1 Table of Contents

Table of Contents

1 Table of Contents 1
1.1 Revision History 1
2 Microbranch with AOS10 2
2.1 Things you need 2
2.2 IP Addressing 3
3 Overlay Route Orchestrator 4
3.1 VPNC Routing Configuration 4
3.2 Testing Overlay Routes 5
3.3 Route Summarisation 7
3.4 Inter Branch Connectivity 8
3.5 BGP Routing Configuration 9
3.6 BGP Routing Testing 12
4 WAN Health Check 14

1.1 Revision History

DATE	VERSION	EDITOR	CHANGES
02 Mar 2024	0.1	Ariya Parsamanesh	Initial creation
07 Apr 2024	0.2	Ariya Parsamanesh	Added WAN health section

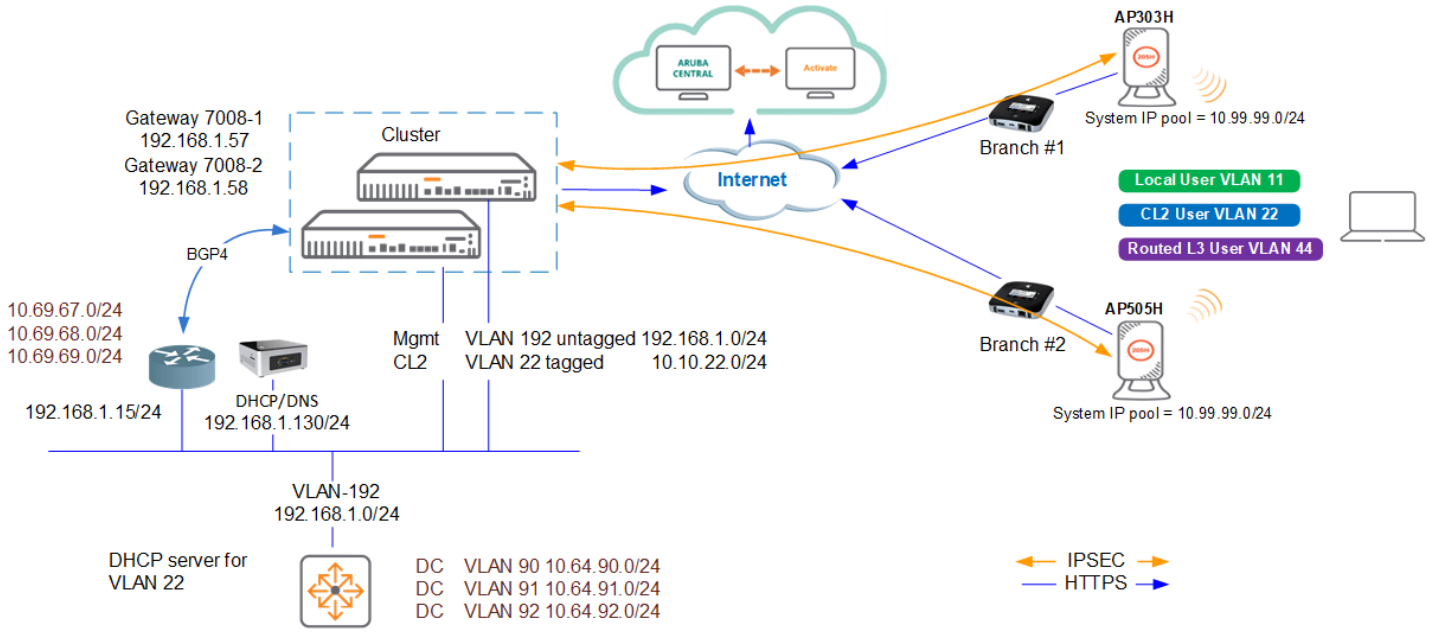
2 Microbranch with AOS10

AOS 10.x enables APs in remote sites to use most of the SD-WAN features and be managed by Aruba Central. For Micro Branch deployments, AOS 10.x currently supports deployment of a single AP as a Micro Branch AP in remote sites. The AOS 10.x enables these APs to form orchestrated IPsec tunnels to the Gateway cluster.

