

Network Configuration in the Real World Standards, Surprises and 'Creative' Implementations

Jens Vogler

About Me

- 2020 – Started at Init7 as Software Engineer
- 2022 – Finished my Bachelor at ZHAW with my Thesis called “Network Infrastructure automation with NetBox”
- Trying to actually implement automation ever since ...
- Picked up woodworking as a hobby

OSS & BSS

OSS - Operations Support System

Network Inventory

Network Operations



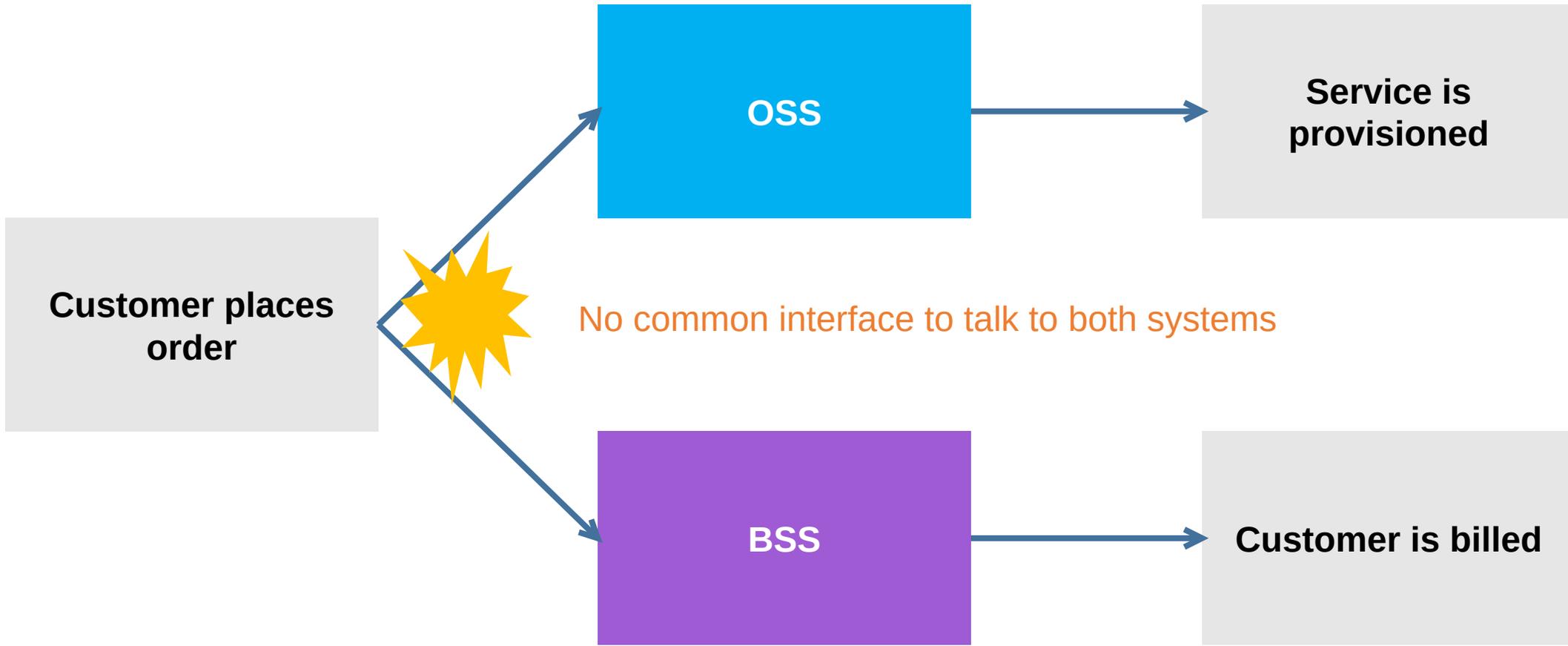
BSS - Business Support System

CRM

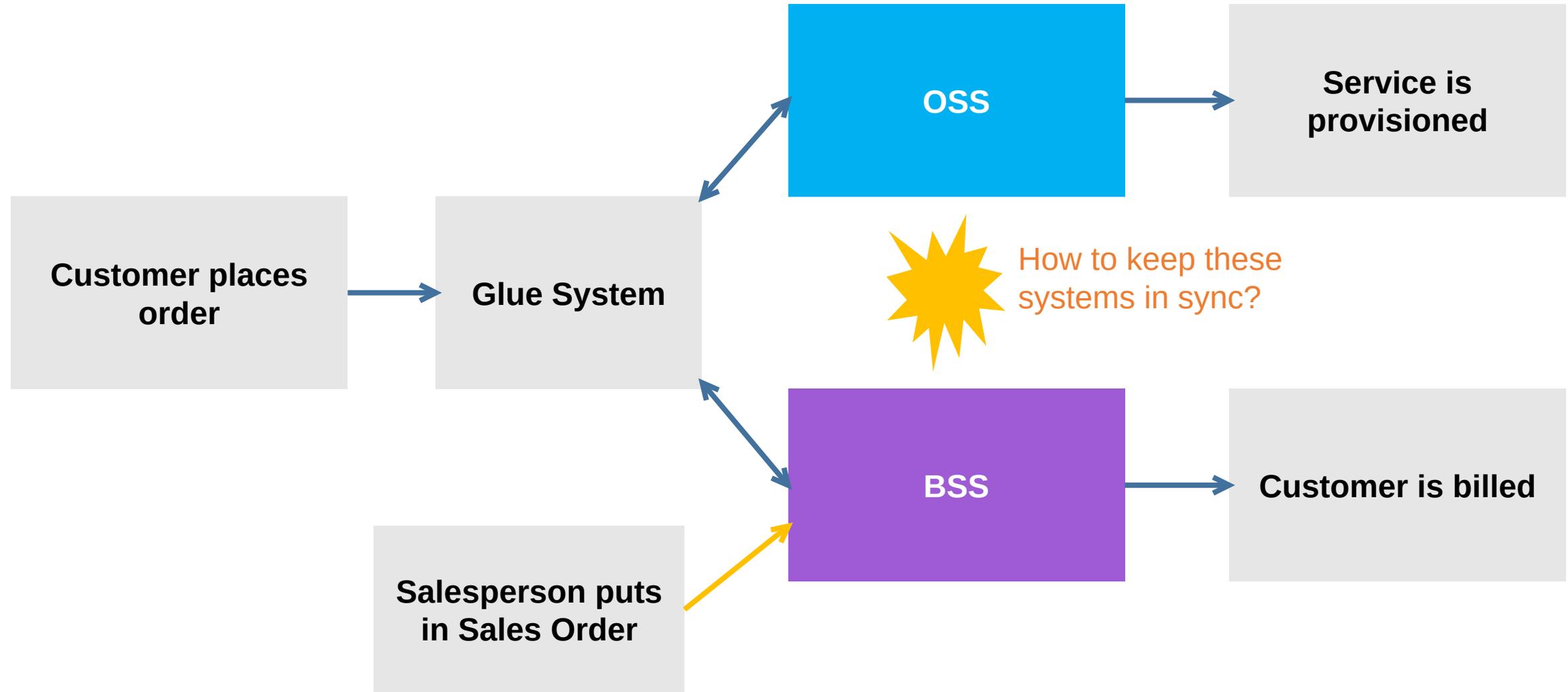
Billing



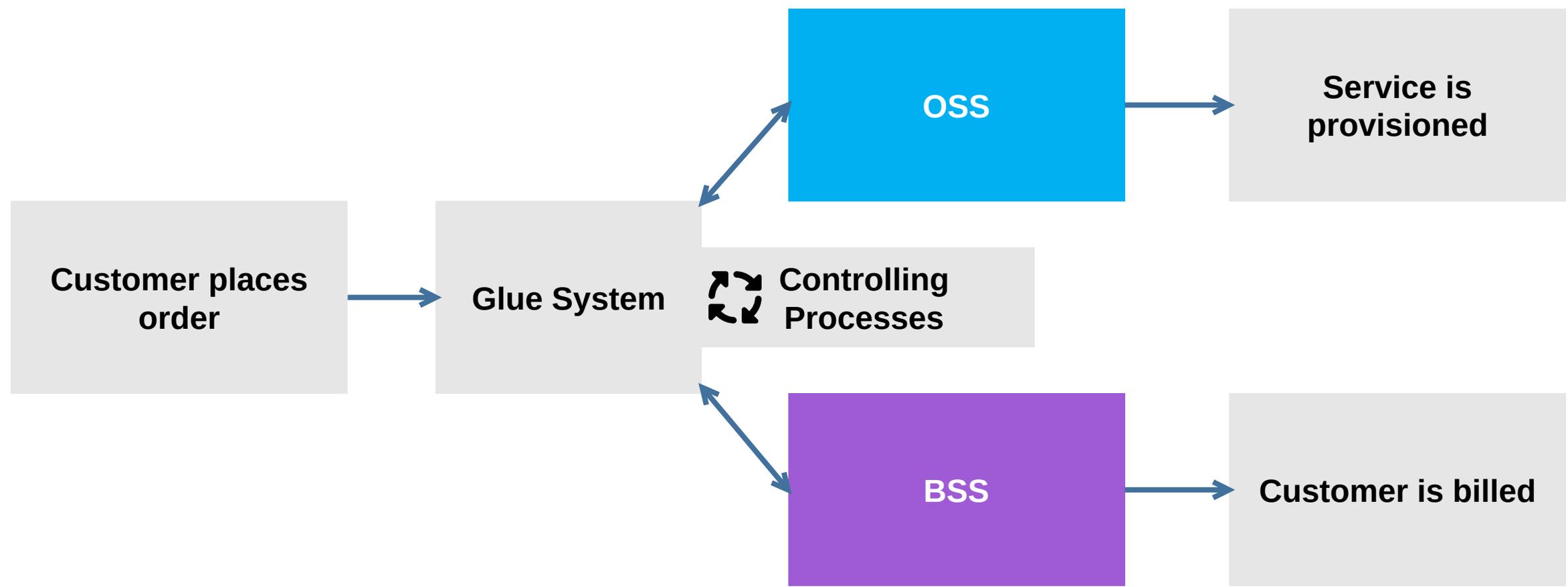
The Process



The Process

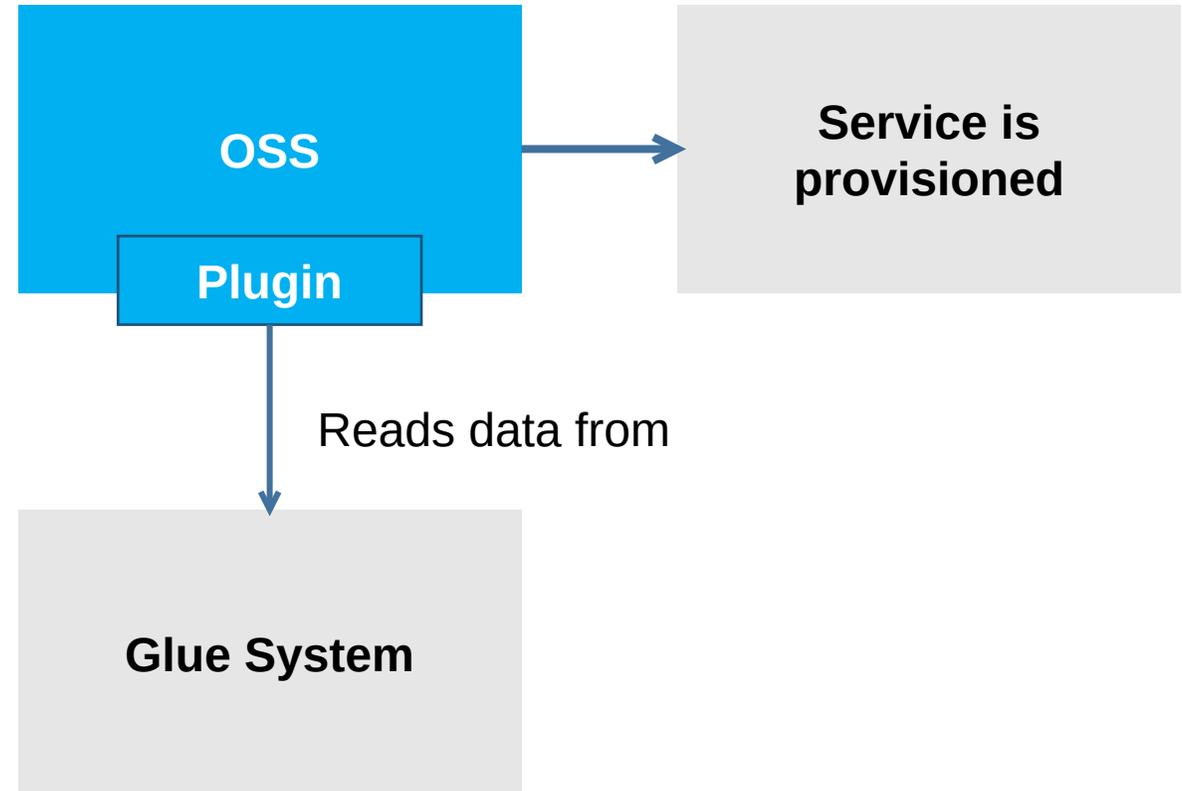


The Process



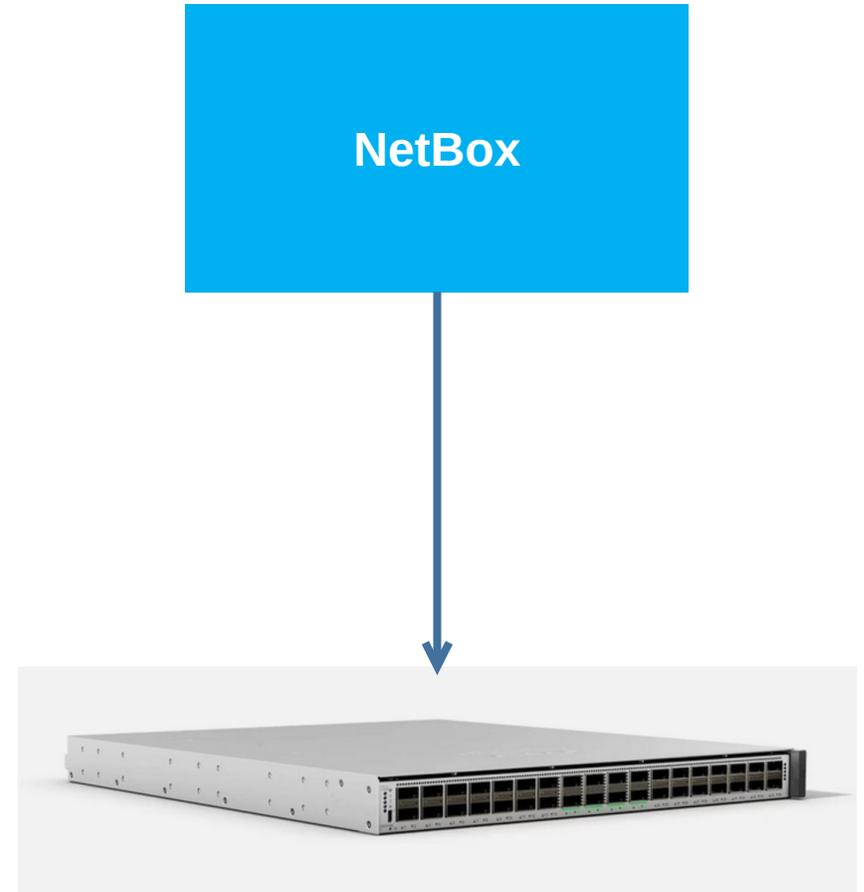
Service provisioning

- Do we have all the data we need?
 - Customer name on the interface description?



Getting the config onto the Device

- NETCONF!
 - RFC 4741 from 2006
 - Open standard and vendor agnostic
 - Supports preparing, validating and atomic commit of configuration
 - Supports replacing specific sections of configuration
 - Supplemented by YANG to get a complete schema of possible configuration



Getting the config onto the Device

- So it's easy right? Just write a template once for your datamodel
 - YANG Models defined by IETF are barely usable
 - OpenConfig tried to solve this, but vendor support is very limited
- Okay fine, so let's write vendor specific templates instead...





