      Priority 24576
                Bridge MAC 906cac6b39fc, MD5 Digest 9999b43d77cc58bba8854f9991c4a487
  Root      MAC 906cac6b39fc, Priority 24576, Path Cost 0, Remaining Hops 20
                (This bridge is the root)
  Regional Root  MAC 906cac6b39fc, Priority 24576, Path Cost 0
                (This bridge is the regional root)
  Active Times  Forward Time 15, Max Age 20, Remaining Hops 20
  TCN Events   Triggered 13 (0d 16h 32m 3s ago), Received 24 (0d 16h 31m 59s ago)
  Port      Speed  Cost  Priority Role    State    HelloTime  Flags
-----
port1      1G    20000  128    DESIGNATED FORWARDING 2    EN
port23     1G    20000  128    DESIGNATED FORWARDING 2    EN ED
port26     -    200000000  128    DISABLED  DISCARDING 2    ED
internal   1G    20000  128    DESIGNATED FORWARDING 2    ED
G101FTK20000639 10G  2000  128    DESIGNATED FORWARDING 2    ED
4EPTF19004524-0 1G    1    128    DESIGNATED FORWARDING 2    EN
Flags: EN(STP enable), ED(Edge), LP(Loop Protection Triggered)
RG(Root Guard Triggered), BG(BPDU Guard Triggered), IC(PVST Port Inconsistent)
MV(PVST Port Vlan Mismatch)

Instance ID 15
  Config      Priority 24576, VLANs 4094
                Bridge MAC 906cac6b39fc
  Regional Root  MAC 906cac6b39fc, Priority 24576, Path Cost 0
                (This bridge is the regional root)

  TCN Events   Triggered 5 (0d 16h 33m 40s ago), Received 3 (24d 8h 56m 49s ago)
  Port      Speed  Cost  Priority Role    State    Flags
-----
internal   1G    20000  128    DESIGNATED FORWARDING ED
G101FTK20000639 10G  2000  128    DESIGNATED FORWARDING ED
4EPTF19004524-0 1G    1    128    DESIGNATED FORWARDING EN
```

Main STP instance

No STP enabled to
FGT and is Edge



FortiLink - STP in a FortiSwitch Tier 1 MCLAG ICL Peer Group

- **Example of a typical customer network**
- **Focus on Tier 1 Peer Group**
- **FortiLink automatically configures MSTP Priority for Tier 1 to be MSTP Root**
- **Both MCLAG Peer switches share same MAC**

```
fortigate2 # diag
Vdom: root

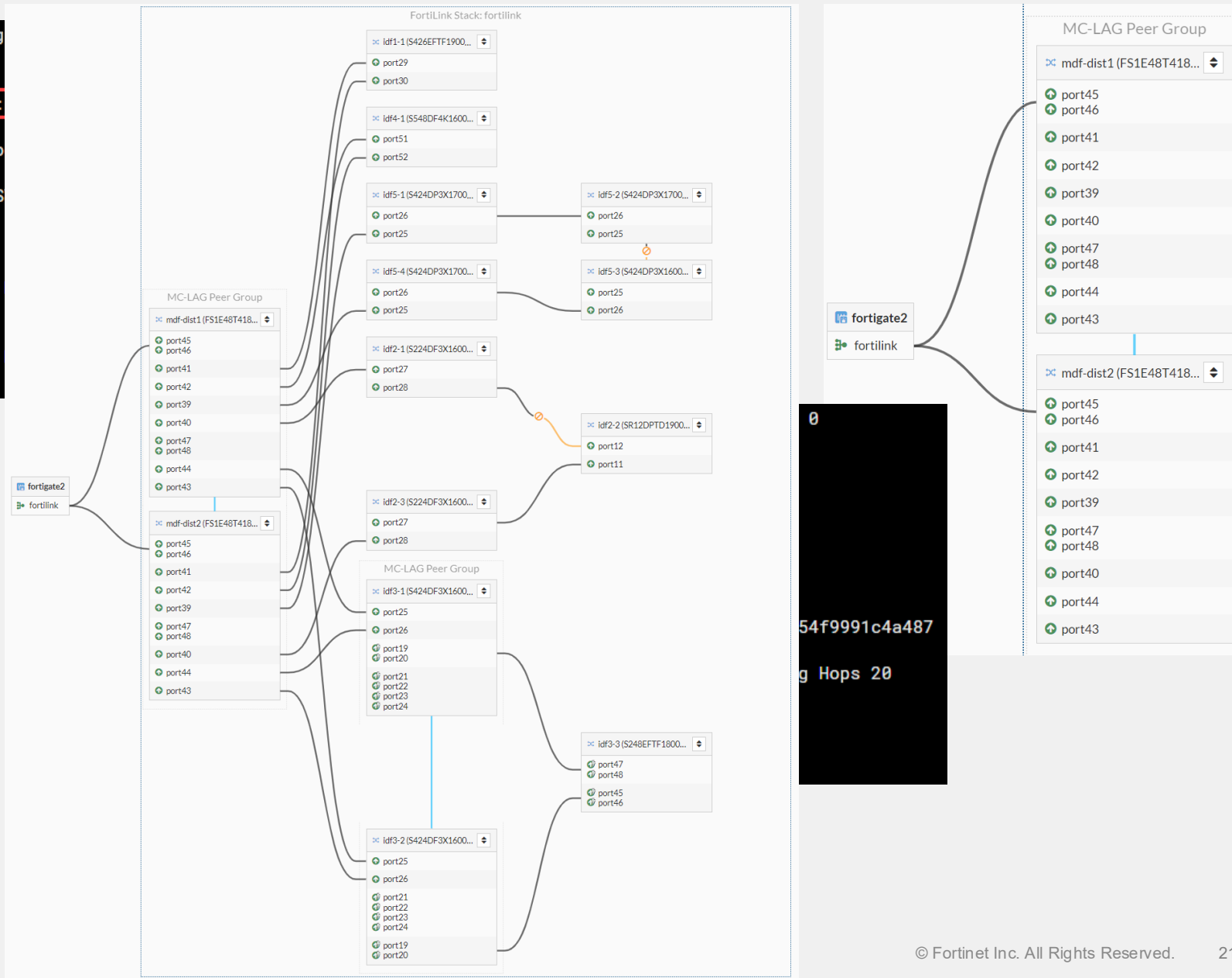
FS1E48T418000172:

MST Instance Info

Instance ID 0 (CS
  Config

  Root

  Regional Root
```



Other FortiLink Modes



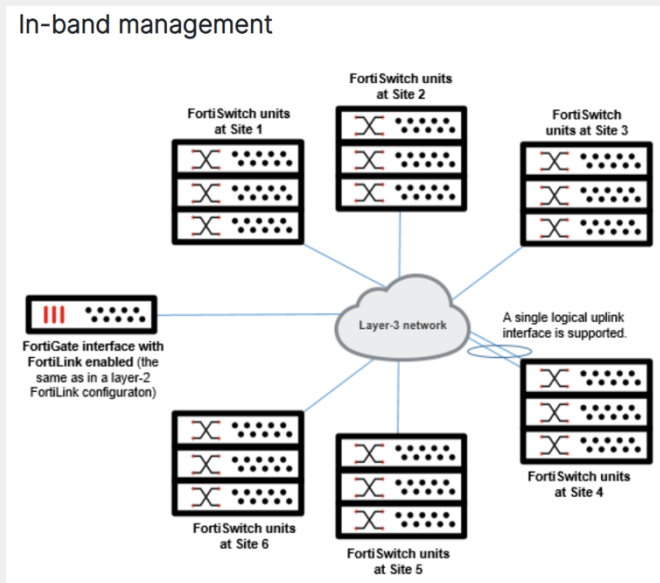
FortiLink Modes

FortiLink Over L3

This feature allows FortiSwitch islands to operate in FortiLink mode over a layer-3 network, even though they are not directly connected to the switch-controller FortiGate unit. FortiSwitch islands contain one or more FortiSwitch units.