Microbranch APs support

- Orchestrated tunnels and routes (hub & spoke)
- VPNC Clustering
- PBR for local breakout (incl. 1st packet classification)
- Gateway Like WAN Monitoring
- Cloud Security Orchestration (Aruba AXIS, ZScaler, etc)

The topology that we'll be deploying is as shown below.



This is a 5x parts microbranch series. The aim here is to provide the starting point to put together a solution that include the AOS10 APs as microbranch, two VPNCs that are clustered along with Aruba Central to configure and monitor the solution.

- Part1 – Solution overview, basic configuration and testing of VPNC and AOS10 AP
- Part2 – Centralised L2 forwarding mode with authentication and policy-based routing
- Part3 – NATed Layer 3 forwarding mode with centralised authentication proxy
- Part4 – Routed Layer 3 forwarding mode with centralised authentication proxy
- Part5 – Overlay Route Orchestrator, route summarisation, BGP routes redistribution and monitoring

2.1 Things you need

- Two AOS10 APs running 10.4.0.2 or later
- AOS10 VPNCs running 10.4.0.2 or later
- Aruba Central account with eval licenses.
- LAN switch
- Operational Internet link

2.2 IP Addressing

This tables shows the IP addressing, subnets and routes that we'll be using.

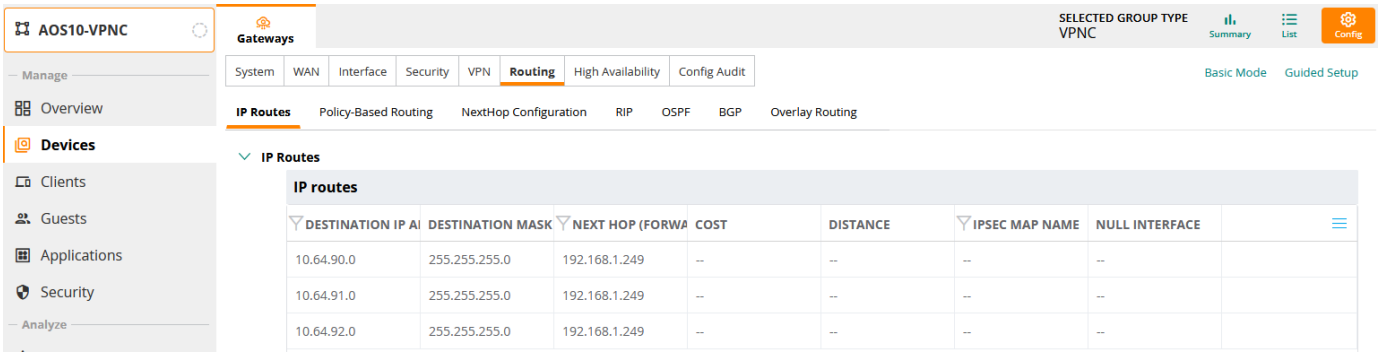
	System IP Pool	Local VLAN (SNAT)	Centralised L2	Routed L3 (shared Pool)	Configured Routes
	Used for Tunnel-inner-ip	VLAN11	VLAN22	VLAN44	
Microbranch1	10.99.99.7/32	10.11.11.1/24		10.44.44.81/28	
Microbranch2	10.99.99.4/32	10.11.11.1/24		10.44.44.17/28	
DC DHCP server			10.10.22.1/24		
VPNC 1	192.168.1.57/24				
VPNC 2	192.168.1.58/24				
VPNC – static routes					10.64.90.0/24 10.64.91.0/24 10.64.92.0/24
VPNC – BGP routes					10.69.67.0/24 10.69.68.0/24 10.69.69.0/24