So what does NETCONF “Support” really mean?

```
1 interface TwentyFiveGigE1/0/42
2 description s1.480tst - 1/0/42
3 switchport access vlan 700
4 switchport mode access
5 switchport protected
6 switchport port-security maximum 5
7 switchport port-security
8 device-tracking attach-policy DT_UNTRUSTED
9 ip access-group IGMP in
10 ipv6 nd raguard
11 ipv6 dhcp-ldra interface-id s1.480tst_1/0/42
12 ipv6 dhcp guard
13 storm-control broadcast level pps 1k
14 storm-control multicast level pps 1k
15 storm-control unknown-unicast level pps 1k
16 storm-control action shutdown
17 no lldp transmit
18 no lldp receive
19 spanning-tree bpdupfilter enable
20 ip igmp max-groups 7
21 ip igmp filter 7
22 ip dhcp snooping vlan 700 information option format-type
    circuit-id string s1.480tst_1/0/42
```

```
1 <rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="181">
2   <edit-config>
3     <target>
4       <running/>
5     </target>
6   </edit-config>
7   <module xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-netconf">
8     <interface>
9       <twentyfiveGigE xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" nc:operation="replace">
10         <name>E1/0/42</name>
11         <description>s1.480tst - 1/0/42</description>
12         <switchport-config>
13           <switchport>
14             <access xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-switch">
15               <vlan>
16                 <vlan700/vlan>
17                   </vlan>
18                 </access>
19             </access>
20             <mode xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-switch">
21               </mode>
22             <port-security-conf xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-switch">
23               <port-security-config xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-switch">
24                 <max-protect>
25                   <max-addresses>
26                     <max-addresses5/>
27                   </max-addresses>
28                 </port-security>
29               </port-security-config>
30             </protected xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-switch">
31               </switchport>
32             </switchport-config>
33           </switchport>
34           <access-group>
35             <access>
36               <act1/>
37               <act1-name>IGMP</act1-name>
38             </act1>
39           </access-group>
40         </switchport>
41       </interface>
42     </module>
43     <dhcp xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-dhcp">
44       <interface>
45         <interface700/ld/>
46           <information>
47             <option>
48               <format-type>
49                 <string1.480tst_1/0/42/string/>
50               </format-type>
51             </option>
52           </information>
53         </interface>
54       </interface>
55     </dhcp>
56   </module>
57   </rpc>
58   <filter xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-igmp">
59     <filter2/filter>
60       <max-groups>
61         <count7/count>
62           </max-groups>
63         </filter>
64       </filter>
65     </filter>
66   </module>
67   <guard xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-dhcp">
68     </guard>
69   </module>
70   </rpc>
71   <logging>
72     <events>
73       <link-status/>
74     </events>
75   </logging>
76   <access-session>
77     <host-mode>multi-auth</host-mode>
78   </access-session>
79   <storm-control>
80     <action>
81       <broadcast/>
82       <broadcast>
83         <level>
84           <rising-threshold>
85             <rising-threshold0/>
86           </level>
87         </broadcast>
88       </action>
89     </storm-control>
90   </module>
91   <ospf xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-ospf">
92     <ospf-config>
93       <ospf-true/>
94     </ospf-config>
95   </module>
96   <server-location/>
97   </location/>
98   </filter>
99   </module>
100   <cts xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-cts">
101     <role-based>
102       <enforcement/>
103     </role-based>
104   </cts>
105   <lldp xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-lldp">
106     <receive/>
107     <transmit/>
108   </lldp>
109   <spanning-tree xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-spanning-tree">
110     <bpdupfilter/>
111   </spanning-tree>
112   <device-tracking xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-switch">
113     <attach-policy/>
114     <attach-policy>
115       <attach-policyDT_UNTRUSTED/>
116     </attach-policy>
117   </device-tracking>
118   </TwentyFiveGigE>
119 </interface>
120 </module>
121 </edit-config>
122 </rpc>
```

So what does NETCONF “Support” really mean?

```
1 interface TwentyFiveGigE1/0/42
2 description s1.480tst - 1/0/42
3 switchport access vlan 700
4 switchport mode access
5 switchport protected
6 switchport port-security maximum 5
7 switchport port-security
8 device-tracking attach-policy DT_UNTRUSTED
9 ip access-group IGMP in
10 ipv6 dhcp guard
11 storm-control action shutdown
12 no lldp transmit
13 no lldp receive
14 spanning-tree bpdudfilter enable
15 ip igmp max-groups 7
16 ip igmp filter 7
17 ip dhcp snooping vlan 700 information option format-type
    circuit-id string s1.480tst_1/0/42
```

So what does NETCONF “Support” really mean?

