OTSDN What Is It and Why Do You Need It?

Jason Dearien

Schweitzer Engineering Laboratories, Inc.

Operational Technology Software-Defined Networking (OTSDN)

- The purpose of OTSDN
- How OTSDN works
- The benefits of OTSDN

Requirements of a Critical OT Network

- Determinism and low latency
- Precise time
- Fast fault detection, isolation, and recovery
- Cybersecurity
- Monitoring, self-testing, and alarming
- Maintainability and diagnostics
- Hardware rated for critical infrastructure

Message Delivery Performance Criteria

Defined by International Standards

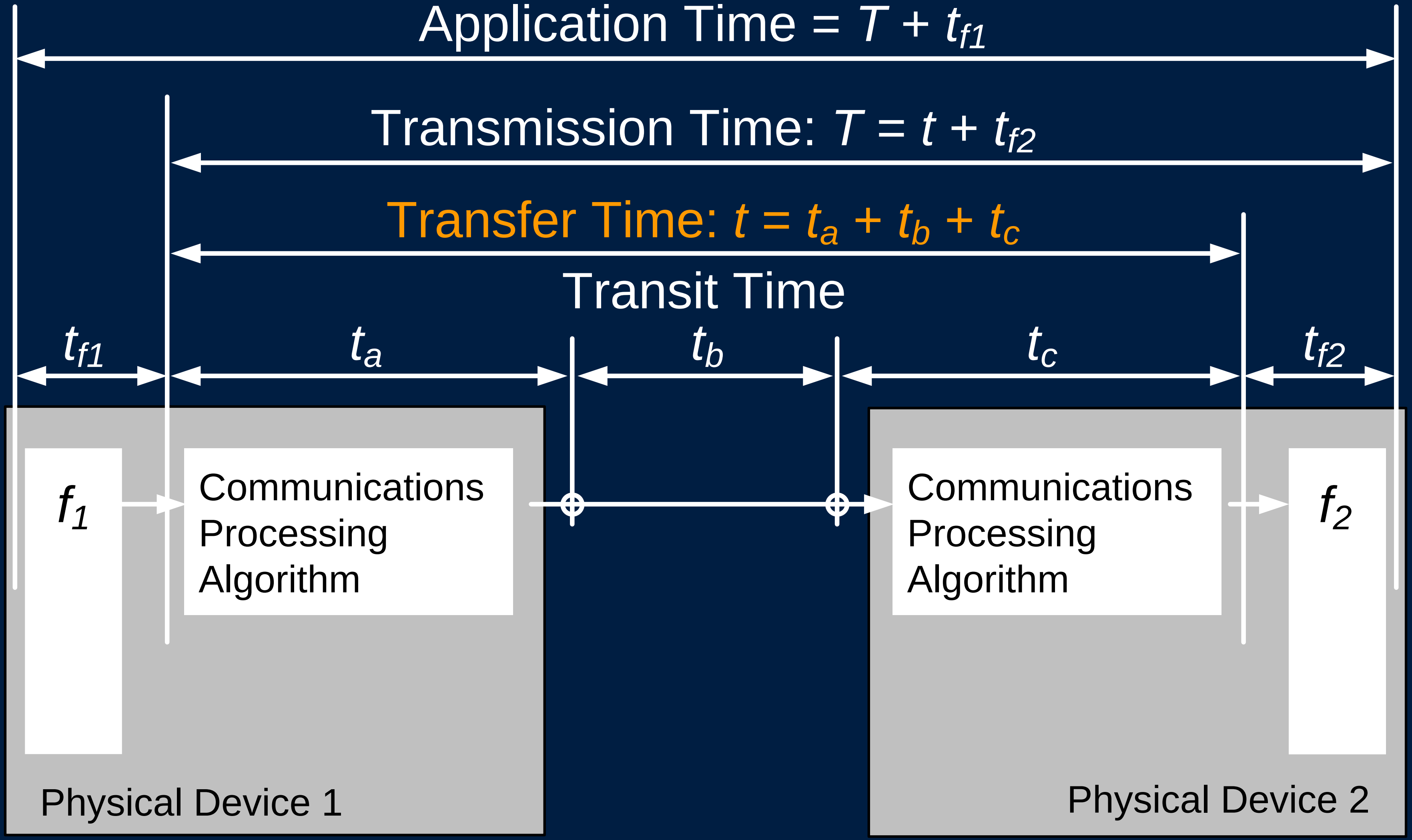
Standard	Performance	Latency	Speed
IEC 61850	✓	✓	✓
IEC 60834	✓	✓	
IEC 15802	✓	✓	
IEEE 802.1	✓	✓	

Message Delivery Quality Criteria

Defined by International Standards

Standard	Dependability and Security	Availability	Reliability
IEC 61850	✓	✓	✓
IEC 60834	✓	✓	
IEEE 802.1		✓	
IEC 60870			✓
IEEE 1613			✓

Signal Data Exchange Is Measured as Transfer Time


Application Time = $T + t_{f1}$
Transmission Time: $T = t + t_{f2}$
Transfer Time: $t = t_a + t_b + t_c$
Transit Time
t_{f1}
t_a
t_b
t_c
t_{f2}
f_1
Communications Processing Algorithm
Communications Processing Algorithm
f_2
Physical Device 1
Physical Device 2