3 Overlay Route Orchestrator

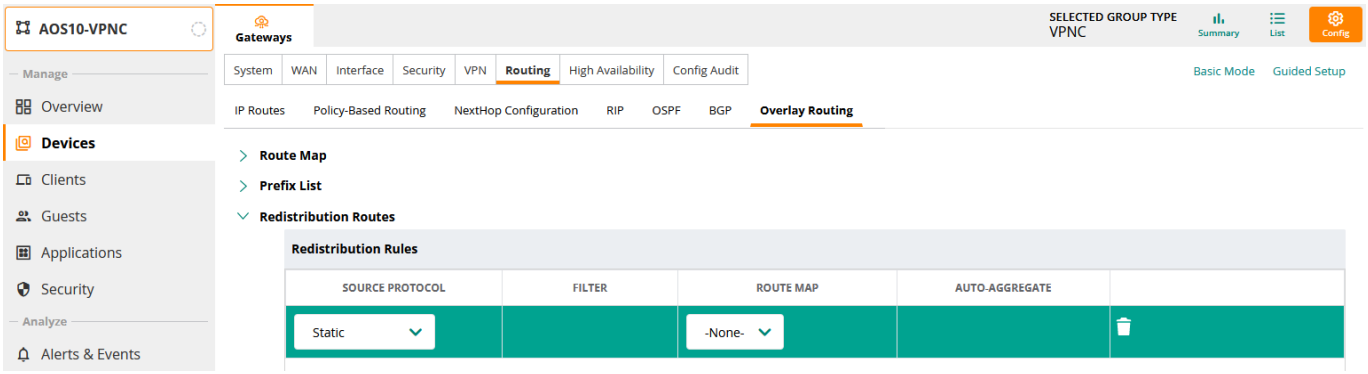
In this section we'll cover the routing configuration and Overlay Route Orchestrator (ORO) that will dynamically update VPNCs with Microbranch APs' L3 mode SSIDs subnets and update VPNCs' routes which have redistributed into Overlay to Microbranch APs.

3.1 VPNC Routing Configuration

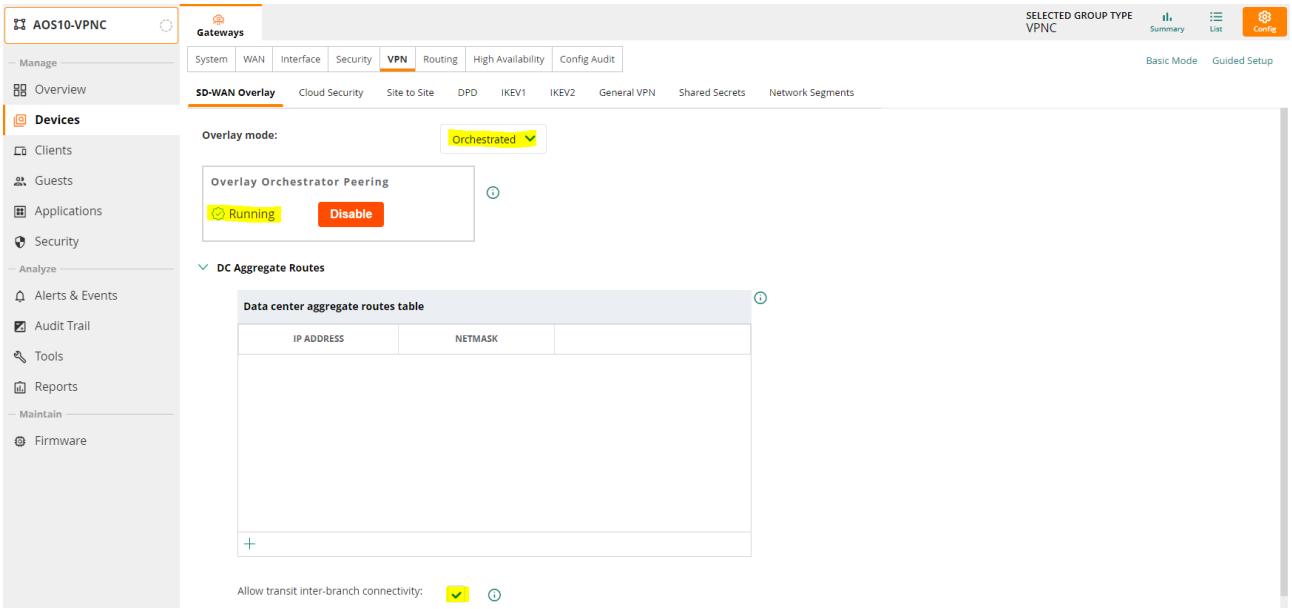
For simplicity we'll just add a few static routes at the group level pointing to the existing VLANs on our DC switch.



