airheads TECH TALK LIVE

aruba
a Hewlett Packard Enterprise company

Network Segmentation in the access

#ArubaAirheads

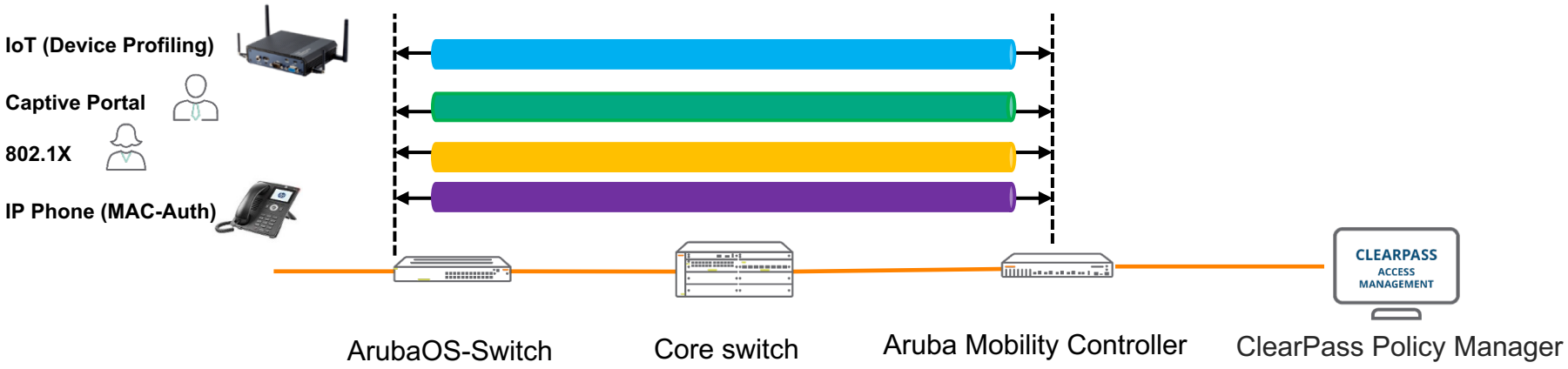
Agenda

- User Based Tunneling refresh
- User Based Tunneling 1.0
- User Based Tunneling 2.0
- Demonstration

User Based Tunneling Refresh

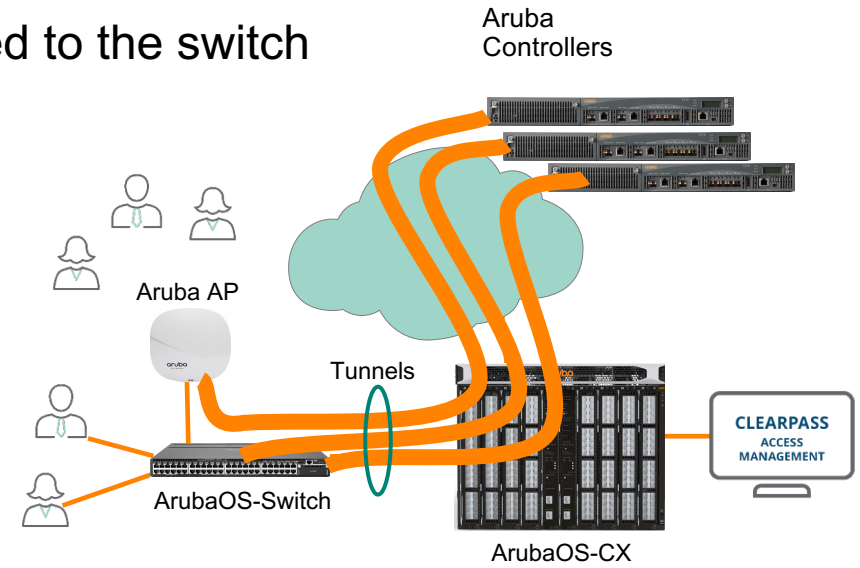
What is User Based Tunneling

- **UBT uses the concept of a colorless access port**
- **It doesn't matter what you connect to the port**
  - Roles and policies are assigned per device
- **Authentication takes place at the access port level**
  - Successful authentication enforces VLAN and ACL assignments
  - Successful authentication creates a per user tunnel to the Mobility Controller
  - Mobility Controller can enforce additional security