Application Latency Classes

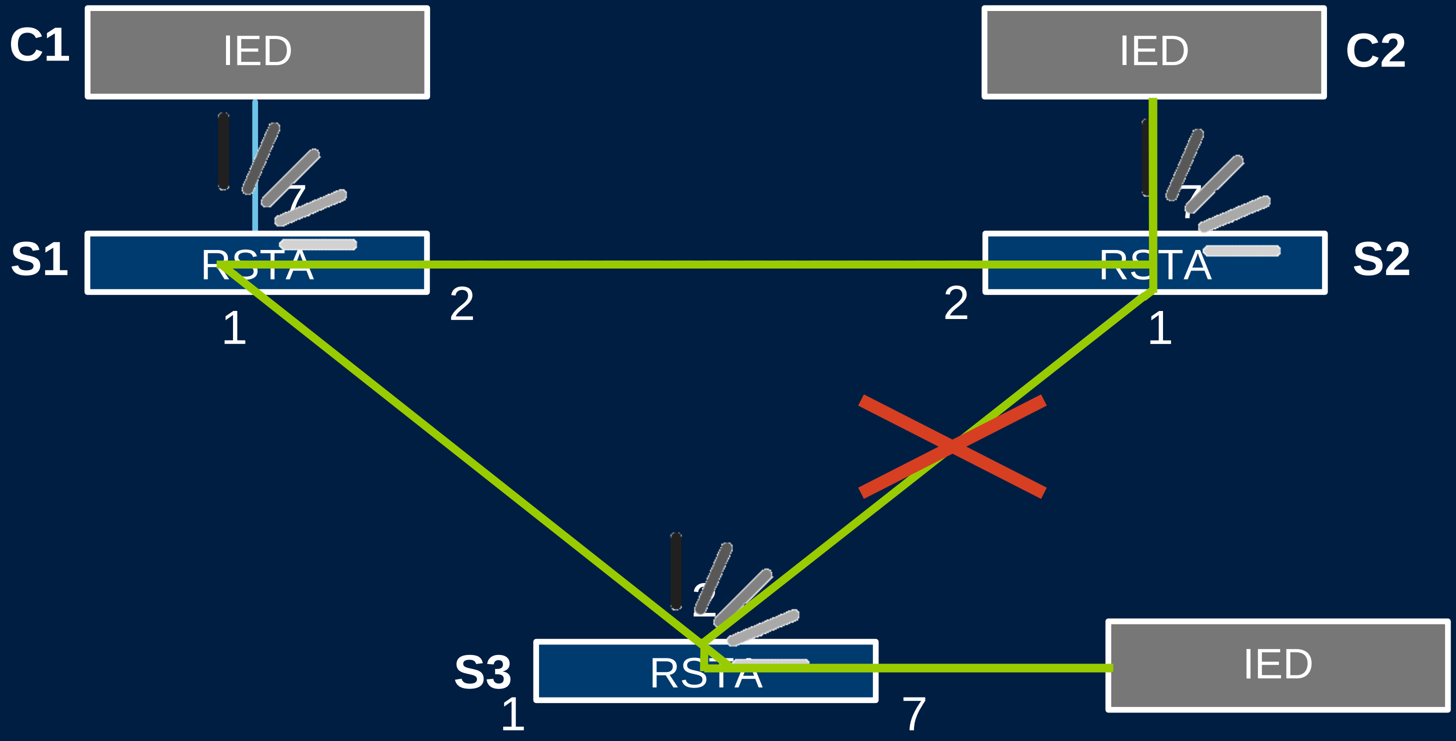
IEC / TR 61850-90-4 Network Engineering Guidelines

Transfer Time Class	Transfer Time (ms)	Application Example
TT0	>1,000	Files, events, and log contents
TT1	1,000	Events and alarms
TT2	500	Operator commands
TT3	100	Slow automatic interactions
TT4	20	Fast automatic interactions
TT5	10	Releases and status changes
TT6	3	Trips and blockings

Challenges of Traditional Ethernet Switching in an OT Environment

- Designed for plug and play
- Conveniently does things “we don’t want”
- Reactive failover
- Topology-dependent performance
- Difficult to achieve 100 percent test coverage

Using IEC 62439-1 RSTA for Network Healing



Peer-to-peer RSTP informs RSTA

How OTSDN Works

- Uses standard SDN technology
- Focuses on solving critical infrastructure problems
  - Performance
  - Security
  - Resiliency
- Does not use typical data center dynamic SDN

True Traffic Engineering for Ethernet

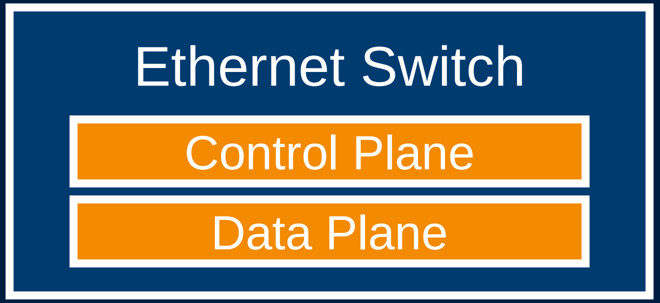
Standardized OpenFlow® Protocol

Traditional Ethernet Switch

Individual control plane and individual data plane

SDN Switch

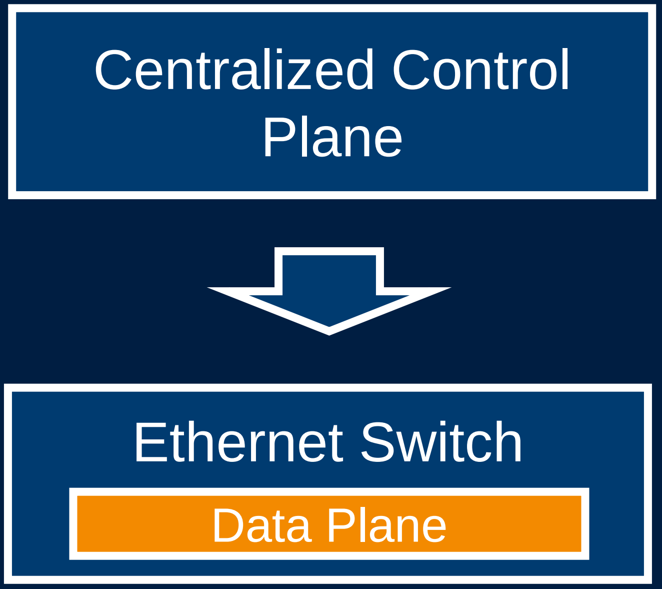
Centralized control plane and individual data plane



