Cisco APIC-EM

- The APIC-EM (Cisco Application Policy Infrastructure Controller Enterprise Module) is Cisco's SDN Controller for enterprise environments
- It is a Linux based server which can be clustered for redundancy
- It supports network programmability via northbound APIs
- It also has several built-in features

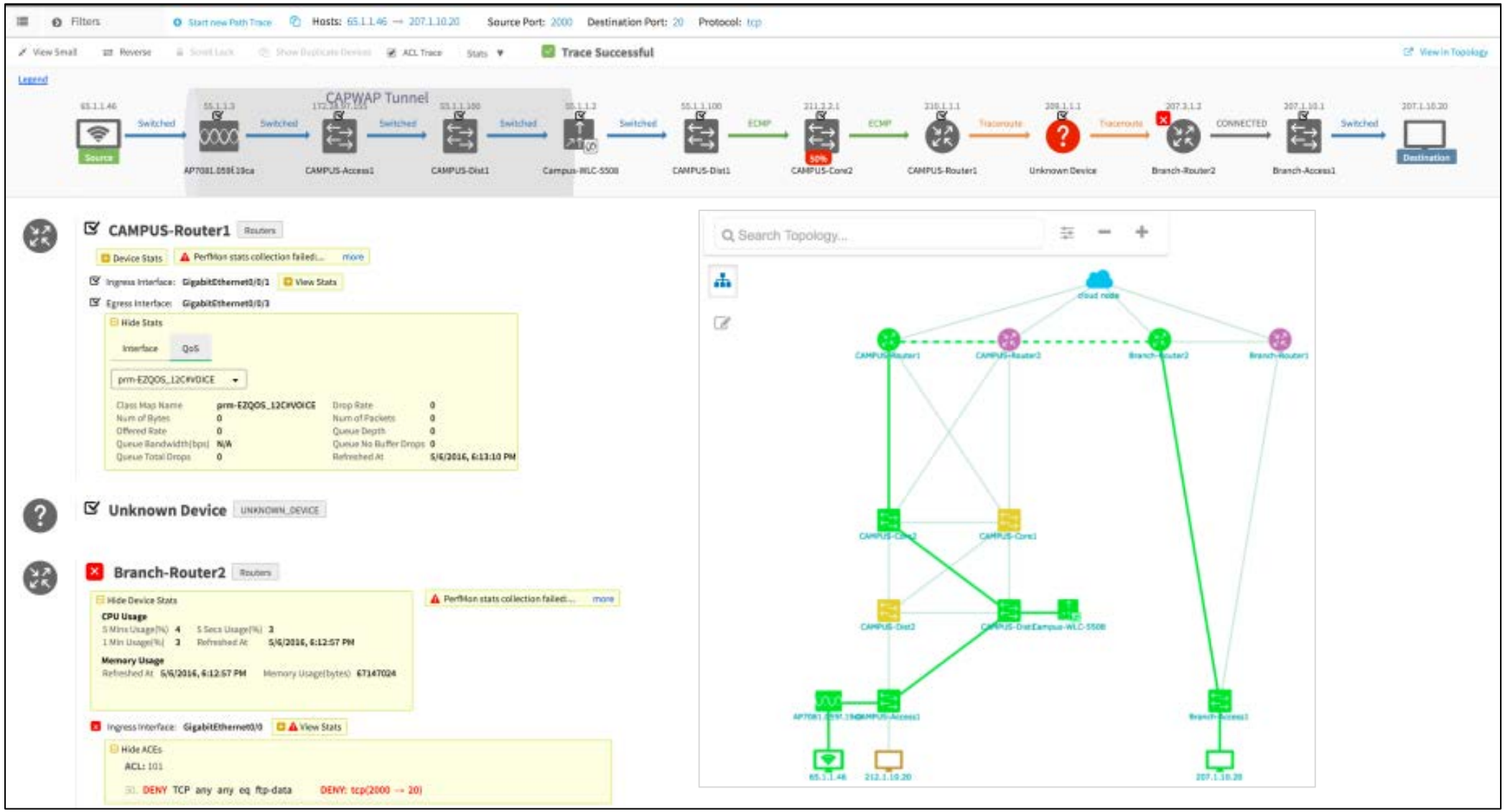
Cisco APIC-EM Features – Network Plug and Play

- Network Plug and Play allows routers, switches and wireless access points to be deployed in remote offices with zero touch configuration
- The device is physically installed in the remote office and connected to the network
- It discovers the APIC-EM through various methods including DHCP
- It then registers with and downloads its configuration from the APIC-EM
- This ensures consistent configuration of remote office devices with no need for a network engineer onsite

Cisco APIC-EM Features – Path Trace

- An engineer can use Path Trace to query APIC-EM for the path that traffic takes over the network
- This aids troubleshooting

Cisco APIC-EM Features – Path Trace



Cisco APIC-EM Features – IWAN

- IWAN (Intelligent WAN) is an SD-WAN feature which automates deployment and optimisation of network connections to branch offices
- It uses Cisco's DMVPN (Dynamic Multipoint VPN) feature to build secure full mesh connectivity between sites
- With Intelligent Path Control the WAN links are monitored and if primary link quality degrades a site can automatically fail over to a backup link
- AVC Application Visibility and Control provides QoS for particular traffic types

Cisco APIC-EM Features – EasyQoS

- EasyQoS provides end-to-end orchestration of QoS across the network
- The network engineer specifies what service is required by what applications in the GUI, with no need to configure CLI commands
- The APIC-EM then pushes the configuration to the network devices, complying with Cisco Validated Design best practice. Device specific CLI is handled under the hood
- This reduces total deployment time from months to minutes
- It can also integrate with Cisco collaboration servers to dynamically update QoS control as calls are set up and torn down

SDN Benefits

- Network infrastructure devices such as routers and firewalls have traditionally been configured on a box by box basis
- The administrator makes configuration changes individually on each device which is time consuming and can lead to non-conforming configurations and errors

SDN Benefits

- SDN enables automated centralised monitoring and configuration
- This allows you to provision changes quickly and in a standardised fashion
- Open APIs support fully customised applications
- Removing the required control plane intelligence allows the use of commoditised network infrastructure devices