User Based Tunneling

- **Secured and flexible control of access layer**
  - With ClearPass or switch configuration, only traffic from a specific user/device role is sent to the Mobility Controller
  - Policies (e.g., QoS, ACL, rate-limit) can be enforced at Tunneled Node ports or at the controller
- **Access to Controller's applications**
  - Users can access Controller's applications such as stateful firewall and AppRF
- **Policy enforcement is achieved by local user roles or downloadable user roles**
  - Local user roles are configured on the switch
  - Downloadable user roles are configured on ClearPass and pushed to the switch
- **High availability and scalability**
  - Load balance to multiple controllers for high scalability
  - Stateful failover to standby mobility controller
- **Supported on 5400R/v3, 3810M, and 2930F/M**
- **Requires AOS 8.1 or later on the Mobility Controllers**



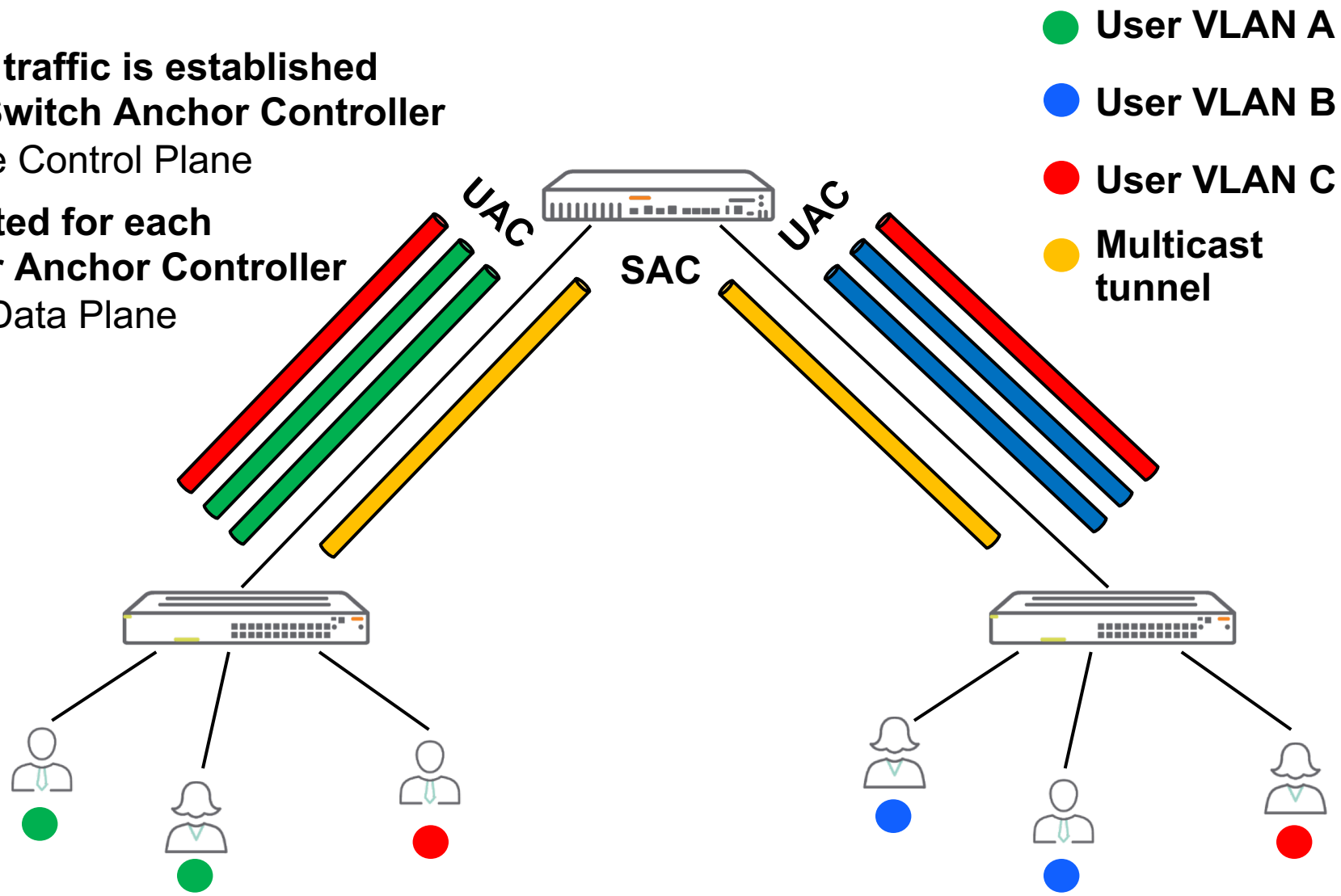
User Based Tunneling 1.0

In User Based Tunneling 1.0 deployments

- **The user VLAN is required to be configured on the access switch and on the Mobility Controller**
  - VLAN also has to be operational on the underlay network across the deployment
  - This does not scale and is difficult to implement in large enterprise grade network infrastructure
- **The root certificate for downloadable user roles has to be downloaded manually**
  - This makes zero touch deployment difficult
- **No license enforcement on the Mobility Controllers for User Based Tunneling**
- **Inefficient Multicast traffic handling (next slide)**

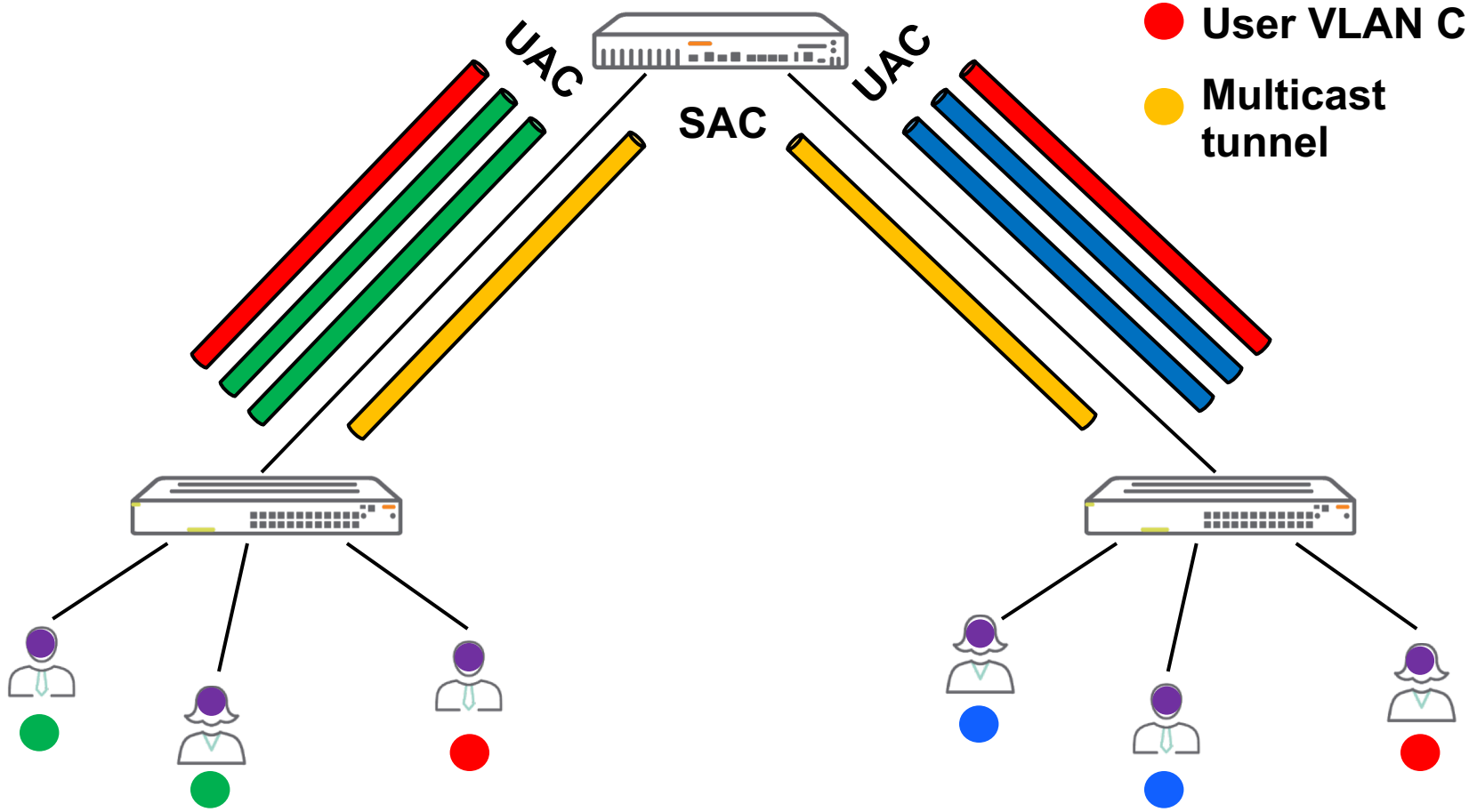
User Based Tunneling 1.0 multicast/broadcast behavior