These routes are not visible in microbranch AP. Now we'll redistribute these static routes into overlay so that ORO is aware and it will then sent it to microbranch AP.

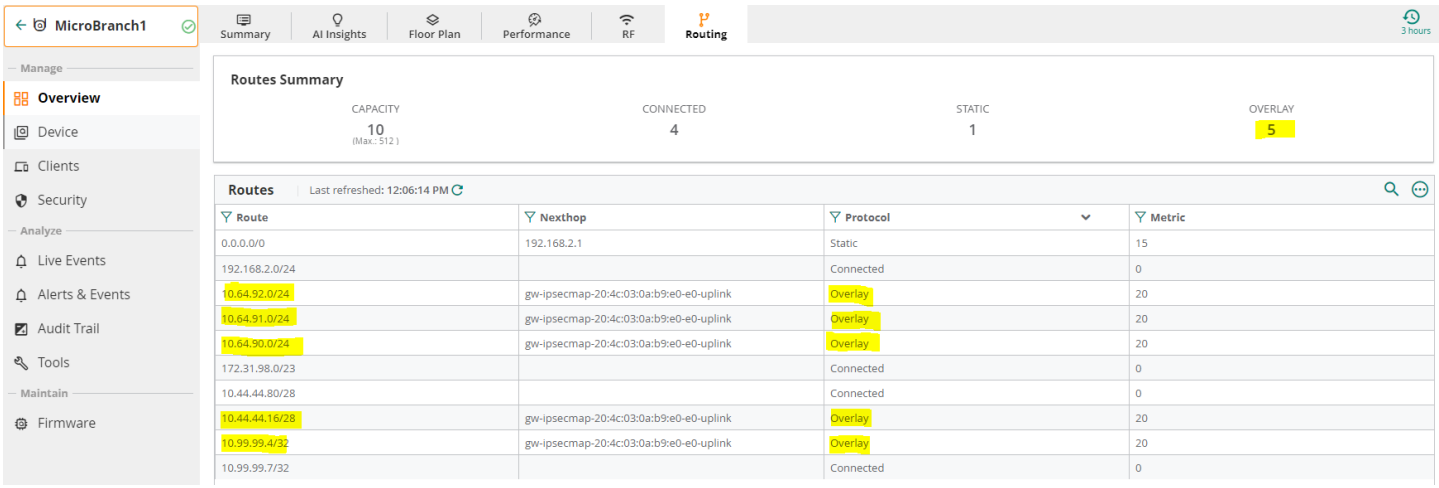


Now ensure you have enabled ORO, if not enable it. Here it is already enabled, and we are allowing transit branch connectivity.



3.2 Testing Overlay Routes

Now we'll see if the redistributed static routes into ORO are visible in the microbranch1 AP.