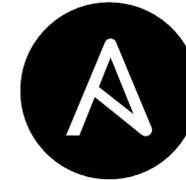
```
1 @@ -1,23 +1,17 @@
2 interface TwentyFiveGigE1/0/42
3   description s1.480tst - 1/0/42
4   switchport access vlan 700
5   switchport mode access
6   switchport protected
7   switchport port-security maximum 5
8   switchport port-security
9   device-tracking attach-policy DT_UNTRUSTED
10  ip access-group IGMP in
11 - ipv6 nd raguard
12 - ipv6 dhcp-ldra interface-id s1.480tst_1/0/42
13  ipv6 dhcp guard
14 - storm-control broadcast level pps 1k
15 - storm-control multicast level pps 1k
16 - storm-control unknown-unicast level pps 1k
17  storm-control action shutdown
18  no lldp transmit
19  no lldp receive
20  spanning-tree bpdupfilter enable
21  ip igmp max-groups 7
22  ip igmp filter 7
23  ip dhcp snooping vlan 700 information option format-type
   circuit-id string s1.480tst_1/0/42
24
25
```

Really?

```
1 <rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0"
2     message-id="urn:uuid:2abb4728-1f78-4f95-a724-b4aac2b11603">
3 <rpc-error>
4   <error-type>application</error-type>
5   <error-tag>invalid-value</error-tag>
6   <error-severity>error</error-severity>
7   <error-message xml:lang="en">inconsistent value: Device refused one or more commands</error-message>
8   <error-info>
9     <severity xmlns="http://cisco.com/yang/cisco-ia">error_cli</severity>
10    <detail xmlns="http://cisco.com/yang/cisco-ia">
11      <bad-cli>
12        <bad-command>no switchport mode access</bad-command>
13        <error-location>15</error-location>
14        <parser-response>Command rejected: Conflict with Port Security</parser-response>
15        <parser-context>no description
16          no switchport access vlan 700
17          no switchport port-security maximum 5
18          no switchport mode access
19        </parser-context>
20      </bad-cli>
21    </detail>
22  </error-info>
23 </rpc-error>
24 </rpc-reply>
```

Back to pushing CLI commands...

- Well established tools - Ansible
- Network Engineers often already have some training
- Applying configuration is non-atomic
- Replacing sections reliably is impossible



```
1 @@ -1,23 +1,19 @@
2 interface TwentyFiveGigE1/0/42
3 - description s1.480tst - 1/0/42
4 - switchport access vlan 700
5 - switchport mode access
6 - switchport protected
7 - switchport port-security maximum 5
8 + description Easy7 / s1.480tst - 1/0/42
9 + switchport private-vlan host-association 701 101
10 + switchport mode private-vlan host
11 + switchport port-security maximum 1
12 switchport port-security
13 + switchport port-security mac-address sticky
14 + switchport port-security violation restrict
15 device-tracking attach-policy DT_UNTRUSTED
16 - ip access-group IGMP in
17 + ip arp inspection limit rate 25
18 ipv6 nd raguard
19 - ipv6 dhcp-ldra interface-id s1.480tst_1/0/42
20 - ipv6 dhcp guard
21 storm-control broadcast level pps 1k
22 storm-control multicast level pps 1k
23 storm-control unknown-unicast level pps 1k
24 storm-control action shutdown
25 no lldp transmit
26 no lldp receive
27 spanning-tree bpdudfilter enable
28 - ip igmp max-groups 7
29 - ip igmp filter 7
30 - ip dhcp snooping vlan 700 information option format-type circuit-id string s1.480tst_1/0/42
31 + ip dhcp snooping vlan 701 information option format-type circuit-id string s1.480tst_1/0/42
```

Learnings & Takeaways

- Current generation software seems to catch up with NETCONF support – though verifying and testing is still necessary
 - Model based configuration system is key
- Tooling around NETCONF, RESTCONF & YANG has room for improvement
 - Cisco YANG Suite – Powerful but slow, glitchy and closed-source
 - libnetconf2, libyang – Low level
 - Pyang, ncclient – Probably the easiest for automation
- Single source of truth doesn't solve all problems
 - Escape hatches are often necessary to fix urgent issues
 - Attempting to represent reality through abstract data models will always contain gaps
 - Once synchronization is introduced, divergence is possible
- You'll always encounter legacy systems where workarounds are needed

Thank you!

Init7