- **Separate tunnel for Multicast traffic is established between access switch and Switch Anchor Controller**
  - Switch Anchor Controller is the Control Plane
- **User Based Tunnels are created for each client, connecting to the User Anchor Controller**
  - User Anchor Controller is the Data Plane



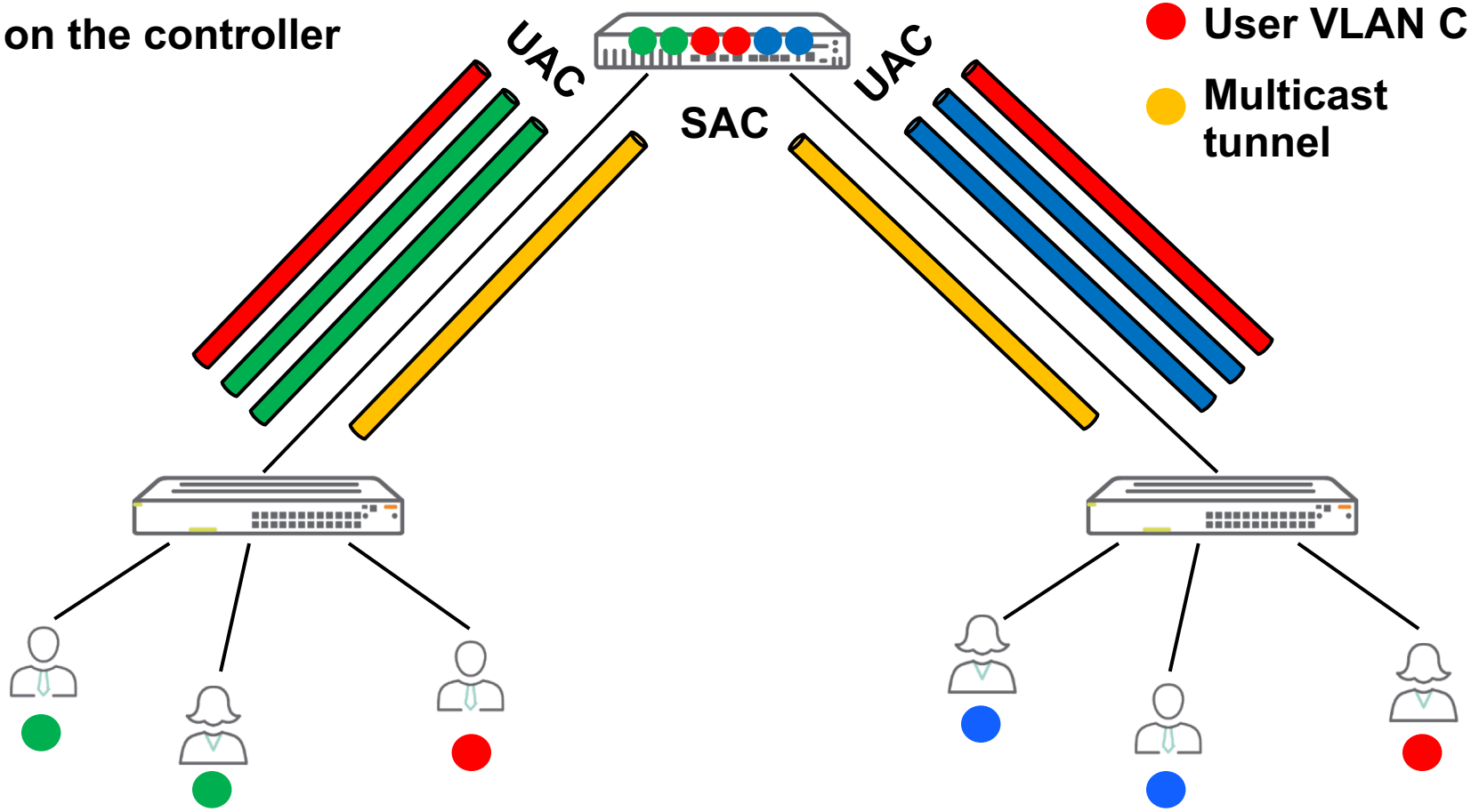
User Based Tunneling 1.0 multicast/broadcast behavior