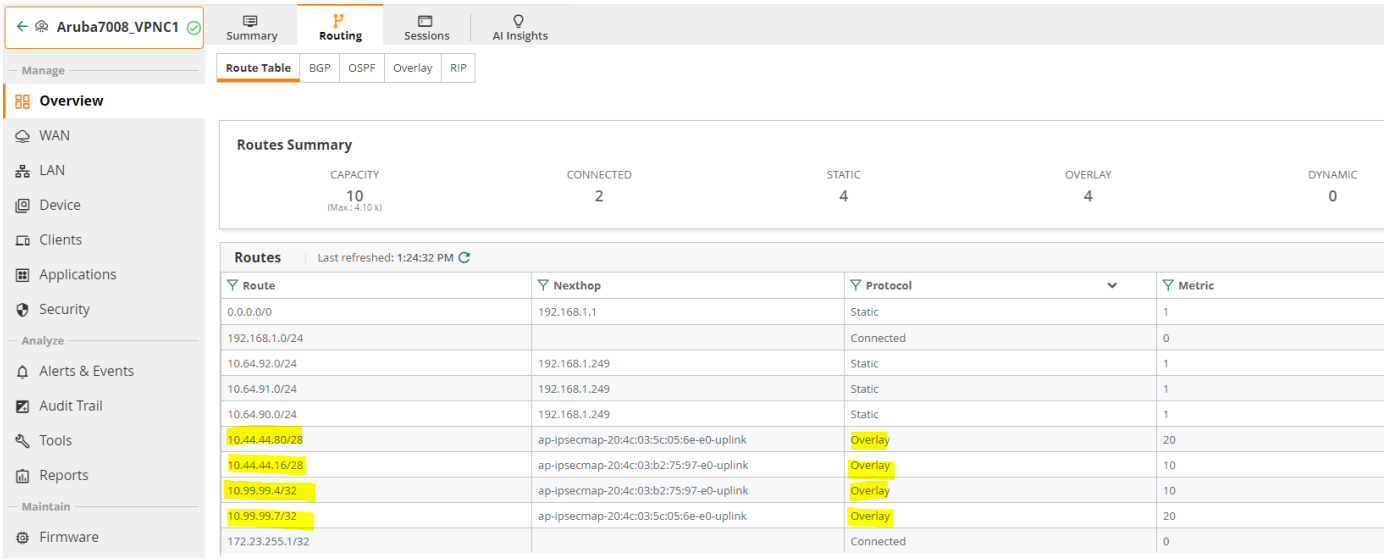


And here is the CLI view of it.

```
MicroBranch1# sh ip route
default via 192.168.2.1 dev br0.4092  metric 15
8.8.8.8 via 192.168.2.1 dev br0.4092
10.44.44.16/28 dev tsgw  src 10.99.99.7
10.44.44.80/28 dev br0.44  src 10.44.44.81
10.64.90.0/24 dev tsgw  src 10.99.99.7
10.64.91.0/24 dev tsgw  src 10.99.99.7
10.64.92.0/24 dev tsgw  src 10.99.99.7
10.99.99.4 dev tsgw  src 10.99.99.7
10.99.99.7 dev tun0
13.239.61.151 via 192.168.2.1 dev br0.4092
169.254.0.0/16 dev br0  src 169.254.1.1
172.31.98.0/23 dev br0.3333  src 172.31.98.1
192.168.1.57 dev tun0
192.168.2.0/24 dev br0.4092  src 192.168.2.50
194.223.11.109 via 192.168.2.1 dev br0.4092  metric -3

MicroBranch1#
```

```
MicroBranch2# sh ip route
default via 10.224.254.129 dev br0.4092  metric 15
3.104.166.215 via 10.224.254.129 dev br0.4092
8.8.8.8 via 10.224.254.129 dev br0.4092
10.44.44.16/28 dev br0.44  src 10.44.44.17
10.44.44.80/28 dev tsgw  src 10.99.99.4
10.64.90.0/24 dev tsgw  src 10.99.99.4
10.64.91.0/24 dev tsgw  src 10.99.99.4
10.64.92.0/24 dev tsgw  src 10.99.99.4
10.99.99.4 dev tun0
10.99.99.7 dev tsgw  src 10.99.99.4
10.224.254.128/25 dev br0.4092  src 10.224.254.157
169.254.0.0/16 dev br0  src 169.254.1.1
172.31.98.0/23 dev br0.3333  src 172.31.98.1
192.168.1.57 dev tun0
194.223.11.109 via 10.224.254.129 dev br0.4092  metric -3

MicroBranch2#
```

And finally, here is the routing table on VPNC1



Note that VPNC1 is seeing VLAN44 because its forwarding mode is RL3, these routes are being learnt and advertised by the Overlay Agent Protocol (OAP) to automatically build the SD-WAN overlay topology. This is the same mechanism that Aruba gateways/VPNCs use.

Here are some useful RL3 and OAP CLI commands for the microbranch gateways.