Ethernet Switch

Control Plane

Data Plane

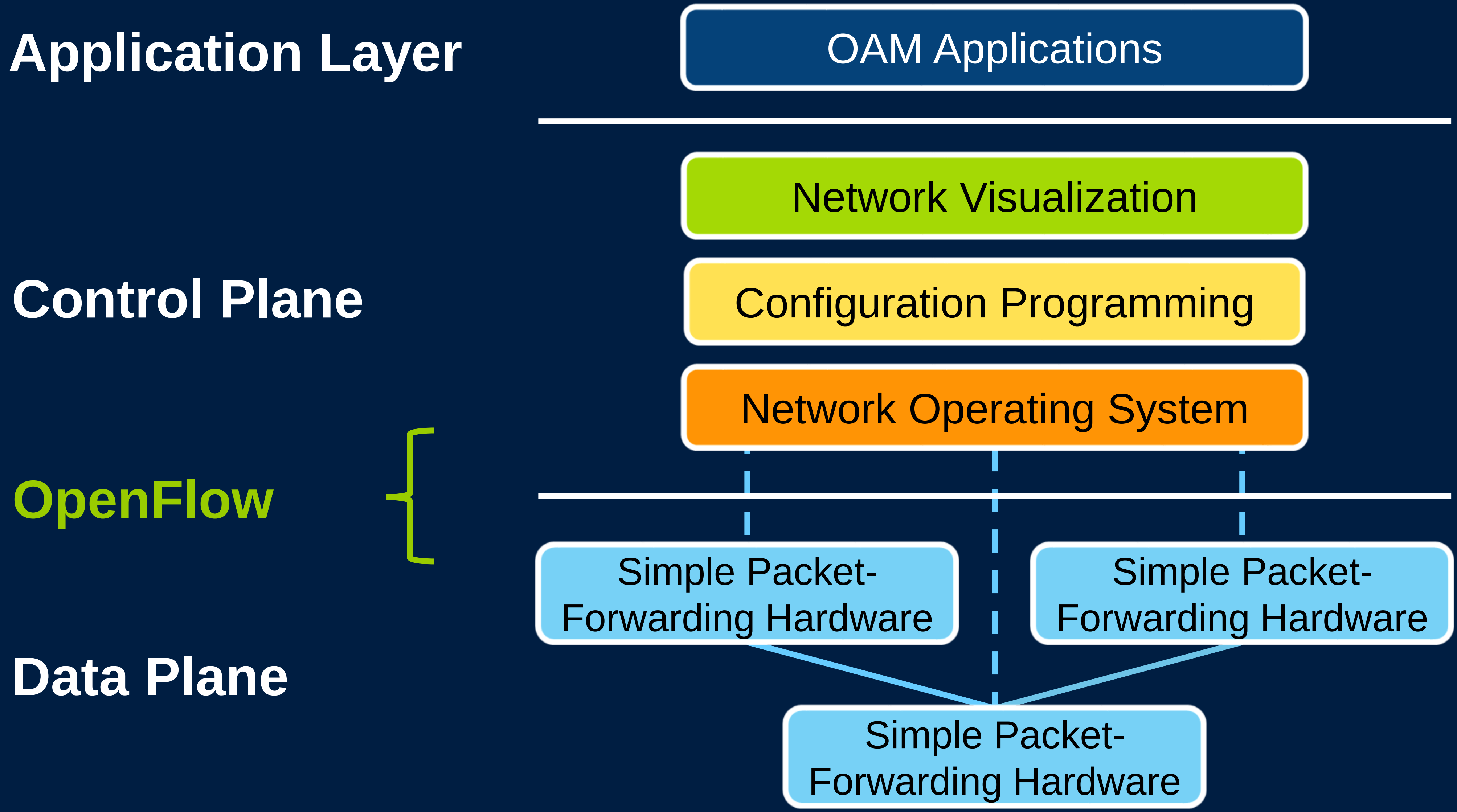


Centralized Control Plane

Ethernet Switch

Data Plane

Introducing SDN and OpenFlow

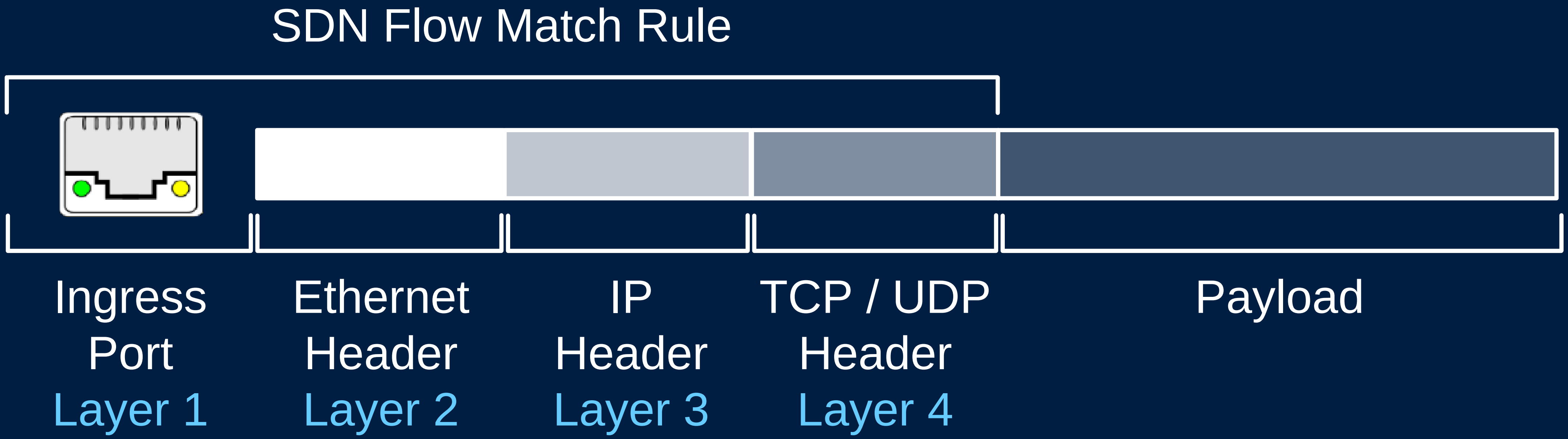

Application Layer
OAM Applications
Network Visualization
Control Plane
Configuration Programming
Network Operating System
OpenFlow
Simple Packet-Forwarding Hardware
Simple Packet-Forwarding Hardware
Data Plane
Simple Packet-Forwarding Hardware

How SDN Works

The data plane inspects each Ethernet packet and performs one or more of the following:

- **Match fields.** Matches flows based on the first four layers of the Ethernet packet
- **Instructions.** Performs one or more programmed actions
- **Counters.** Increments counters and sends counter data to a centralized point

Multilayer Matching Rules Allow Forwarding of Approved Packets



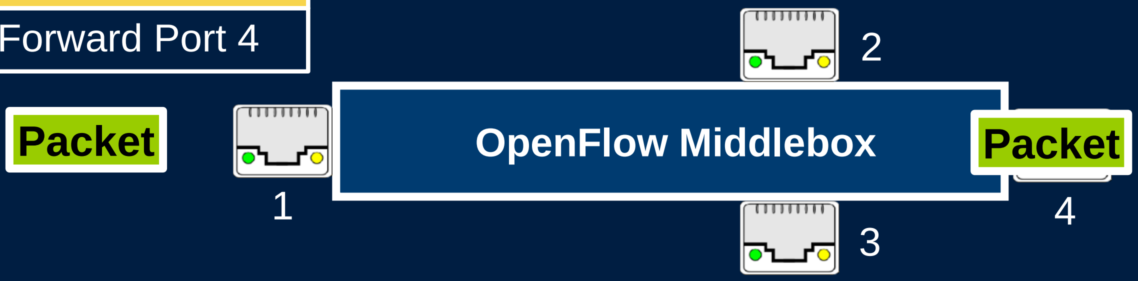
OpenFlow Match / Action Example

L2 Unmanaged Switch

Physical Port ID	Src MAC	Dst MAC	Ether Type	VLAN ID	IPv4 Src	IPv4 Dst	TCP/UDP Src	TCP/UDP Dst
1	*		*	*	*	*	*	*

