Dynamic Segmentation Enhancements

Justin Noonan

Technical Marketing Engineer

UBT Enhancements

Overview – User-Based Tunneling Enhancements

UBT Fallback Role

- Utilizes a “fallback” local role on the switch in the case of unreachability to a gateway or cluster (zone)
- Provides alternate connectivity to tunneled clients
- Only one command needed to enable on interface
- Supported on Aruba CX 4100i, 6200, 6300, 6400 platforms

UBT MultiZone – Same VRF

- Users can tunnel to a separate Gateway or Cluster (zone) within the same VRF
- Eliminates the need to create separate VRFs for additional zones
- Supported on Aruba CX 6300, 6400 platforms

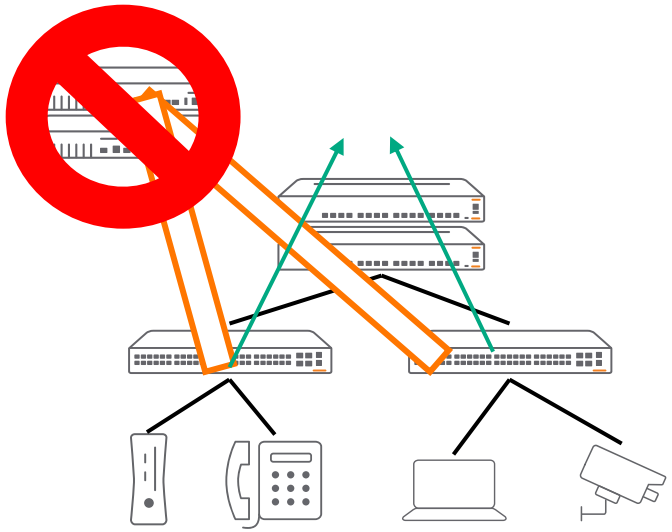
User-Based Tunneling Fallback Role

Understanding the UBT Fallback Role

- Maximum number of UBT Fallback Roles per port = 1
- Maximum number of user roles per system (switch or stack) = 1017 (6400/6300), 64 (6200), 32 (4100i)

Caveats

- In the UBT fallback role, the user VLAN cannot be part of the switch uplink to the gateway when using the VLAN Extend (UBT 1.0) mode



Configuring the UBT Fallback Role

Make sure user role is configured first

```
port-access role ubt-fallback
    vlan access 10
```

New command to allow the fallback role to be configured at the interface level

```
Switch(config)# interface 1/1/3
    no shutdown
    no routing
    vlan access 1
    port-access ubt-fallback-role ubt-fallback
    aaa authentication port-access client-limit 10
    aaa authentication port-access mac-auth
        enable
    exit
```

From the client table, the fallback role can be seen as applied when gateway or cluster has lost connectivity

```
Switch# show port-acc clients

Port Access Clients

Status Codes: d device-mode, c client-mode, m multi-domain

------------------------------------------------------------------------------------------------
  Port     MAC-Address       Onboarding     Status      Role                              Device Type
                             Method
------------------------------------------------------------------------------------------------
c 1/1/3    56:78:90:00:00:08 mac-auth       Success     ubt-fallback2, UBT-Fallback
```

UBT Fallback Role Application Flow

UBT Operational State	Apply UBT Fallback Role?
Down – UBT Zone Not Ready	Yes
Up – UBT Zone Ready	No
Down – Gateway Not Reachable	Yes
Up – Gateway Reachable	No
Down – UBT Profile Disabled	Yes
Up – UBT Profile Enabled	No
Down – Mgmt. Module or VSF Switchover	Yes