There are two main deployment scenarios:

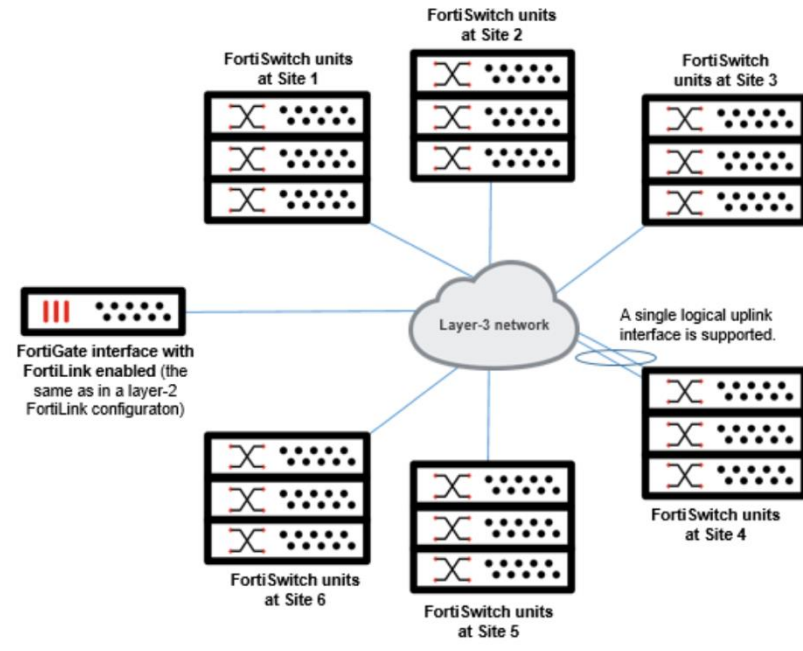
- In-band management, which uses the FortiSwitch unit's internal interface to connect to the layer-3 network
- Out-of-band management, which uses the FortiSwitch unit's mgmt interface to connect to the layer-3 network



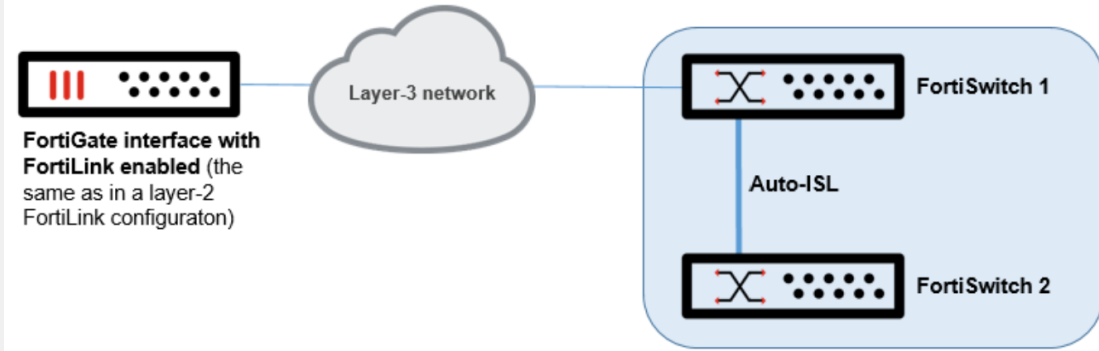
FortiLink Modes

FortiLink Over L3

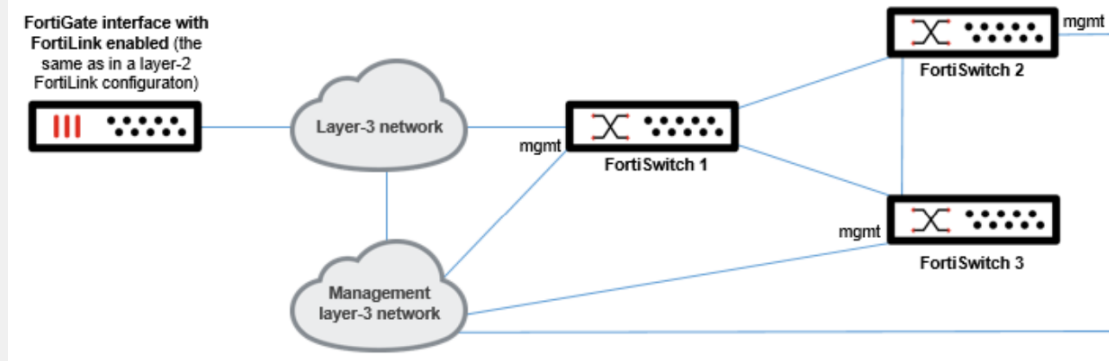
In-band management



Connecting additional FortiSwitch units to the first FortiSwitch unit



Out-of-band management



FortiLink Modes

FortiLink Over L3 Limitations

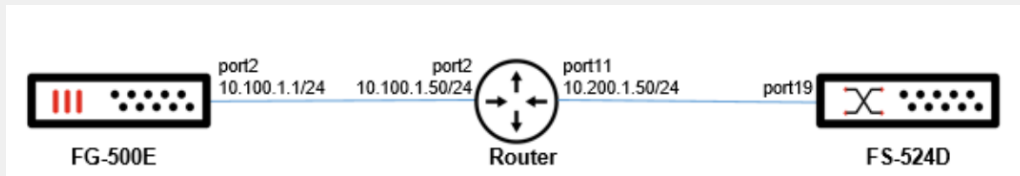
- FortiSwitch NAC is not supported.
- No layer-2 data path component, such as VLANs, can span across layer 3 between the FortiGate unit and the FortiSwitch unit.
- All FortiSwitch units within an FortiSwitch island must be connected to the same FortiGate unit.
- The FortiSwitch unit needs a functioning layer-3 routing configuration to reach the FortiGate unit or any feature-configured destination, such as syslog or 802.1x.
- Do not connect a layer-2 FortiGate unit and a layer-3 FortiGate unit to the same FortiSwitch unit.
- If the FortiSwitch management port is used for a layer-3 connection to the FortiGate unit, the FortiSwitch island can contain only one FortiSwitch unit. All switch ports must remain in standalone mode. If you need more than one physical link, you can group the links as a link aggregation group (LAG).