00:30:A7:06:11:97

Action
Output Forward Port 4



OpenFlow Match / Action Example

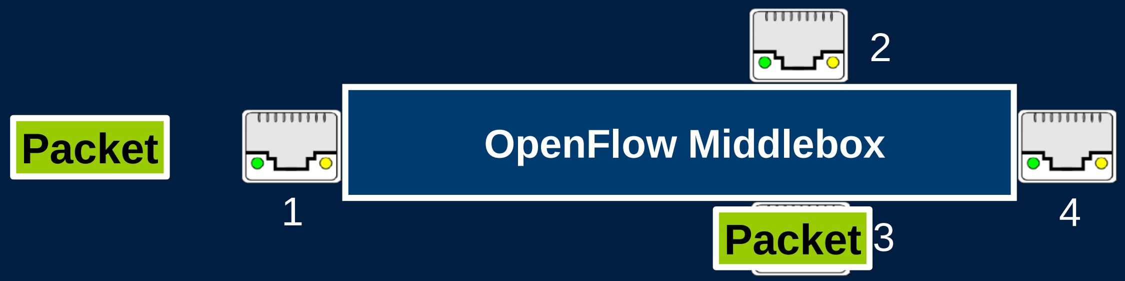
L3 Router

Physical Port ID	Src MAC	Dst MAC	Ether Type	VLAN ID	IPv4 Src	IPv4 Dst	TCP/UDP Src	TCP/UDP Dst
1	*		*	*	1.1.1.2	2.2.2.2	*	*

00:30:A7:06:13:29

Action
Set Source MAC 00:30:A7:06:29:01

Action
Output Forward Port 3



OpenFlow Match / Action Example

L4 Network Address Translation (NAT)

Physical Port ID	Src MAC	Dst MAC	Ether Type	VLAN ID	IPv4 Src	IPv4 Dst	TCP/UDP Src	TCP/UDP Dst
1	*		*	*	1.1.1.2	2.2.2.2	*	TCP 20000