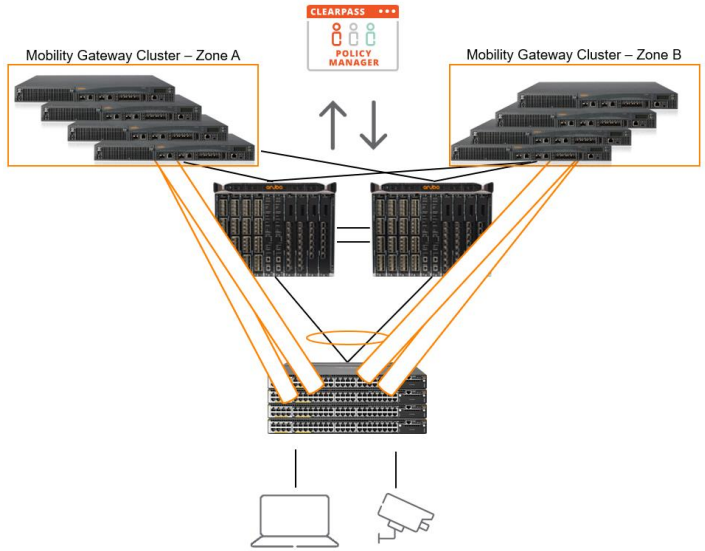
UBT MultiZone – Single VRF

Understanding UBT MultiZone – Single VRF

- Maximum number of zones supported on switch or stack is 8
- **New in AOS-CX 10.09** - Maximum number of zones per VRF is 8
- Supports 1017 total number of tunneled clients across different zones per system (switch or stack)

Caveats

- Overlapping user role VLANs should not be present across zones on the same switch - leads to cross-zone traffic (BUM)
- *Supported only for Aruba CX 6300 and 6400 Switch Series*



Demo

VNBT Enhancements

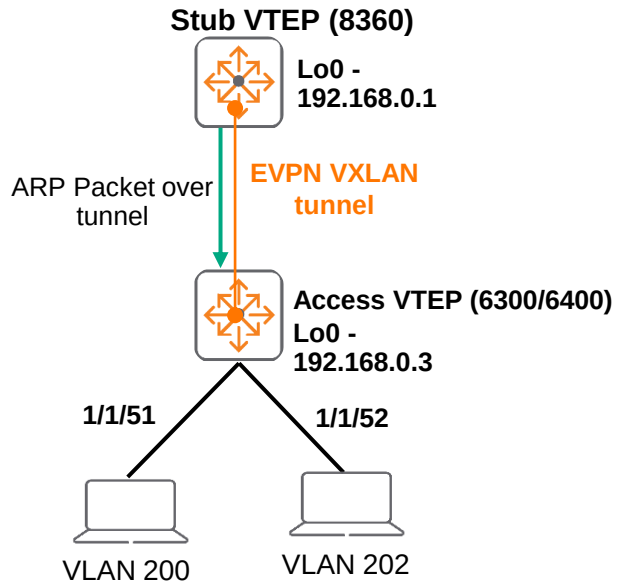
Reserved GBP ID for Infrastructure (Switch Generated) Traffic

- New Built-in role for any CPU-generated, infrastructure traffic packets (ARP, DHCP relay, Ping, etc) called “infra”
- Before AOS-CX 10.09, infrastructure traffic would be marked with the default role and an ID of 0
- “infra” has a default ID of 2 and can be changed by the user
- New command added

```
Switch(config)# gbp role infra
  <1-8191>  Set the infra role id (Default: 2)
  <cr>
```

- Example packet capture

```
> Frame 15502: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface \Device\NPF_{4BBCB234-BD58-4933-9074-763EA7C1D72C}, id 0
> Ethernet II, Src: ArubaaHe_b7:b5:00 (64:e8:81:b7:b5:00), Dst: ArubaaHe_b7:16:00 (64:e8:81:b7:16:00)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.2
> User Datagram Protocol, Src Port: 9022, Dst Port: 4789
v Virtual eXtensible Local Area Network
  v Flags: 0x8800, GBP Extension, VXLAN Network ID (VNI)
      1... .... .... .... = GBP Extension: Defined
      .... .... .0.. .... = Don't Learn: False
      .... 1... .... .... = VXLAN Network ID (VNI): True
      .... .... .... 0... = Policy Applied: False
      .000 .000 0.00 .000 = Reserved(R): 0x0000
    Group Policy ID: 2
    VXLAN Network Identifier (VNI): 200
    Reserved: 0
> Ethernet II, Src: 12:00:00:00:01:00 (12:00:00:00:01:00), Dst: aa:aa:aa:00:00:50 (aa:aa:aa:00:00:50)
> Address Resolution Protocol (reply)
```



Reserved GBP ID for Infrastructure - Caveats

Caveats

- All CPU generated control packets (CPU Tx to Port) must be transmitted from an SVI and not a routed port to be placed in the “infra” role
- All CPU re-forwarded packets will still get the “Default” role (DHCP Snooping v4/6, Captive Portal, ND Snooping, RA-Guard, IGMP, MLD, and mDNS)
- The same “infra” role to ID mapping must be consistent across the tunnel path
- Supported on Aruba CX 6300 and 6400 switch platforms

aruba
a Hewlett Packard Enterprise company

Thank you

justin.noonan@hpe.com