- Do not connect a FortiSwitch unit to a layer-3 network and a layer-2 network on the same segment.
- If the network has a wide geographic distribution, some features, such as software downloads, might operate slowly.
- After a topology change, make certain that every FortiSwitch unit can reach the FortiGate unit.
- NAT is not supported between the FortiSwitch unit and FortiGate unit.



FortiLink Modes

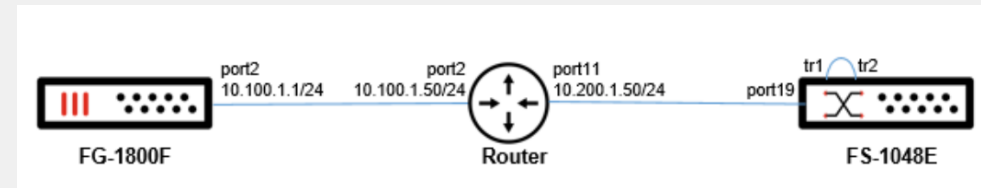
Managing FortiSwitch units on VXLAN interfaces

VXLAN for Management Traffic

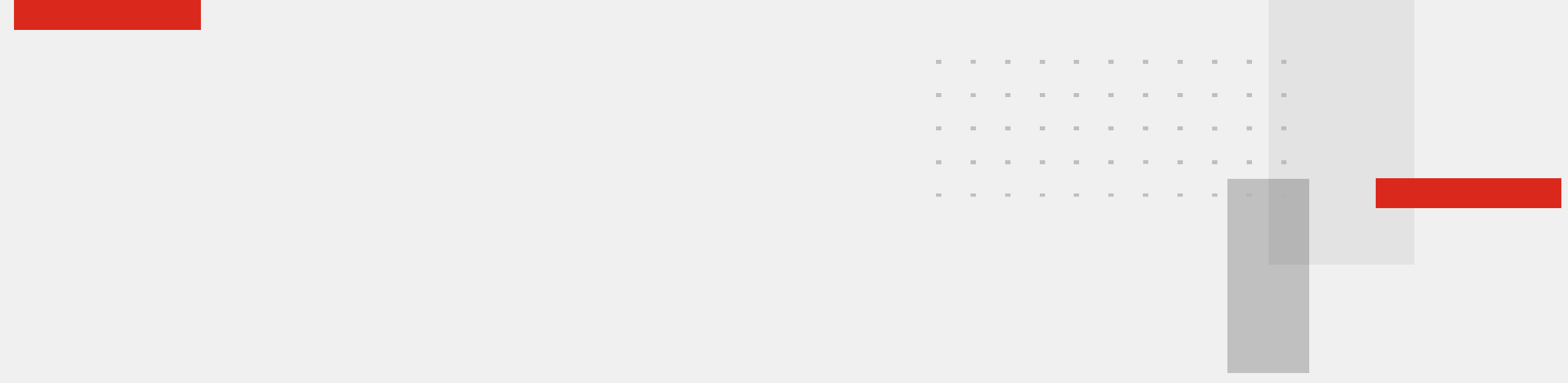


- Management traffic travels through the vxlan tunnel
- User's traffic stays local
- If routing is required, a layer 3 device should handle this task

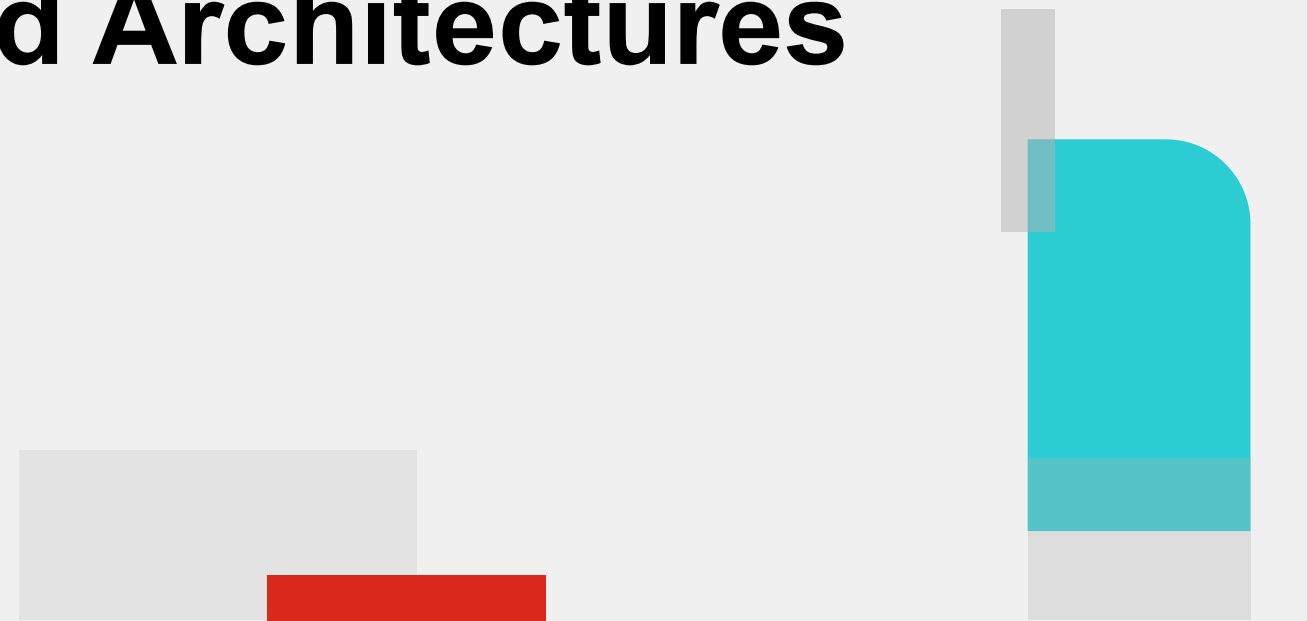
FortiSwitch VLANs over VXLAN

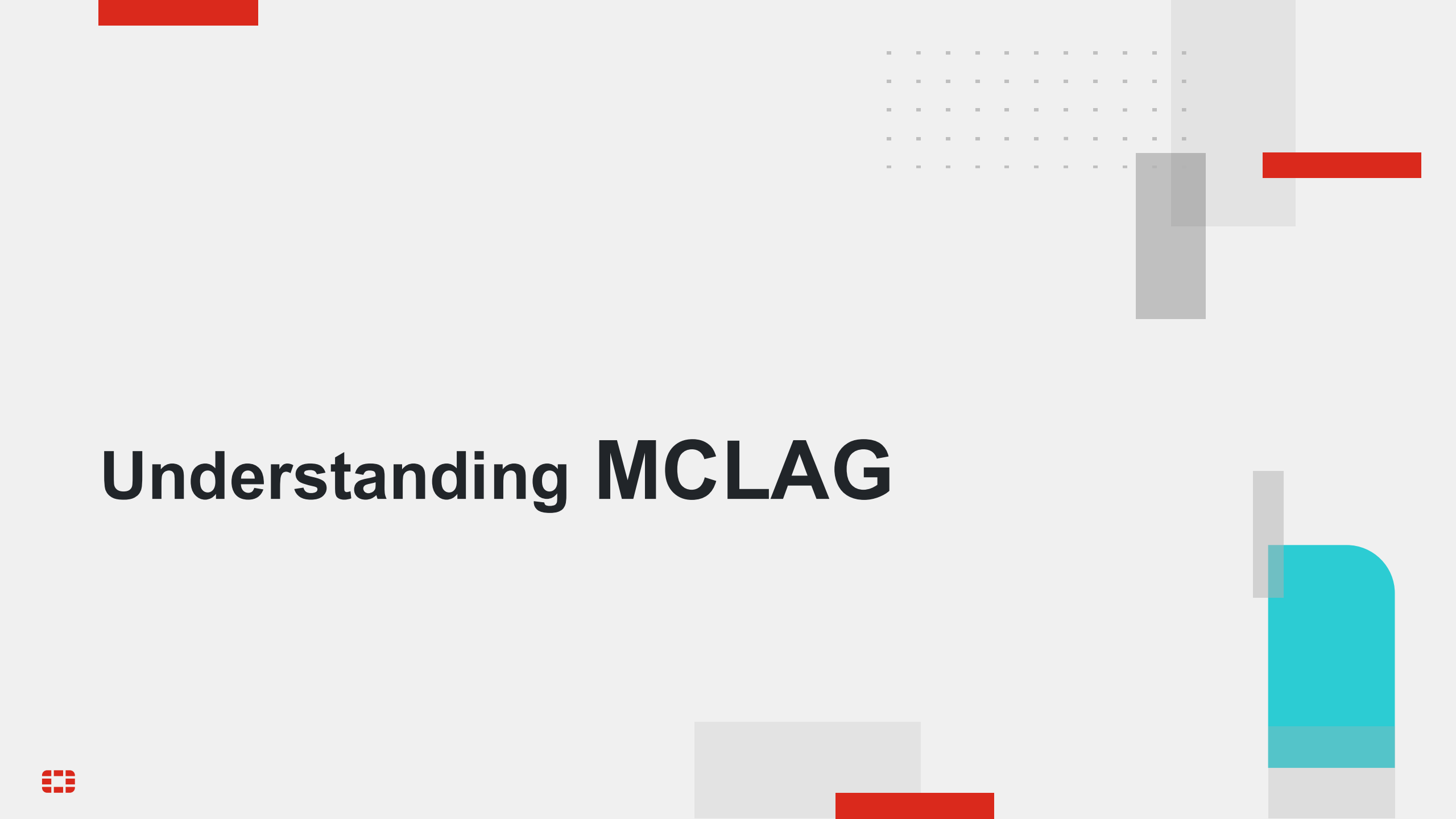


- Management and user traffic travels through the vxlan tunnel
- Allows Security Fabric functionality to be applied to devices connecting to the FortiSwitch unit
- [Check Fortiswitch Compatibility Matrix](#)



FortiLink Advanced Architectures



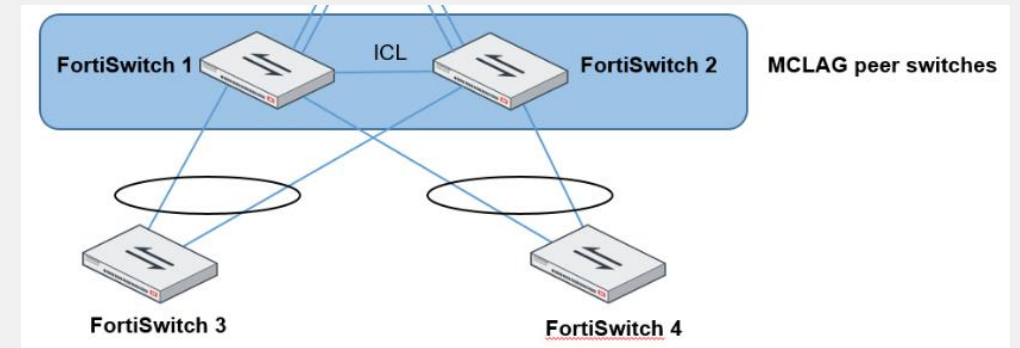
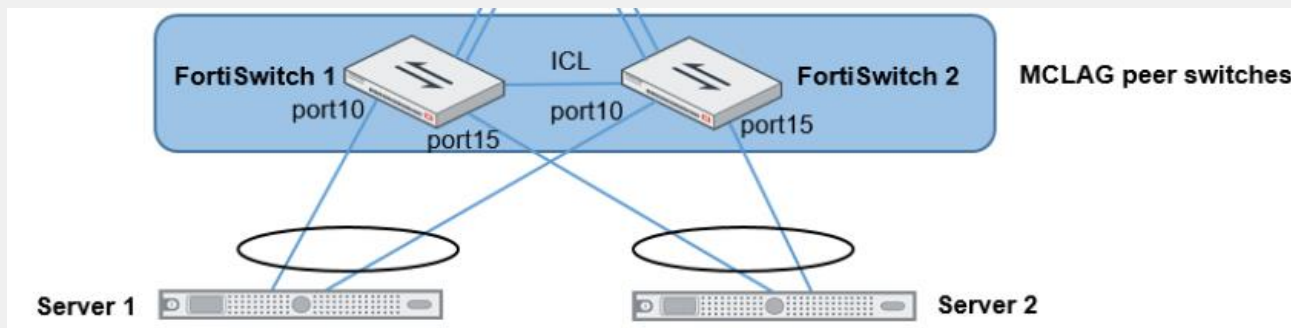


Understanding MCLAG



Understanding MCLAG

- **MC-LAG – Multi-chassis link aggregation group.**
Type of link aggregation group (LAG) with constituent ports that terminate on separate chassis, primarily for the purpose of providing redundancy in the event one of the chassis fails.