- Unicast/Multicast/Broadcast traffic from client to controller always uses the UAC



User Based Tunneling 1.0 multicast/broadcast behavior

- All Multicast/Broadcast traffic from controller to client uses the multicast tunnel
- Multicast/Broadcast distribution is performed on the switch
- There is no control of MC/BC on the controller



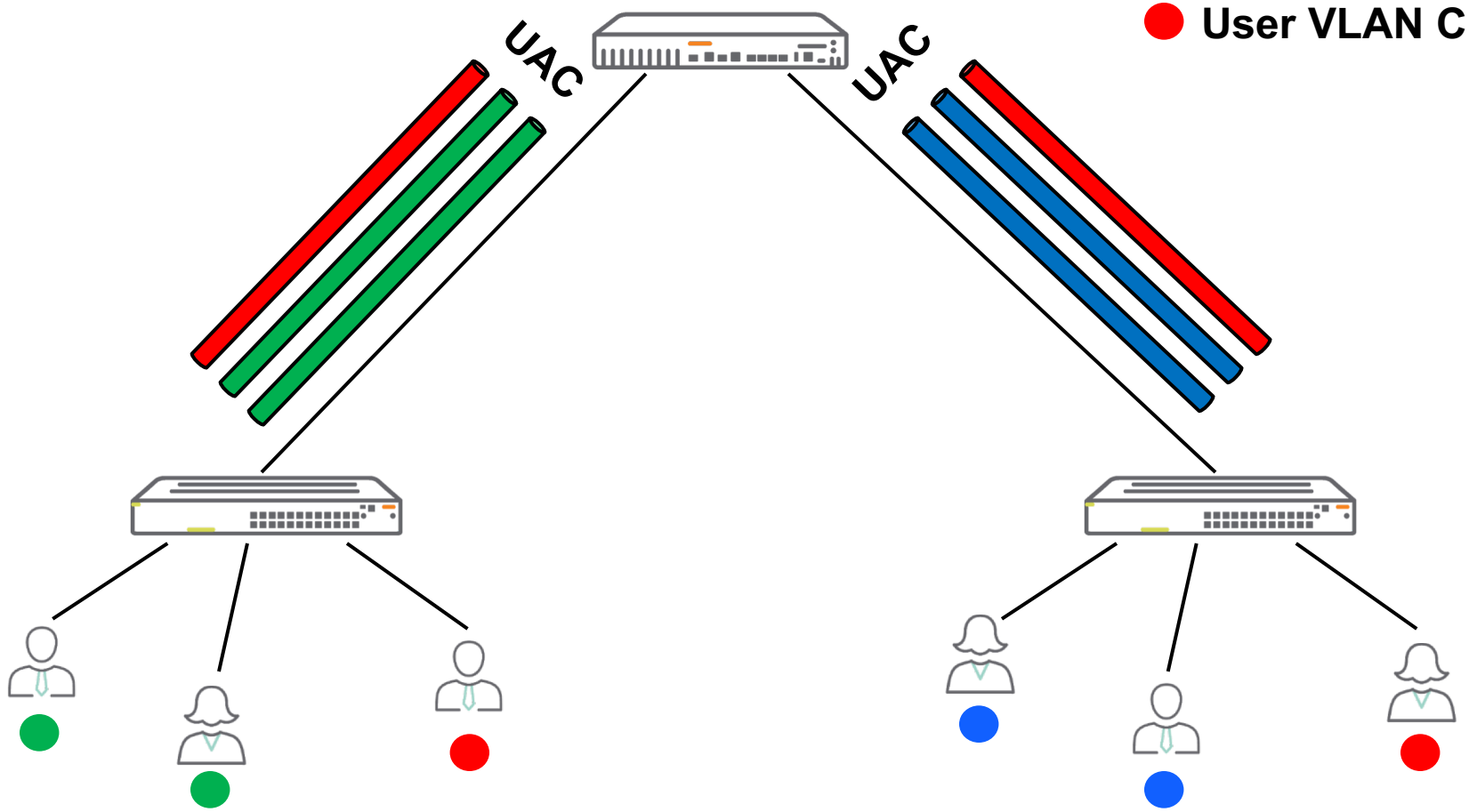
User Based Tunneling 2.0

In User Based Tunneling 2.0 deployments

- **No more user VLAN requirement on the Mobility Controller and Access Switches**
  - The user VLAN is configured on the Mobility Controller in the role configuration
  - Huge simplification of the switch configuration
  - Switch is not aware of the user VLAN anymore, this is enforced on the Mobility Controller