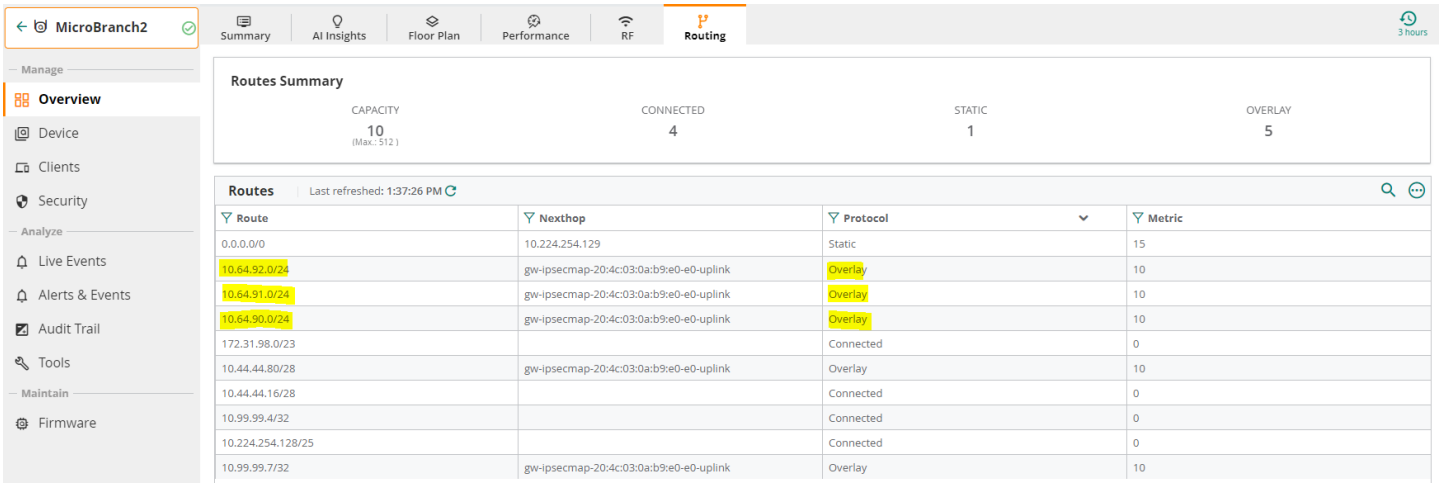
```
MicroBranch2# sh l3d oap

OAP Status
Admin State:                UP
Oper State:                 UP
Master:                     127.0.0.1:50050
Channel state:              CONNECTED
Serial:                     CNK6KSM03Q
MAC:                        20:4c:03:b2:75:97
Site ID (Channel):          20:4c:03:b2:75:97 (20:4c:03:b2:75:97)
Tenant ID (Channel):         ()
Tenant ID:
Tunnel Interface:           tsgw
Channel UP since:           2024-03-10 09:13:40.413
Channel Down count:         0
Learnt Routes:              3
 IPv4 checksum:             0x4bd7bfbb915e4265/3, Inst_1.2.POD_TABLE.1.1.0
Advertised Routes:          2
 IPv4 checksum:             0x83268f2ecf361585/2
Tunnels:                    3
RTB Gen ID:                 1707191867437060
PCM Gen ID IPv4 routes:     1709857414473267
Graceful Restart timer:     86400 seconds
Num of Create Channel:             1
Num of SyncReq Sent:               157
Num of SyncRep Received:           156
Num of SyncReq since last SyncRep Received:         0
Last SyncReq Sent:          2024-03-10 11:51:02.414
Last SyncRep Received:      2024-03-10 11:51:02.947
Num of FullSyncReq Sent:           0
Num of FullSyncReq Received:       1
Last RX: 2024-03-10 11:51:02.946, RX process: 2024-03-10 11:51:02.947 QSz: 0 MaxQSz: 2
Last TX: 2024-03-10 11:51:02.414, queue: 0
Peak Routes IPv4:           3 at 2024-03-10 09:15:44.239
Peak Tunnels:               3 at 2024-03-10 09:15:03.647

MicroBranch2#
```

```
MicroBranch2# sh l3d oap tunnels
```