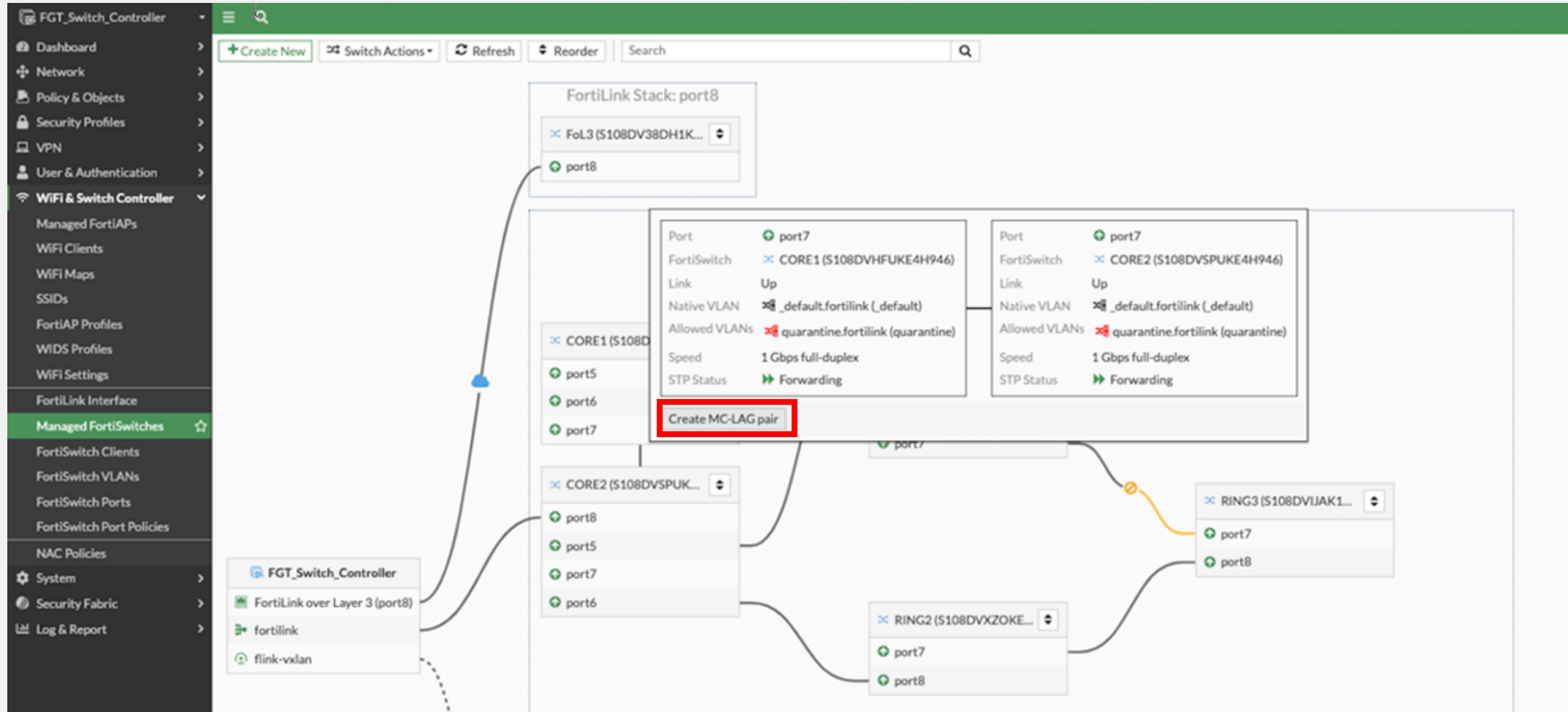
MCLAG Requirements

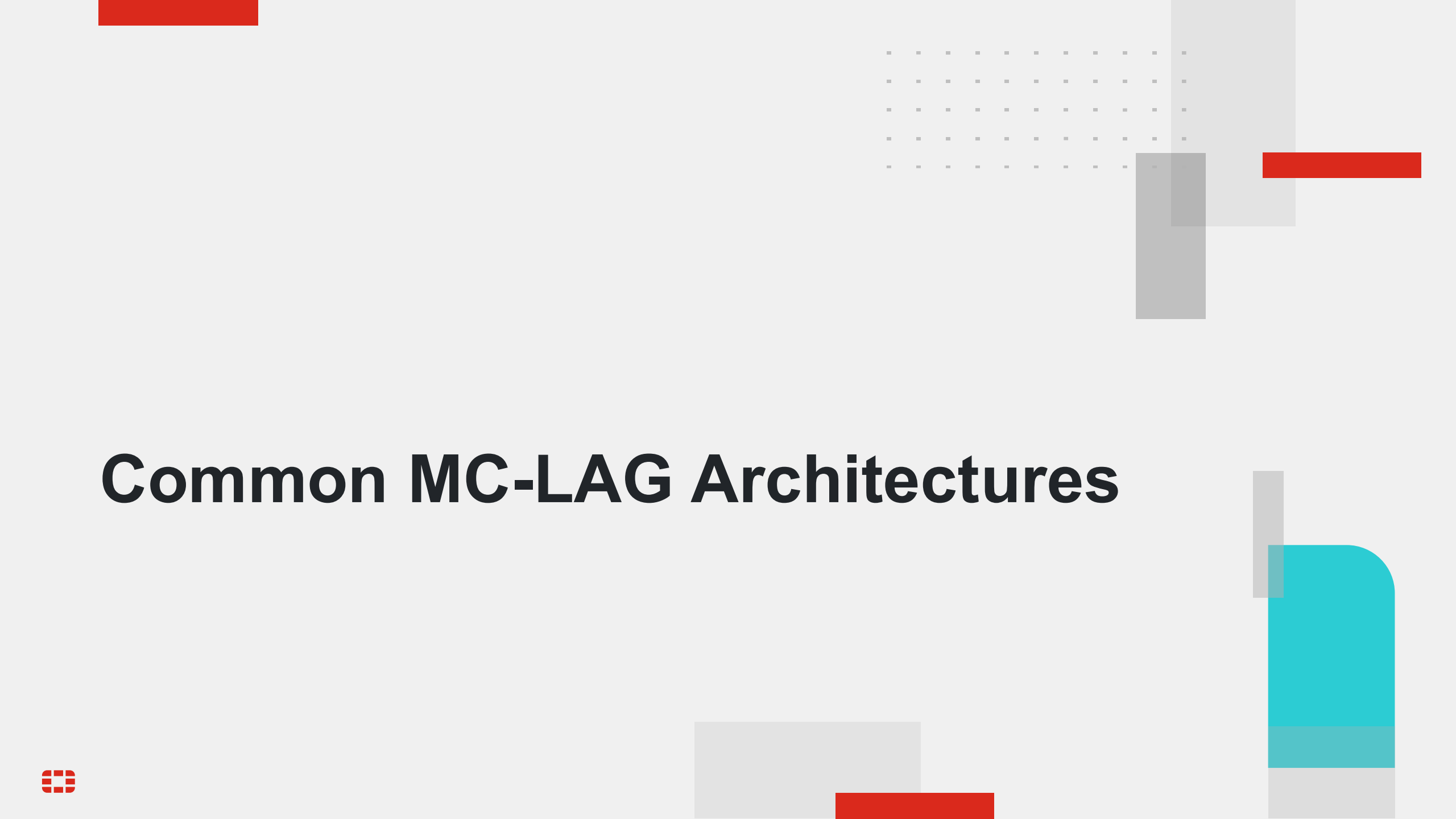
- **SAME HARDWARE MODEL AND SOFTWARE**
 - Mismatched configs are not officially supported.
- Max of 2 Switches per MCLAG Cluster
- Routing features not available in Fortilink (**This has changed in 7.4.1**)
- MCLAG-ICL (inter-chassis link) must be created each FSW MCLAG peer.