  - Only requires a reserved VLAN for establishing the SAC tunnel (automatically created)
- **The root certificate for downloadable user roles is downloaded automatically**
  - Allows for zero touch deployment
- **License enforcement on the Mobility Controllers for User Based Tunneling**
  - Per Switch IP address: Access Point (AP), Policy Enforcement Firewall (PEF) and RFProtect (RFP) license
  - Mobility Controller limits are also enforced
    - If a MC supports 32 AP's, number of switches **AND** AP's cannot exceed 32
  - License enforcement is with UBT 1.0 and 2.0. Enforcement is done by the Mobility Controller running software release 8.4
- **More controlled Multicast traffic handling (next slide)**

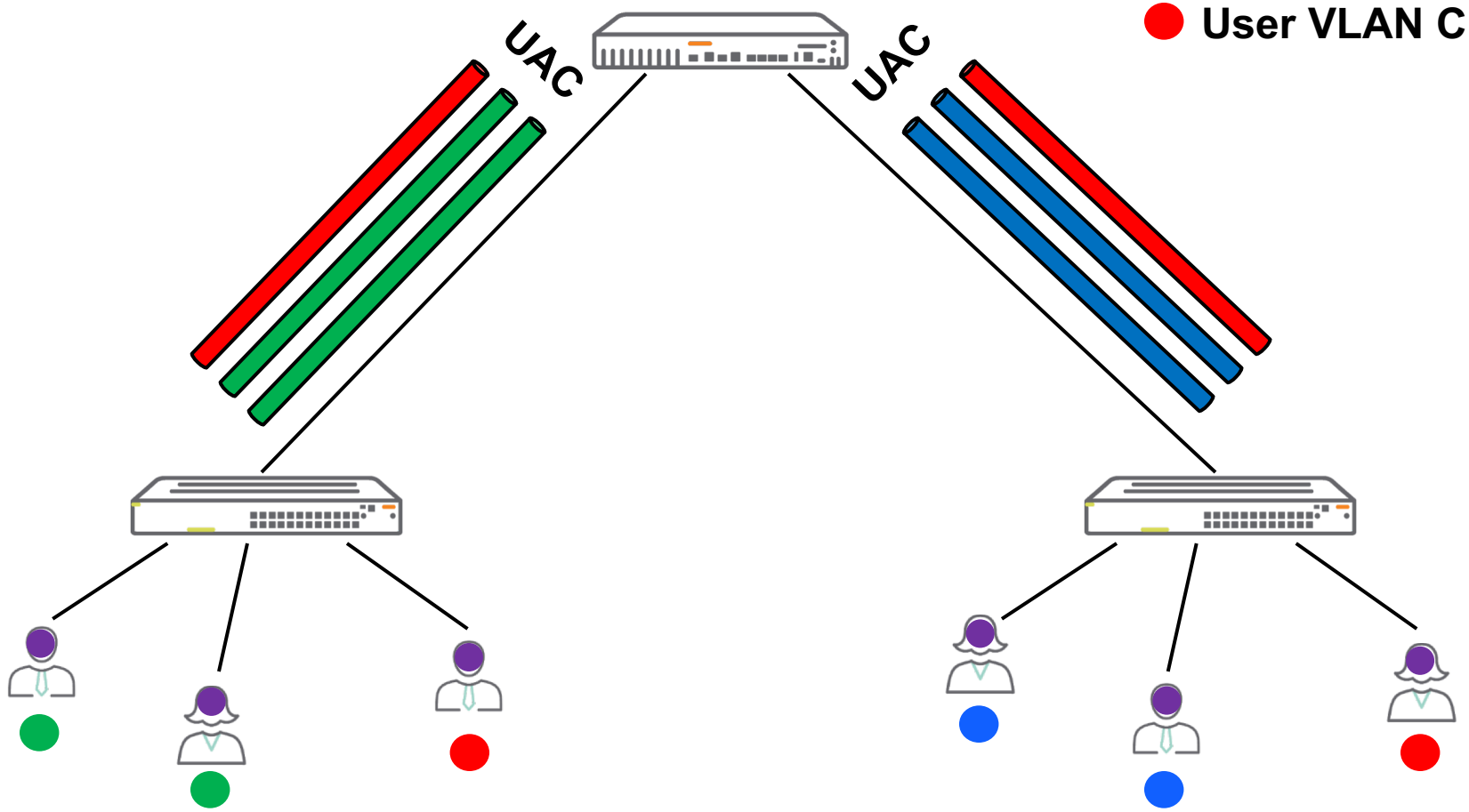
User Based Tunneling 2.0 multicast/broadcast behavior