00:30:A7:06:13:29

Action

Set Source MAC 00:30:A7:06:29:01

→

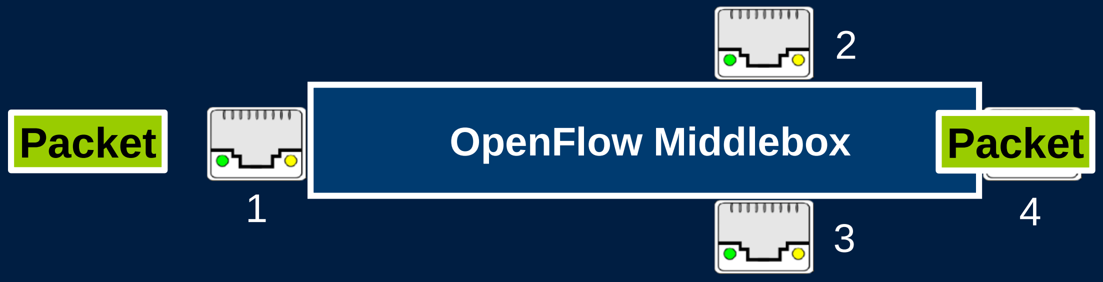
Action

Set IPv4 Source 2.2.2.1

→

Action

Output Forward Port 4



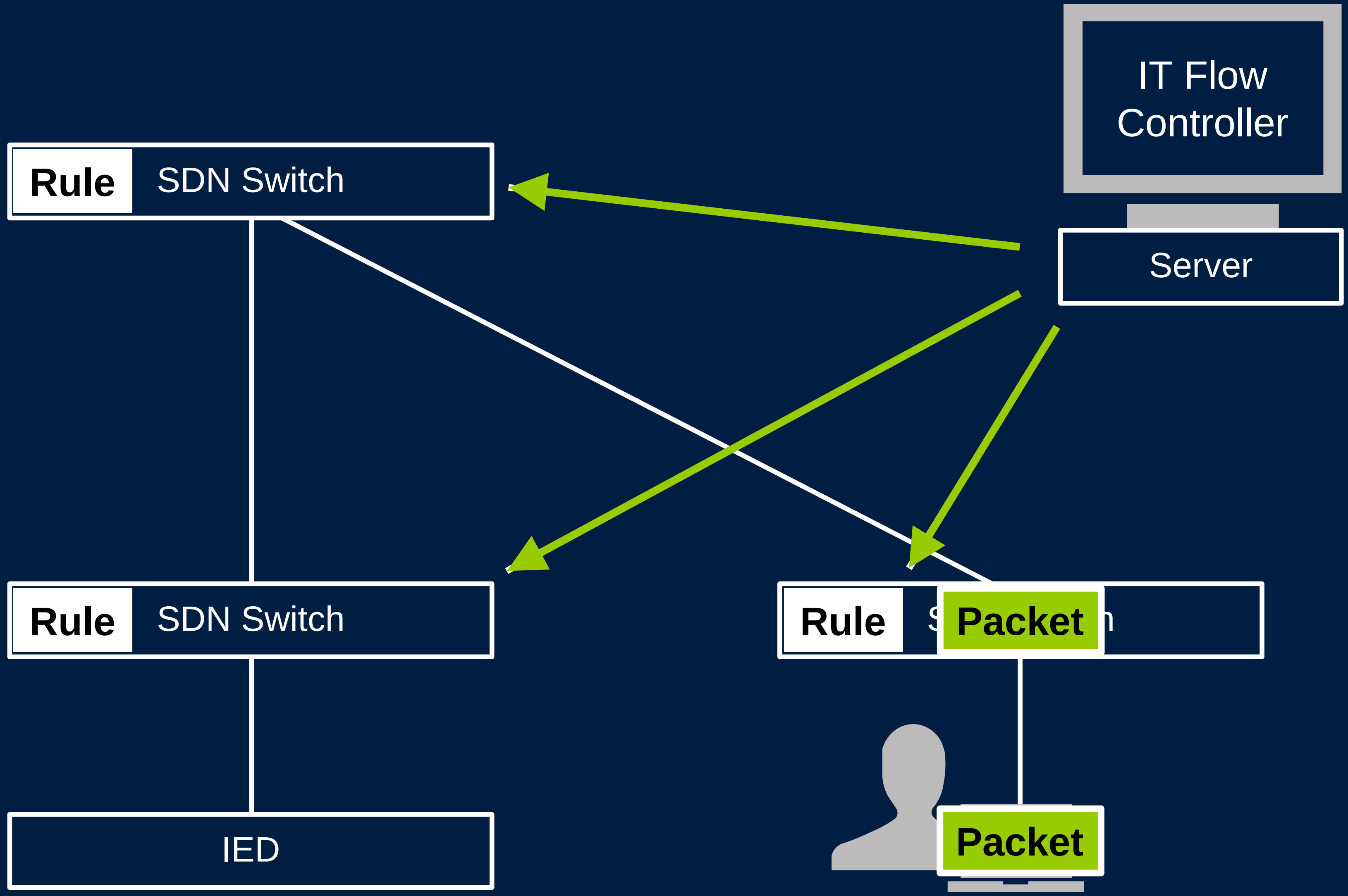
Traditional SDN vs. OTSDN

Reactive vs. Static Flows

Traditional SDN uses reactive flows to dynamically respond and adapt to changes in the network and traffic, resulting in the following weaknesses

- Reduced security
- Uncertain network performance
- SDN controller performance bottlenecking