- 2XX series and up support ICL connection to form MCLAG peers

Feature	GUI Supported	FSR-108F	FSR-112F-POE	FSR-216F-POE	FSR-424F-POE	1xxE, 1xxF	110G-FPOE, 124G, 124G-FPOE	200 Series	4xxE	500 Series	6xxF	1024E, 1048E, 1048G, T1024E, T1024F-FPOE	2048F	3032E, 3032G
MCLAG (multichassis link aggregation group)	Partial	—	—	—	🔗	—	—	🔗	🔗	🔗	🔗	🔗	🔗	🔗
STP supported in MCLAGs	—	—	—	—	🔗	—	—	🔗	🔗	🔗	🔗	🔗	🔗	🔗
IGMP snooping support in MCLAG	✓	—	—	—	🔗	—	—	🔗	🔗	🔗	🔗	🔗	🔗	🔗
Layer-3 (IPv4) routing in MCLAG	—	—	—	—	VRRP and static	—	—	VRRP and static	VRRP and static	✓	—	✓	✓	✓



Single Tier MCLAG Configuration

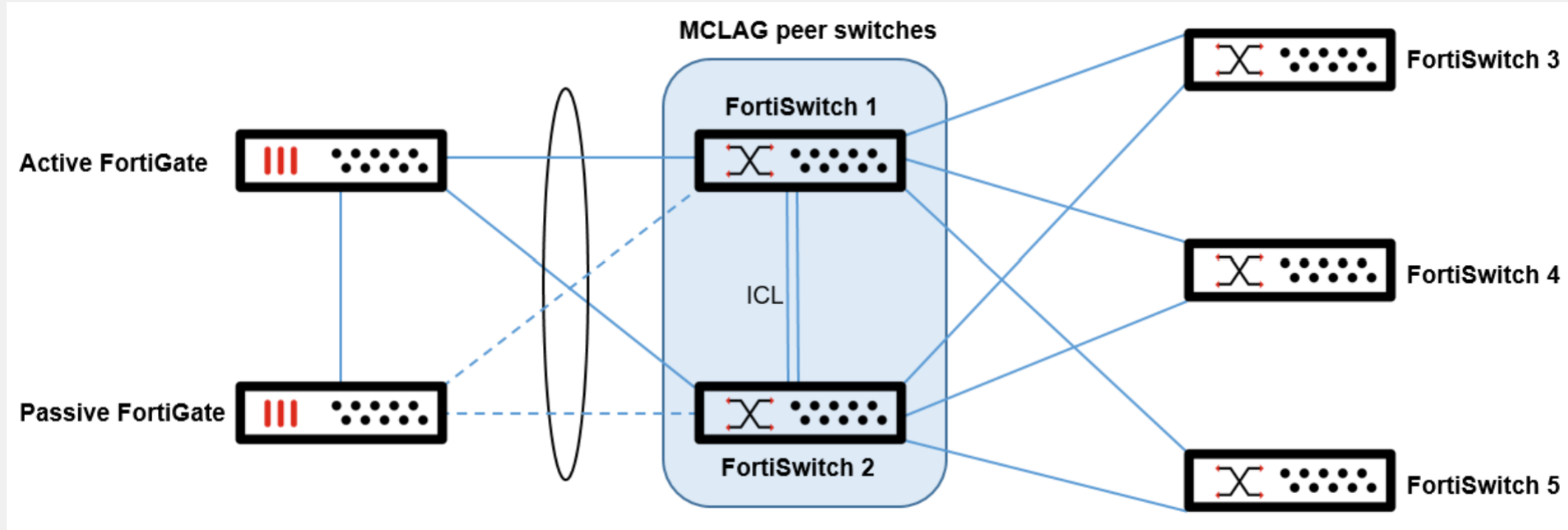




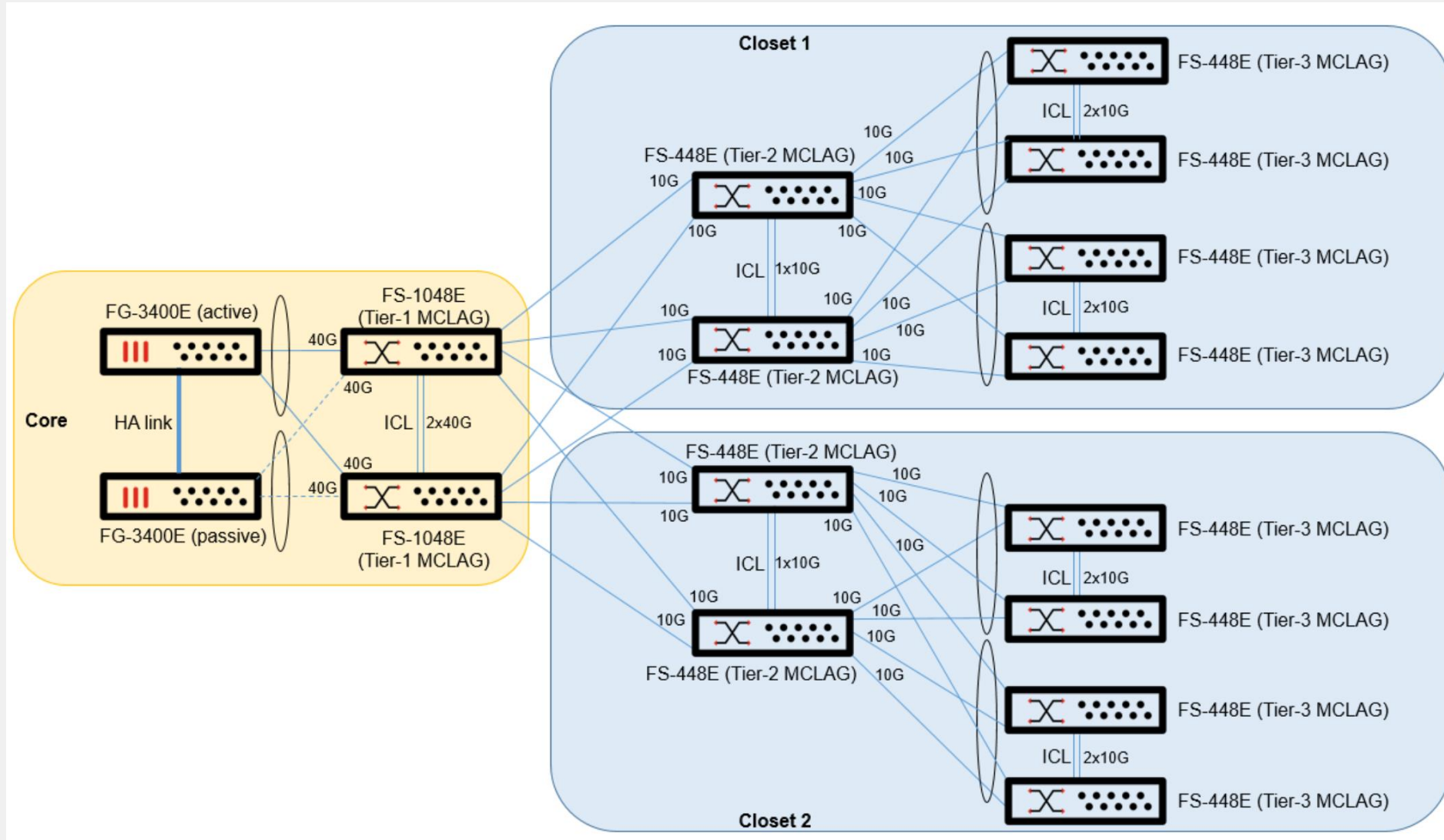
Common MC-LAG Architectures