- No separate tunnel for Multicast traffic, there are only User Based Tunnels



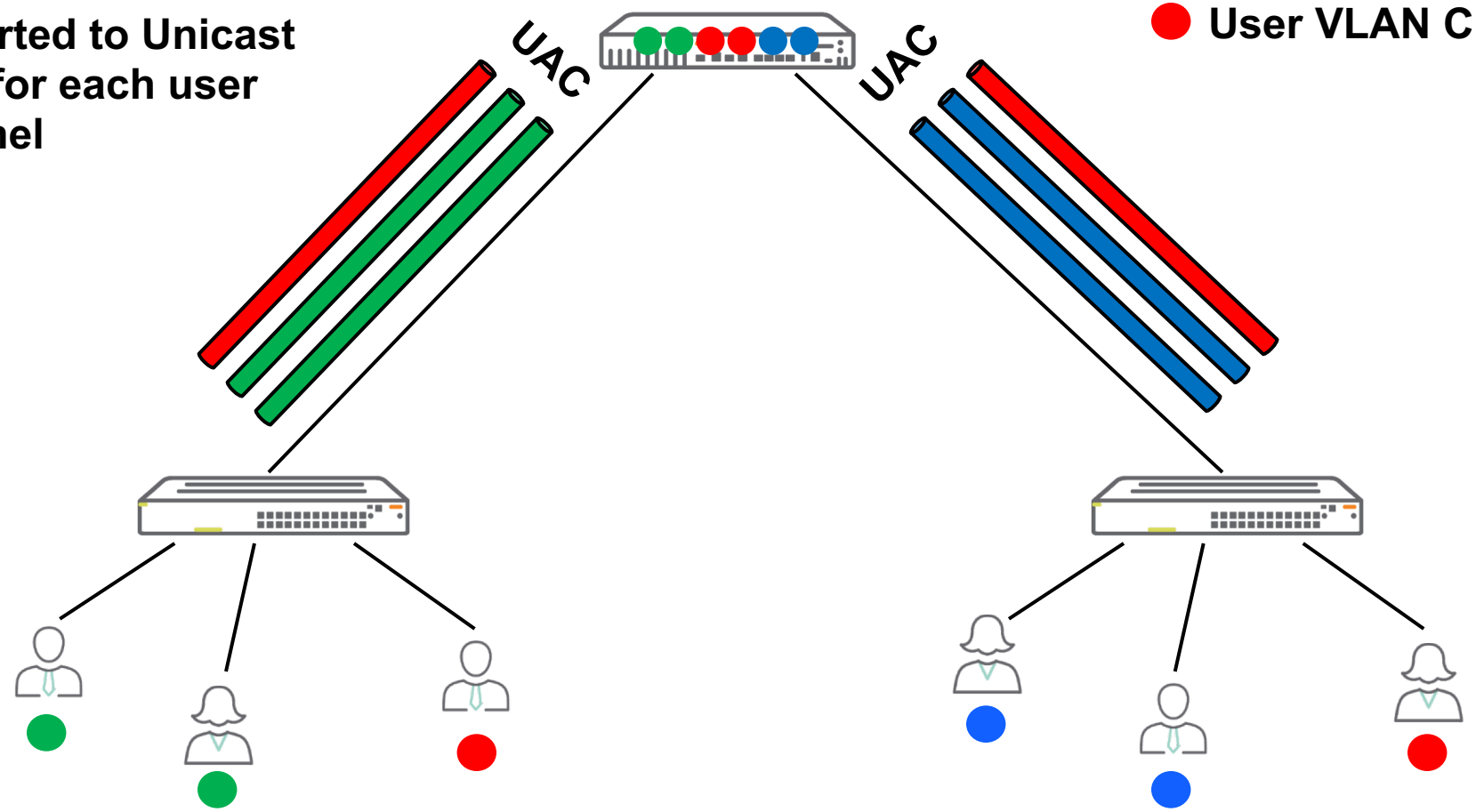
User Based Tunneling 2.0 multicast/broadcast behavior