Reactive IT SDN in Operation



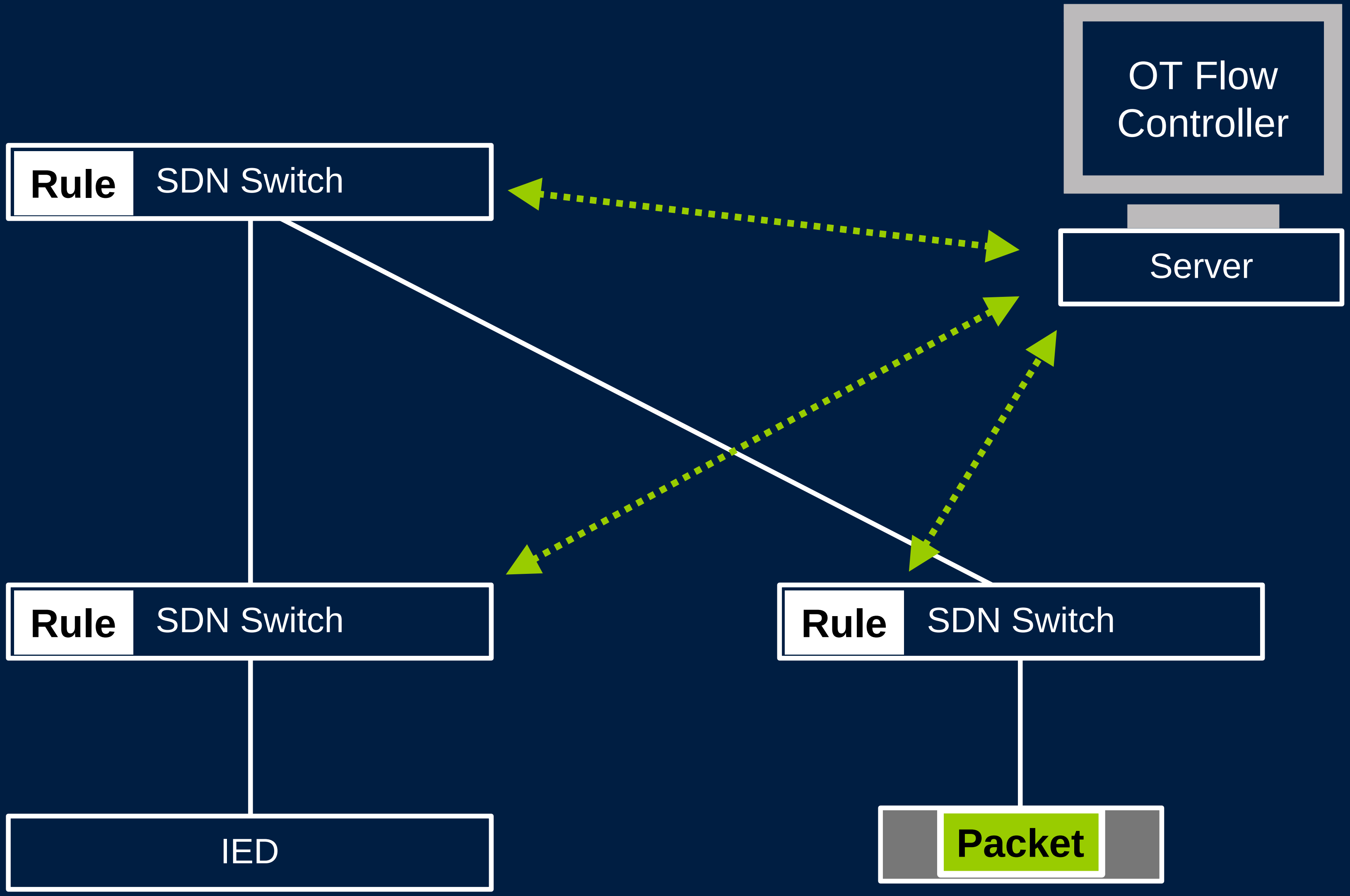
Traditional SDN vs. OTSDN

Reactive vs. Static Flows

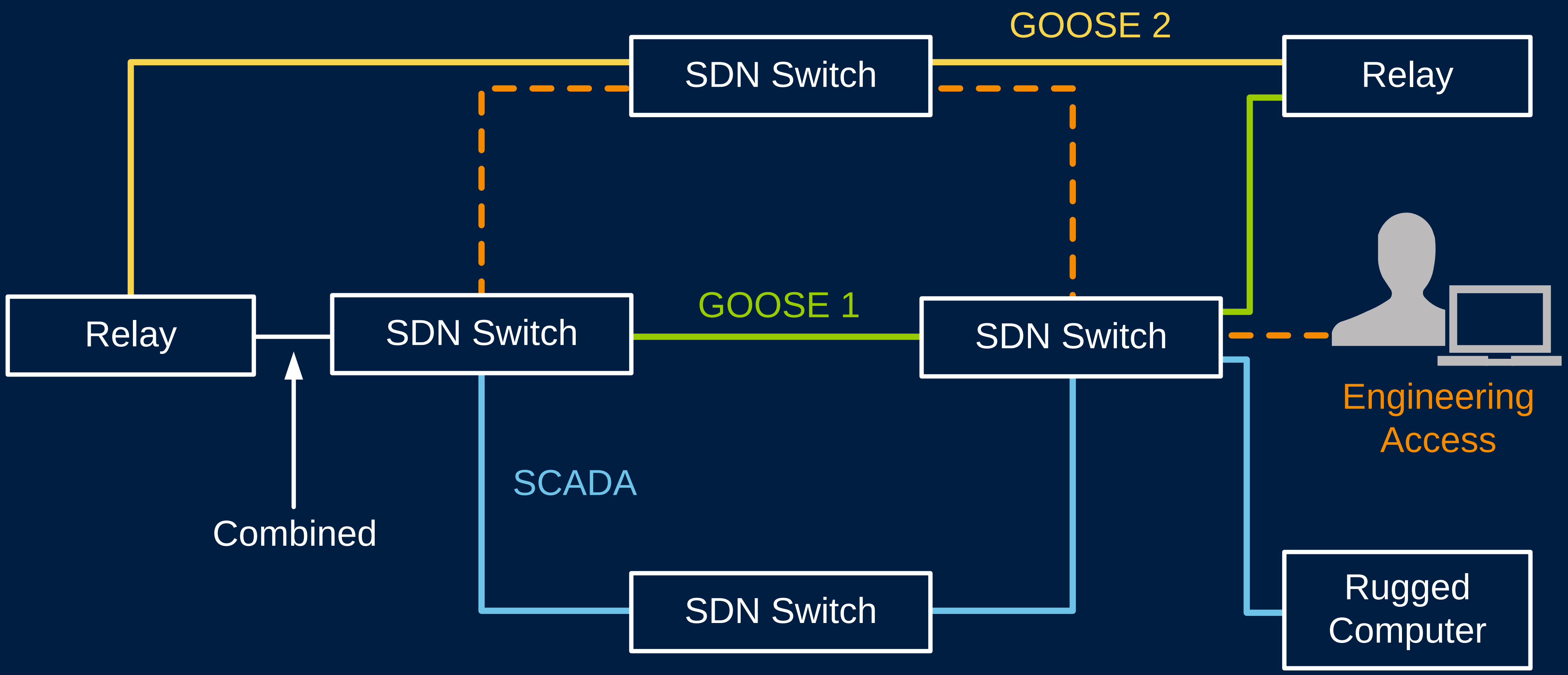
OTSDN uses static flows for proactive engineering of a known network configuration

- Static flows can be used because all traffic is known
- Networks never add or remove traffic or devices without an official change order
- New or unexpected traffic is dropped
- Network state and performance is always known and executes as designed

Proactive OTSDN in Operation

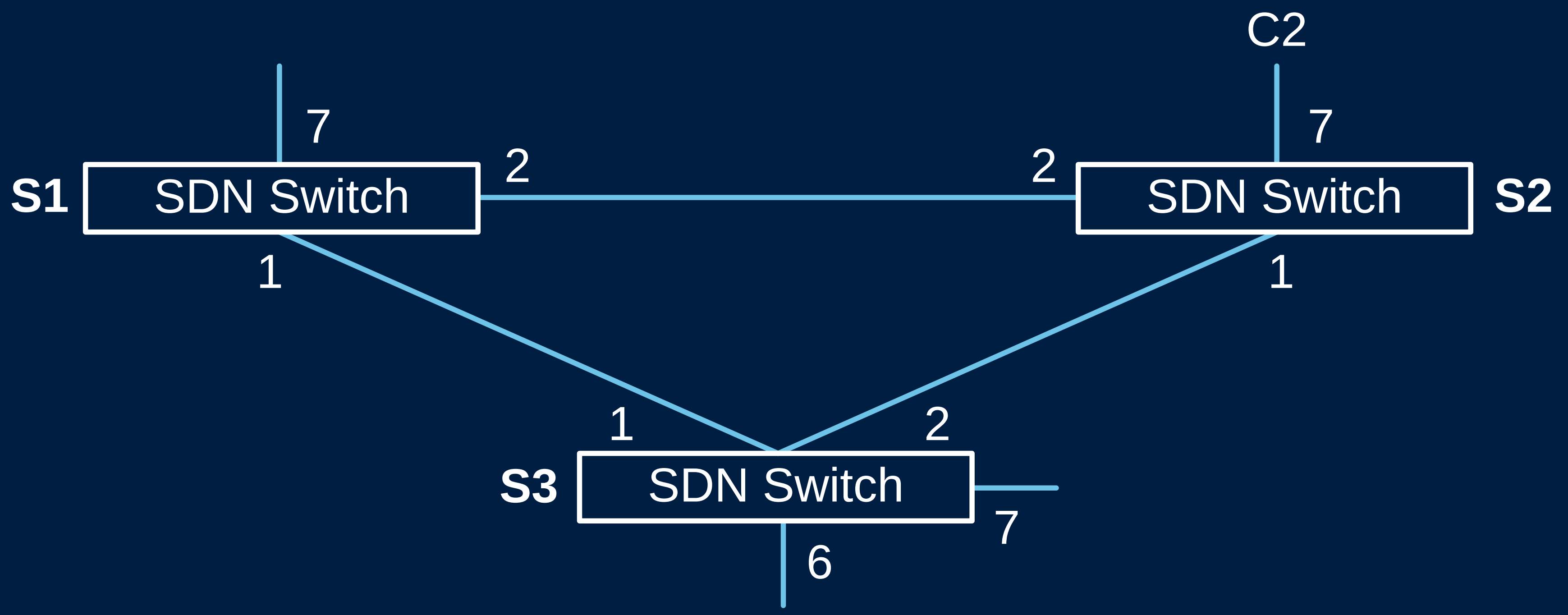


Design Traffic Paths Based on Requirements and Applications



Note: A flow controller is not required for network operation

Fast Failover SDN Rules



Rule	Switch	In Port	Ethertype	Destination IP	UDP Port	Action
A	S3	7	IPv4	C2	*	2, 1
B	S1	1	*	*	*	2
C	S2	1, 2	IPv4	C2	*	7