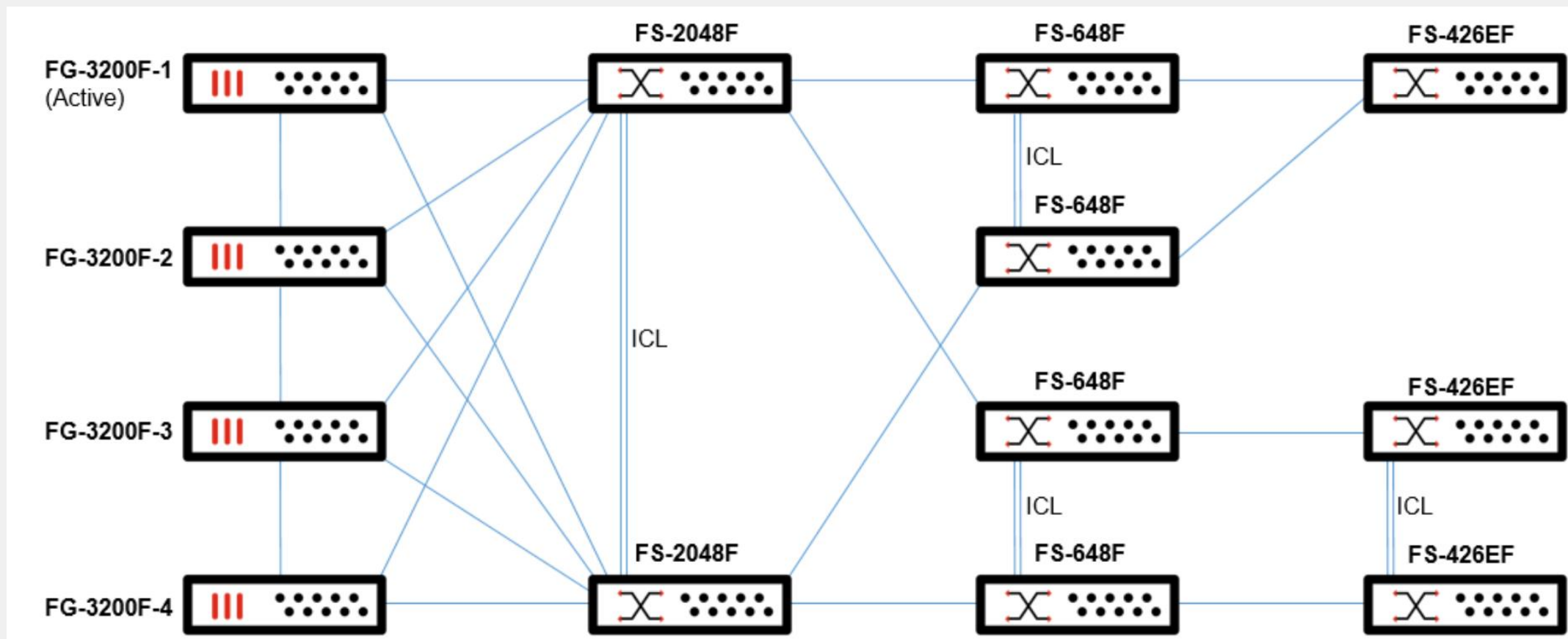
Switch redundancy with MCLAG



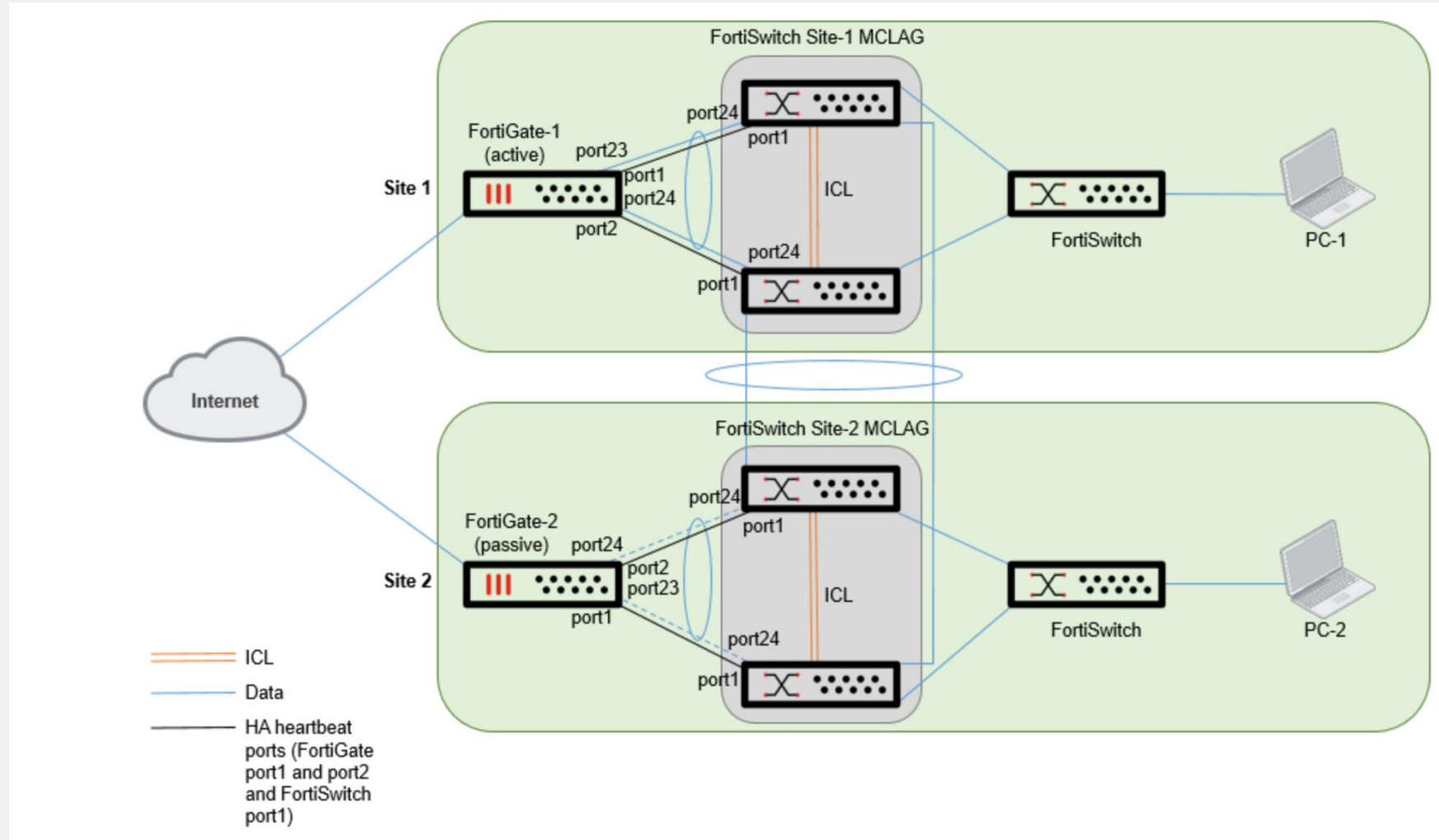
Three-tier FortiLink MCLAG configuration



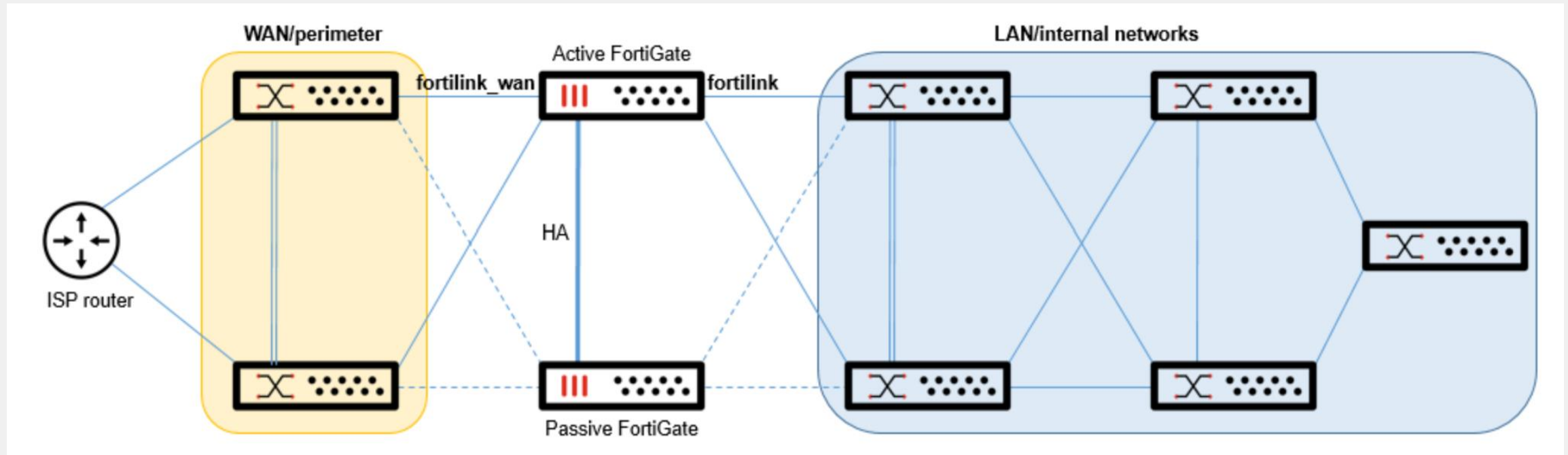
FortiLink with an HA cluster of four FortiGate units

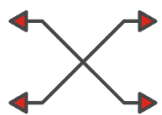


HA-mode FortiGate units in different sites



Isolated LAN/WAN with multiple FortiLink interfaces



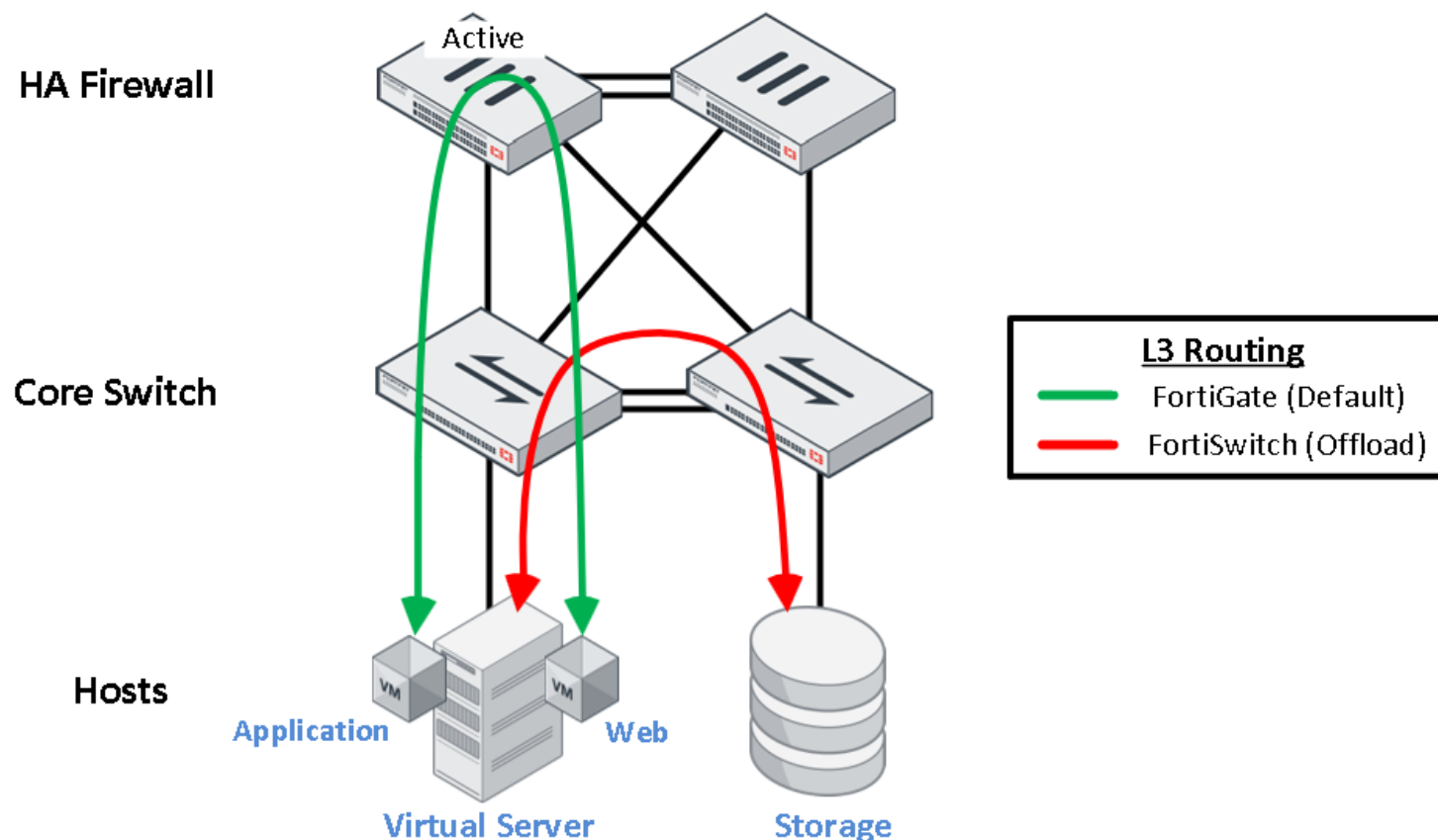


FortiLink Inter-VLAN Routing Offload

• DATA CENTER USE CASE

- Application VM has traffic routed from 'application' VLAN to 'web' server VLAN with the FortiGate doing the L3 inter-VLAN routing. FortiGate provides firewall policy enforcement, UTM/UTP protection, and traffic visibility.