- Unicast/Multicast/Broadcast traffic from client to controller always uses the UAC

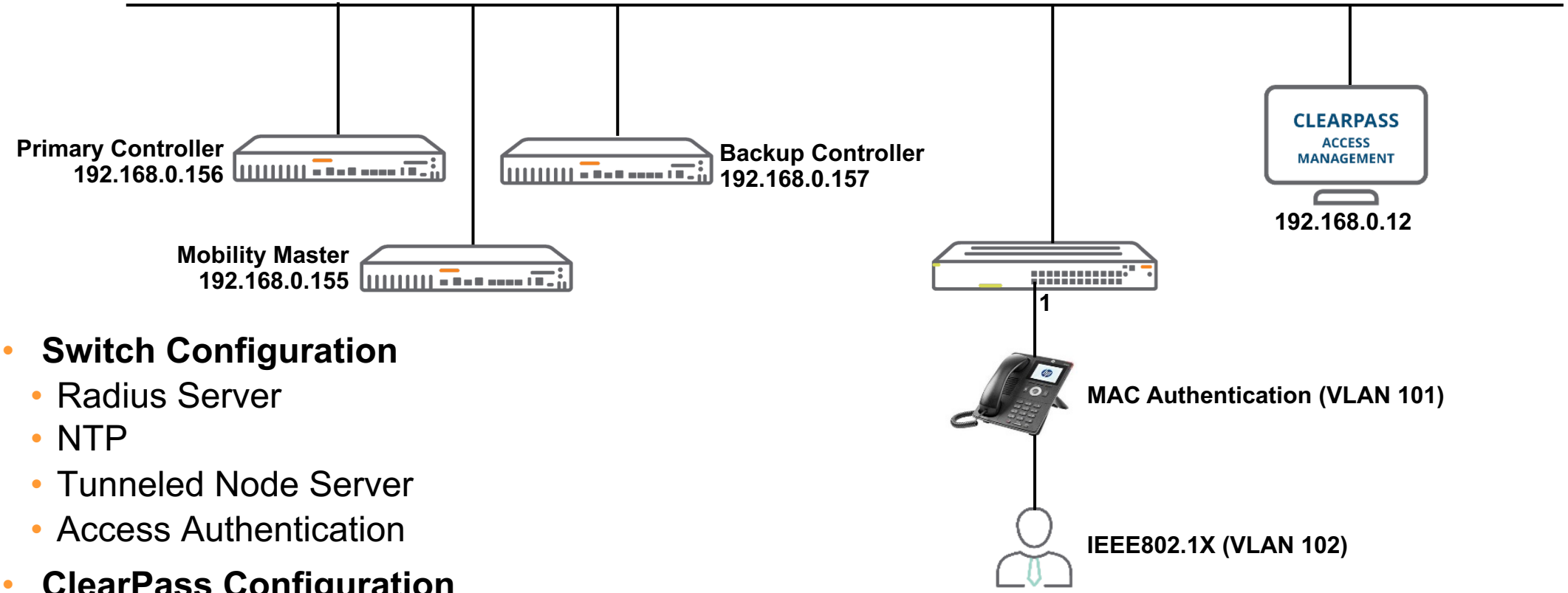


User Based Tunneling 2.0 multicast/broadcast behavior

- The Mobility Controller performs head end replication
- Multicast/Broadcast control is on the Mobility Controller
- Multicast/Broadcast is converted to Unicast packet and sent individually for each user through the User Based Tunnel



Demonstration



- **Switch Configuration**
  - Radius Server
  - NTP
  - Tunneled Node Server
  - Access Authentication
- **ClearPass Configuration**
  - Device (RAS client), enforcement profile, enforcement policy and service for MAC Auth and 802.1X
- **Mobility Controller**
  - VLAN interfaces (with IP configuration and inside NAT)
  - Roles and policies for MAC Authentication and 802.1X)

aruba
a Hewlett Packard
Enterprise company

airheads

TECH TALK LIVE