The Benefits of OTSDN

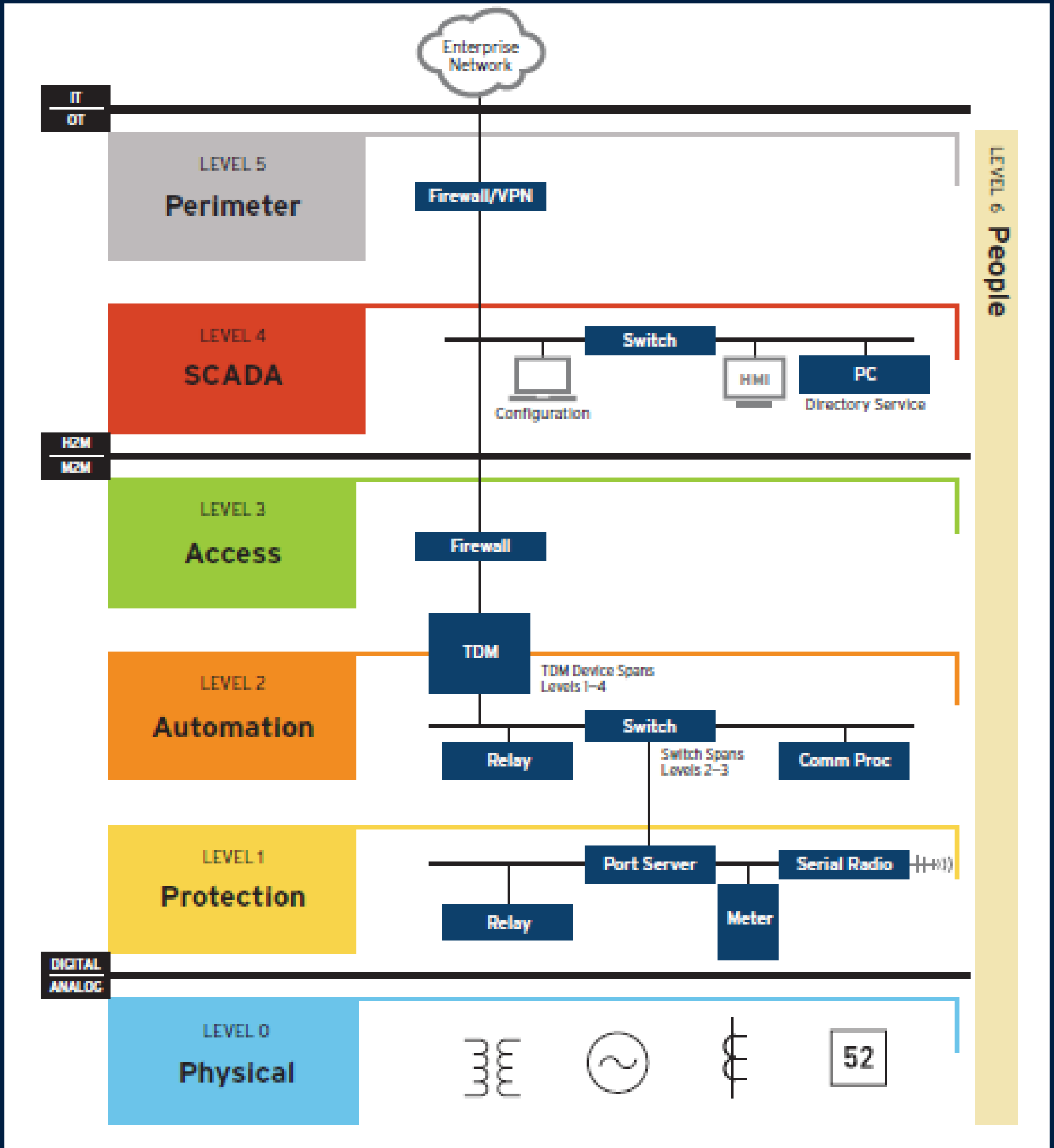
- Based on SDN standards
- Broad topology support
- Fast failover
- Application-focused circuits
- Greater cybersecurity
- Greater network efficiency

Static Traffic Engineering

Reduced Network Burden

- Only required traffic is allowed and only where needed
- Broadcast and multicast traffic do not unnecessarily burden end-devices or waste bandwidth
- Critical traffic paths are always kept open and ready

Traditional Gateway Architecture



OTSDN

Cybersecurity at Every Network Hop

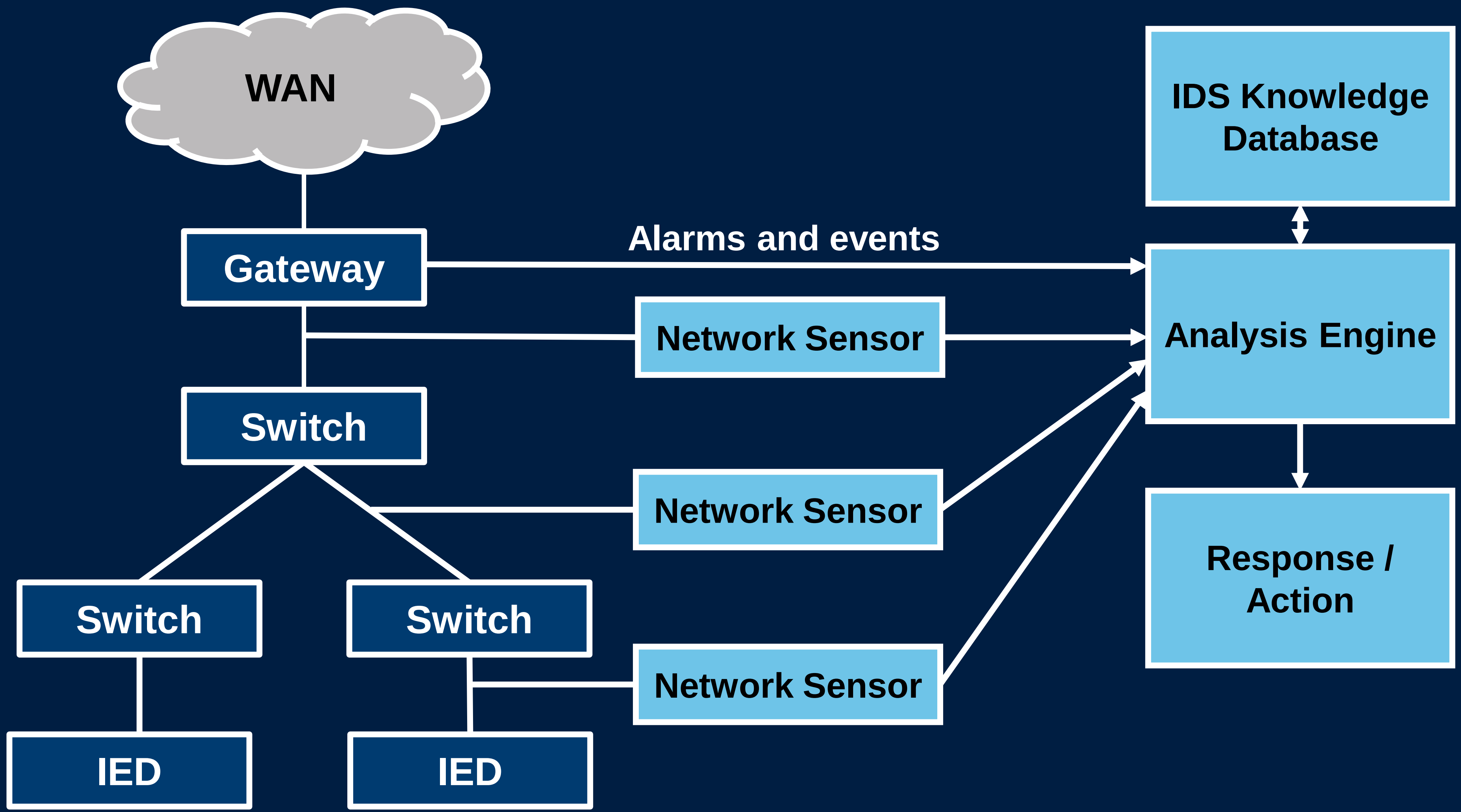
- Only allows required traffic and only where needed
  - No ARP cache poisoning
  - No broadcast storms
  - No BPDU attacks
- Hosts only see traffic for them and nothing else