- Virtual Infrastructure Server has traffic routed from 'compute' VLAN to 'storage' VLAN to access shared storage on SAN storage appliance. Inter-VLAN routing done on the managed FortiSwitches provides high speed, low-latency connectivity. Inter-VLAN Routing Offload will be enabled for this traffic.

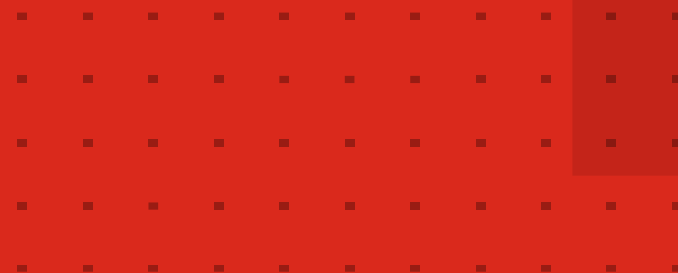
Inter-VLAN Routing Offload Data Center Use Case

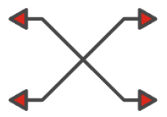




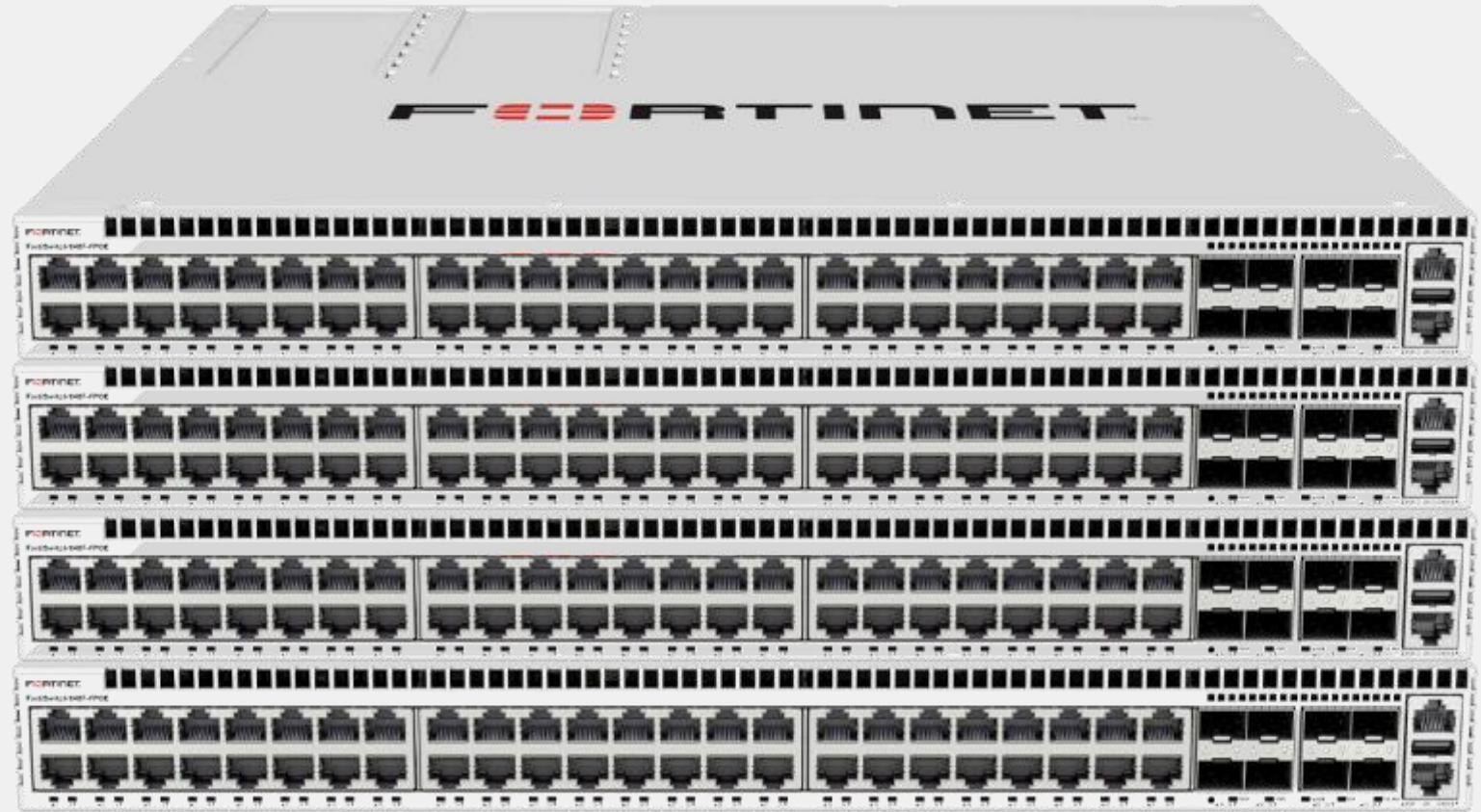
FortiSwitch Stacking

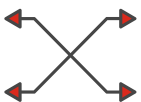
Deployment and Management





FortiSwitch Stacking

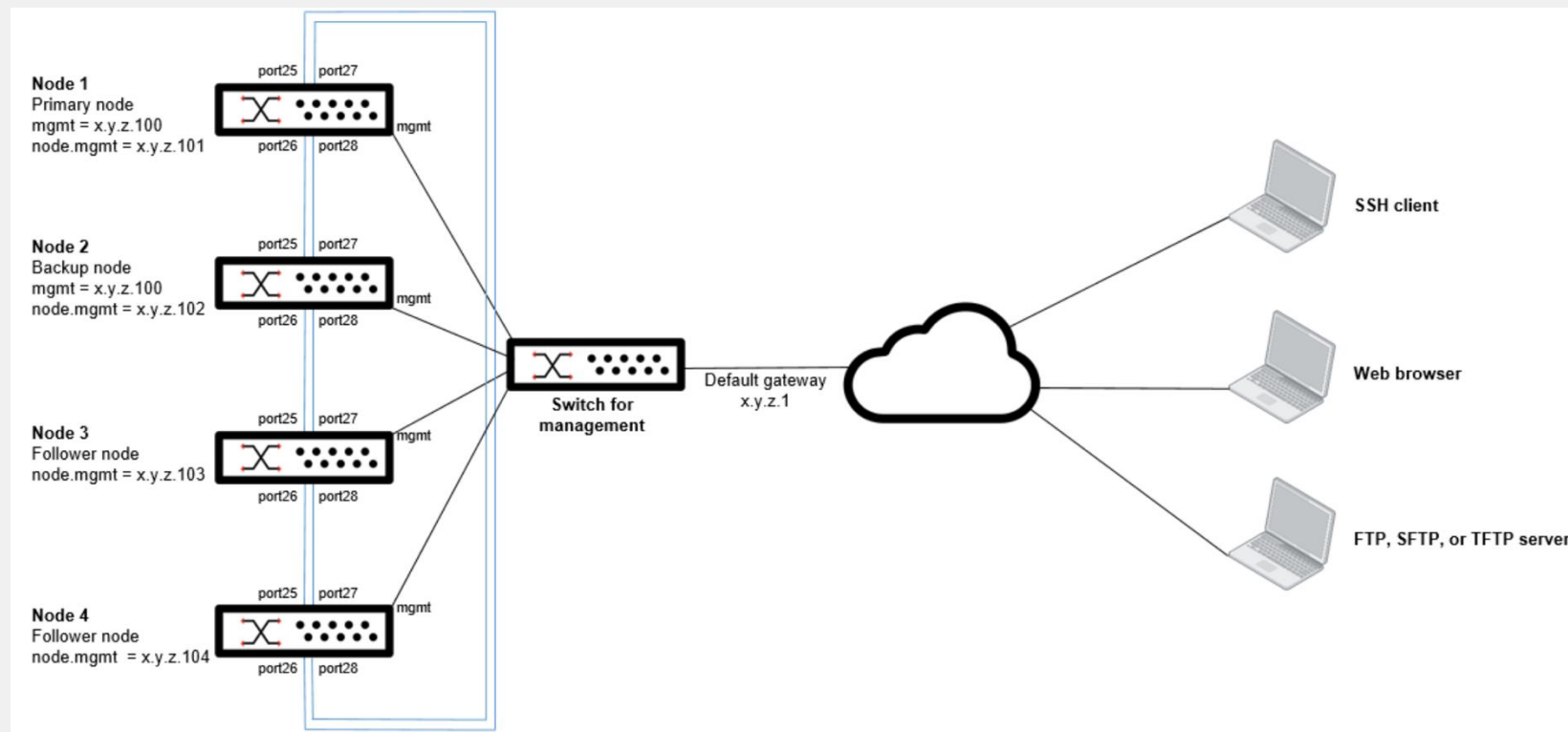


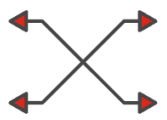


Stacking

FS-6xxF

- Single Management IP
- Active-standby controllers
- L2 [STP, LLDP, LACP]
- Cross-stack LAG
- 802.1X
- Mirror
- Flow Tracking
- 4 nodes same model
- FSWOS 7.6.2-based image
- [Stacking Guide](#)

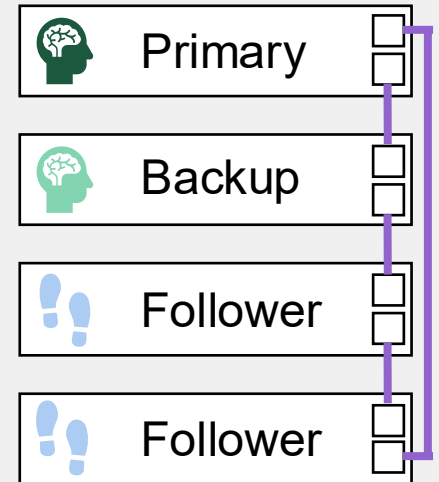


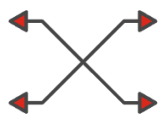


Node roles in a stack

Stack members have different roles within the stack:

- **Primary** : This switch acts as the main controller, managing the stack's configuration
- **Backup** : If the primary switch fails, the backup switch automatically takes over the primary's role, ensuring network continuity
- **Follower** : These switches participate in the stack, contributing to the overall network capacity and functionality, but they don't have the same level of control or responsibility as the primary or backup

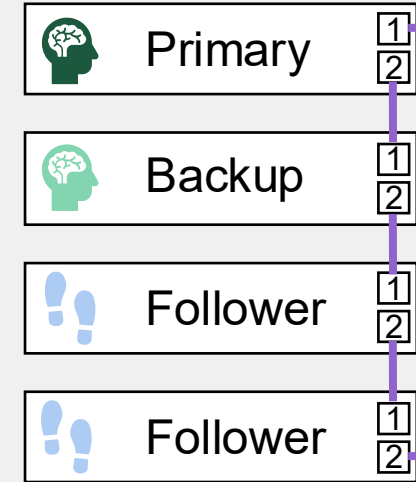




Cabling

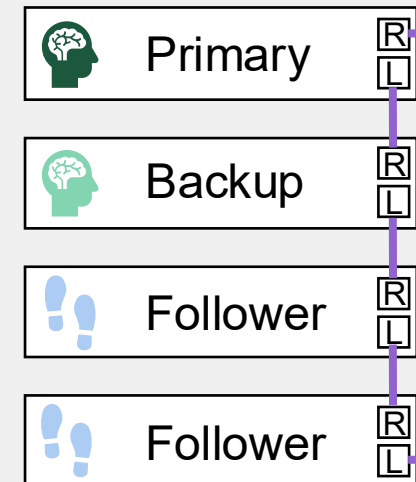
A stack is a ring ...