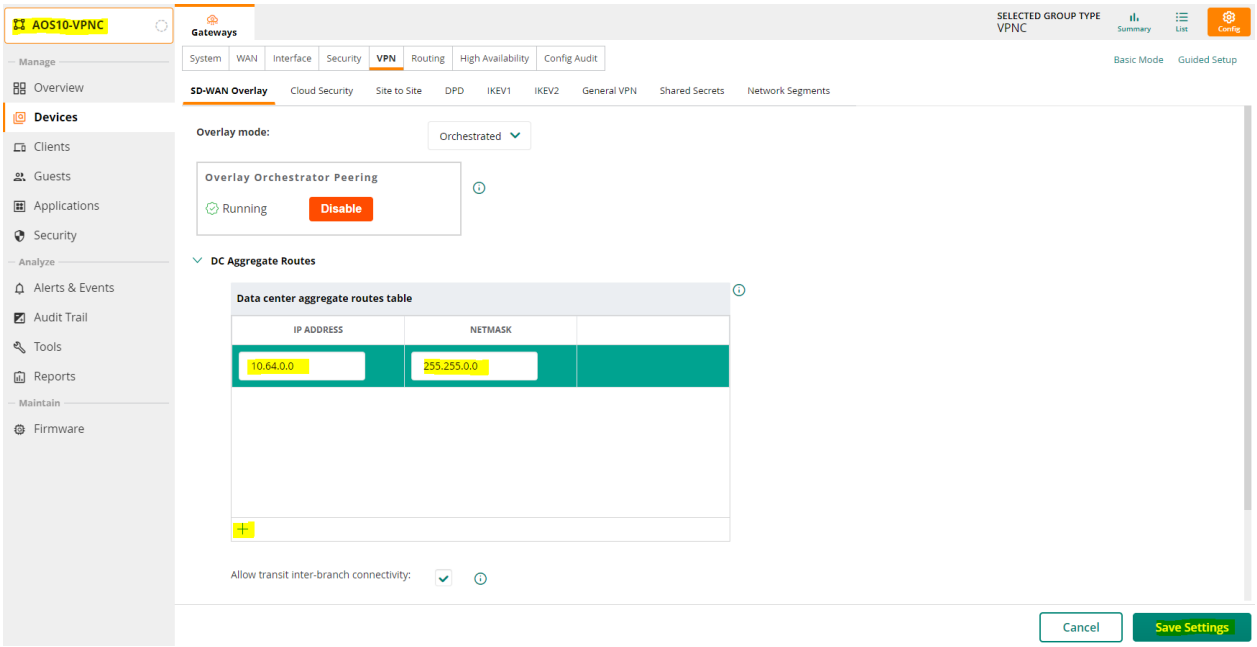
```
L3D OAP Tunnel Table
--------------------
Peer MAC            Map Name                                                Map Id    State
GenId         Pair UUID
--------            --------                                                ------    -----     ---
--          ---------
20:4c:03:0a:b9:e0  gw-ipsecmap-20:4c:03:0a:b9:e0-e0-uplink                  0x50001   Up
171831599     28827c19-c630-4d94-8bc9-893b2e7cc1f3

MicroBranch1#
MicroBranch1# sh l3d oap advertise

L3D OAP Advertised IPv4 Routes
------------------------------
Num   Prefix              Nexthop             Age           GenId
---   ------              -------             ---           -----
0     10.44.44.80/28      br0.44              14362.802     1639190506625830
1     10.99.99.7/32       tun0                14303.586     1639190506625831

CheckSum:0x832172f2b73a1281 entries:2

MicroBranch2#
```