No Traffic Injection From Unexpected Locations

- Locked down flows restrict what traffic is allowed on the network at every point
- Spoofing a device MAC / IP address will not work
- Packets that match allowed traffic cannot get onto the network unless they originate at the designed location
- Any attempt to spoof a device from an alternate location can be tracked and alarmed

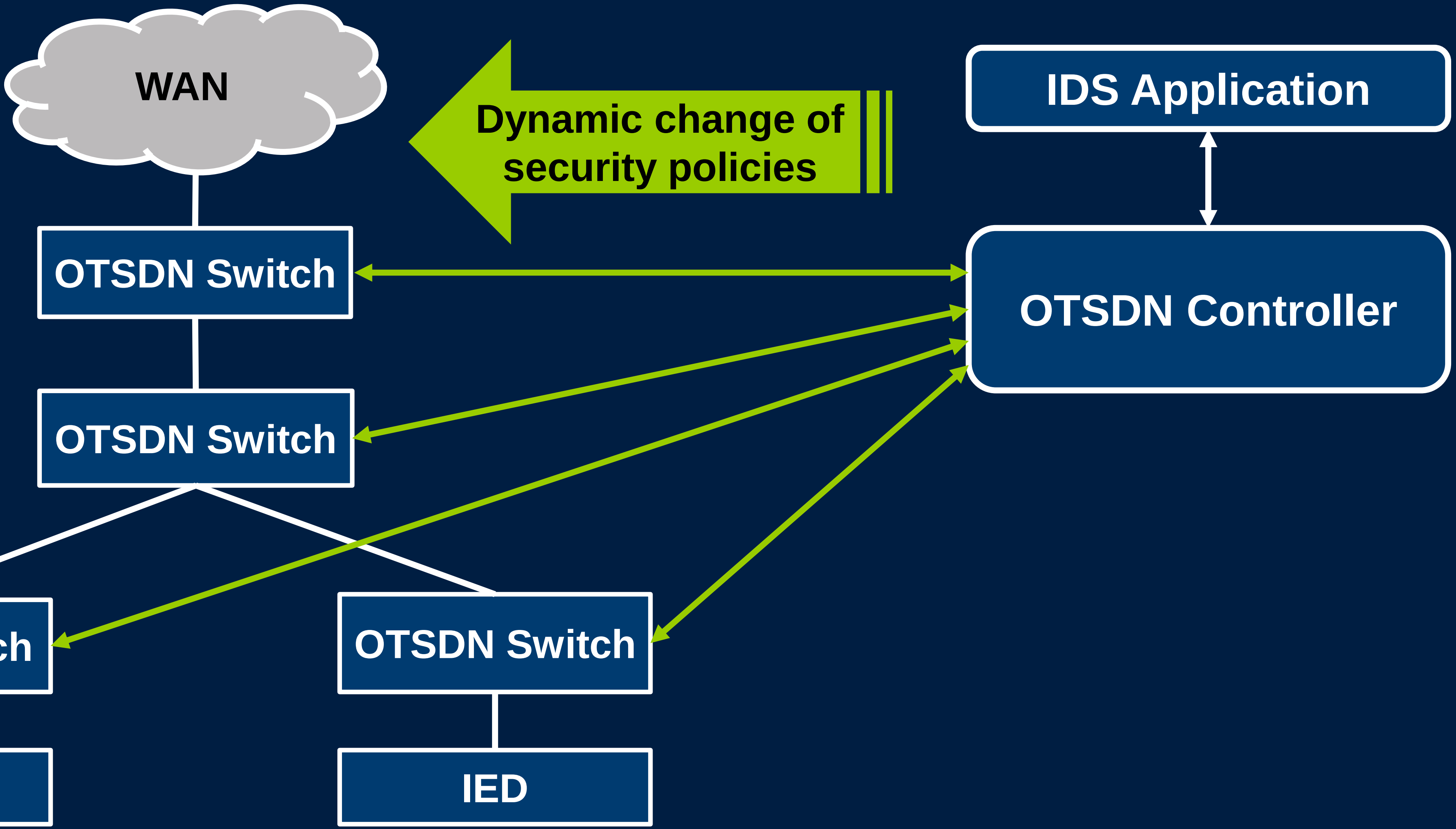
Traditional Intrusion Detection System (IDS)

External With Slow Action Response



SDN IDS

Integrated With Fast Dynamic Response



Targeted IDS

- All necessary traffic is engineered to go where it was designed to go
- Any unmatched traffic can be discarded or sent to an IDS
- The IDS only sees the traffic that was not already engineered
  - The IDS is less burdened by not watching all traffic
  - More scrutiny can be given to unwanted traffic

Targeted Deep Packet Inspection (DPI)

Focused DPI Processing Only Where Needed

- Individual flows from individual switches can easily be sent to a DPI processor
  - The DPI process can determine if the packets should be allowed on the network
  - If allowed, send it back to the OTSDN switch for further processing, otherwise drop / log
- Reduced burden on the DPI device by only processing the chosen stream of data

Conclusion

- OTSDN is standard technology, but it uses a different methodology
- Purpose-engineered networks allow deny-by-default cybersecurity at every hop in the network
- Easy DPI and IDS on selected flows
- Reduced network burden with enhanced security
- Controlled change management and network access

Questions?