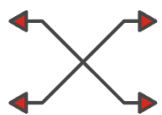
- Port 1 connects to port 2 and so on ...



On Fortiswitch the notion of Right ports and Left ports is used.

- Right ports connect to Left ports



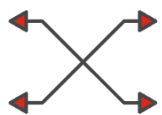


Interfaces

sw#/port#

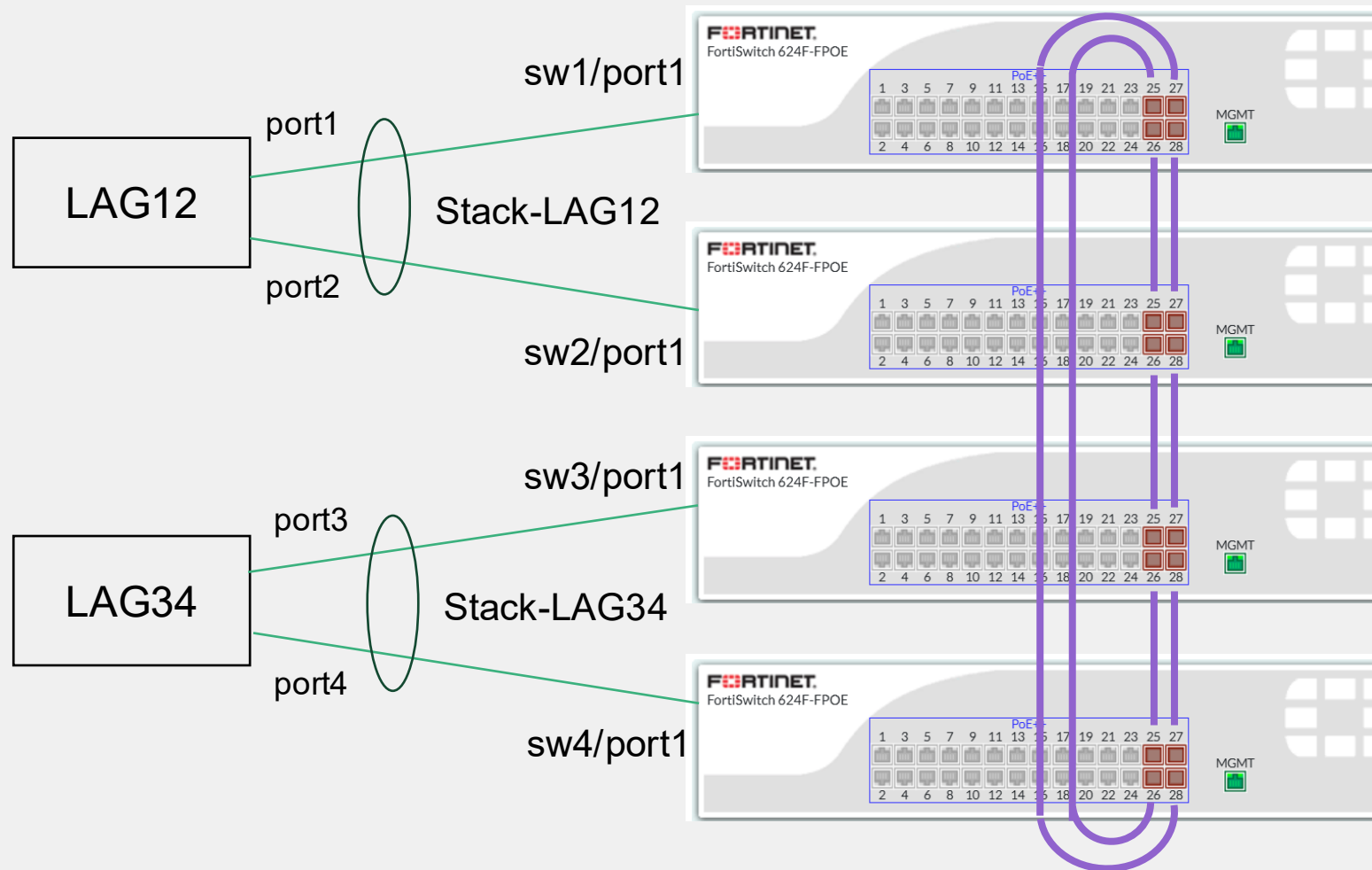
FortiSwitch 624F-FPOE FSW-Stack-GA				
System	Name	Traffic (Last Day)	Speed Setting	
Switch				Link
Physical Ports				
Trunks	sw2/port17	0.000bps	Auto-Negotiation	↑
Interfaces	sw2/port18	0.000bps	Auto-Negotiation	↑
Port Security	sw2/port19	0.000bps	Auto-Negotiation	↑
MAC Security	sw2/port20	0.000bps	Auto-Negotiation	↑
STP	sw2/port21	0.000bps	Auto-Negotiation	↑
Flap Guard	sw2/port22	0.000bps	Auto-Negotiation	↑
DHCP Snooping	sw2/port23	0.000bps	Auto-Negotiation	↑
MAC Limit	sw2/port24	0.000bps	Auto-Negotiation	↑
LLDP-MED	sw2/port25	0.000bps	Max Speed Supported by Module	↑
ACL	sw2/port26	0.000bps	Max Speed Supported by Module	↑
POE	sw3/port1	23.73kbps	Auto-Negotiation	↑
sFlow	sw3/port2	25.18kbps	Auto-Negotiation	↑
Mirror	sw3/port3	0.000bps	Auto-Negotiation	↑
VLAN	sw3/port4	0.000bps	Auto-Negotiation	↑
Storm Control	sw3/port5	0.000bps	Auto-Negotiation	↑
MAC Entries	sw3/port6	0.000bps	Auto-Negotiation	↑
QoS	sw3/port7	0.000bps	Auto-Negotiation	↑
Monitor	sw3/port8	0.000bps	Auto-Negotiation	↑
Router	sw3/port9	0.000bps	Auto-Negotiation	↑
Log	sw3/port10	0.000bps	Auto-Negotiation	↑
	sw3/port11	0.000bps	Auto-Negotiation	↑

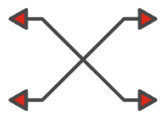




Cross-stack LAG

Trunk with members in different nodes





Phase I Implementation

L2 Features

- VLANs
- VLAN Assignment / Mapping
- STP
- Trunks (LACP/Static)
- LLDP
- POE
- Port Mirror
- Packet Sampling (sniffer)
- Flow tracking
- Static MAC
- 802.1x
- SFP Module Support

System Features

- Single IP management
- CLI/GUI
- Config Sync
- Single failure recovery (1 ring or 1 node)
- 4 homogeneous nodes (all same model, same ring port config)
- DHCP Server
- DHCP Client

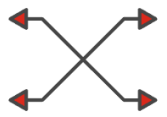
System Features

- Single IP management
- DHCP Client

Failover protection

L2 Features

- STP
- Trunks (LACP/Static)



Connecting stack to FortiLink fabric