3.3 Route Summarisation

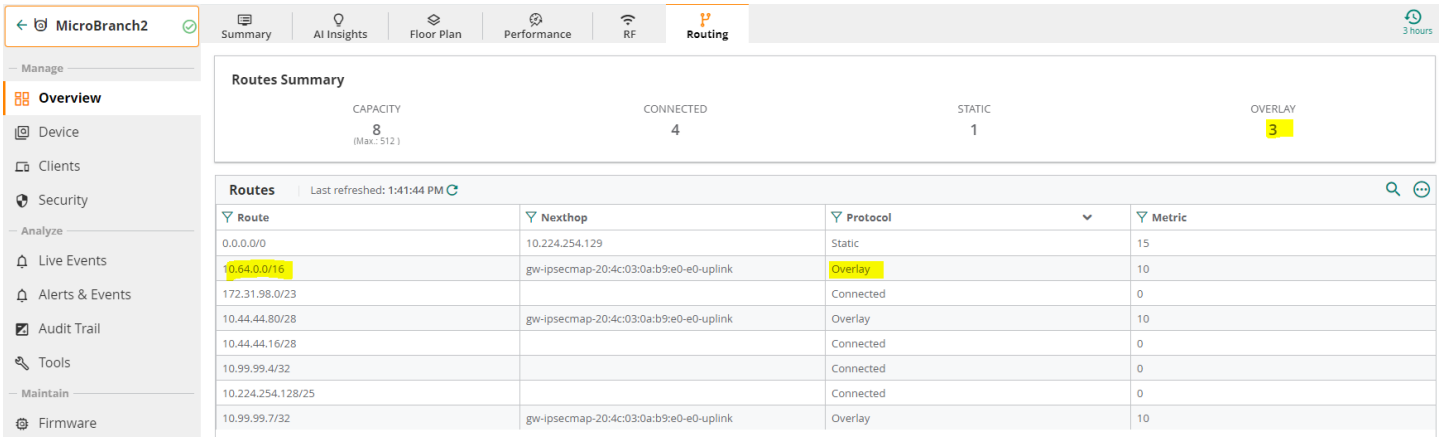
You noted that there were 3x routes being learnt by the microbranch APs.



In most cases it is a good practice to summarise the routes. So, we'll do that from the VPNC group configuration.



Once we have saved it, we'll check the routing table of microbranch2 AP.



3.4 Inter Branch Connectivity

In this sub-section we'll test the inter branch connectivity between VLAN44, remember that it is a RL3 subnet, and it is being transited through the VPNC. We'll ping microbranch2 (10.44.44.17) AP from microbranch1 (10.44.44.81) AP.

Before we start our ping, we'll see no entries for 10.44.44.17 in the route cache entries.

```
MicroBranch1# sh ip int brief
Interface                        IP Address / IP Netmask       Admin   Protocol
br0                             169.254.1.1 / 255.255.0.0      up      up
br0.44                          10.44.44.81 / 255.255.255.240  up      up
br0.3333                        172.31.98.1 / 255.255.254.0    up      up
br0.4092                       192.168.2.50 / 255.255.255.0    up      up
MicroBranch1#

MicroBranch1# sh datap route
Route Table Entries
-------------------

Flags: L - Local, P - Permanent,  T - Tunnel, Y - Dirty, I - IPsec, M - Mobile, A - ARP,
D - Drop, U - Use Default Gateway, G - PPPoE/3G/4G Gateway

       IP              Mask            Gateway        Cost  VLAN  Flags
---------------  ---------------  ---------------  ----  ----  -----
0.0.0.0          0.0.0.0          192.168.2.1         0  4092
10.44.44.16      255.255.255.240  192.168.1.57        0     0  T
10.44.44.80      255.255.255.240  10.44.44.81         0    44  LP
10.64.0.0        255.255.0.0      192.168.1.57        0     0  T
10.99.99.4       255.255.255.255  192.168.1.57        0     0  T
169.254.0.0      255.255.0.0      169.254.1.1         0  4092  LP
172.31.98.0      255.255.254.0    172.31.98.1         0  3333  D
192.168.2.0      255.255.255.0    192.168.2.50        0  4092  LP

Route Cache Entries
-------------------

Flags: L - local, P - Permanent,  T - Tunnel, I - IPsec, M - Mobile, A - ARP, D - Drop, G
- 3G/4G

       IP              MAC              VLAN      Flags      TunIdx
---------------  -----------------  -----------  ---------  ------
192.168.1.57     00:00:00:00:00:00  tunnel   31  PT              1
192.168.2.1      B0:B9:8A:A6:CA:3A         4092  A
192.168.2.50     20:4C:03:5C:05:6E         4092  LP
10.99.99.7       20:4C:03:5C:05:6E         4092  LP
10.44.44.81      20:4C:03:5C:05:6E           44  LP
172.31.98.1      20:4C:03:5C:05:6E         3333  LP
```

```
169.254.1.1      20:4C:03:5C:05:6E         4092  LP
MicroBranch1#
```

Now we'll start the ping test.

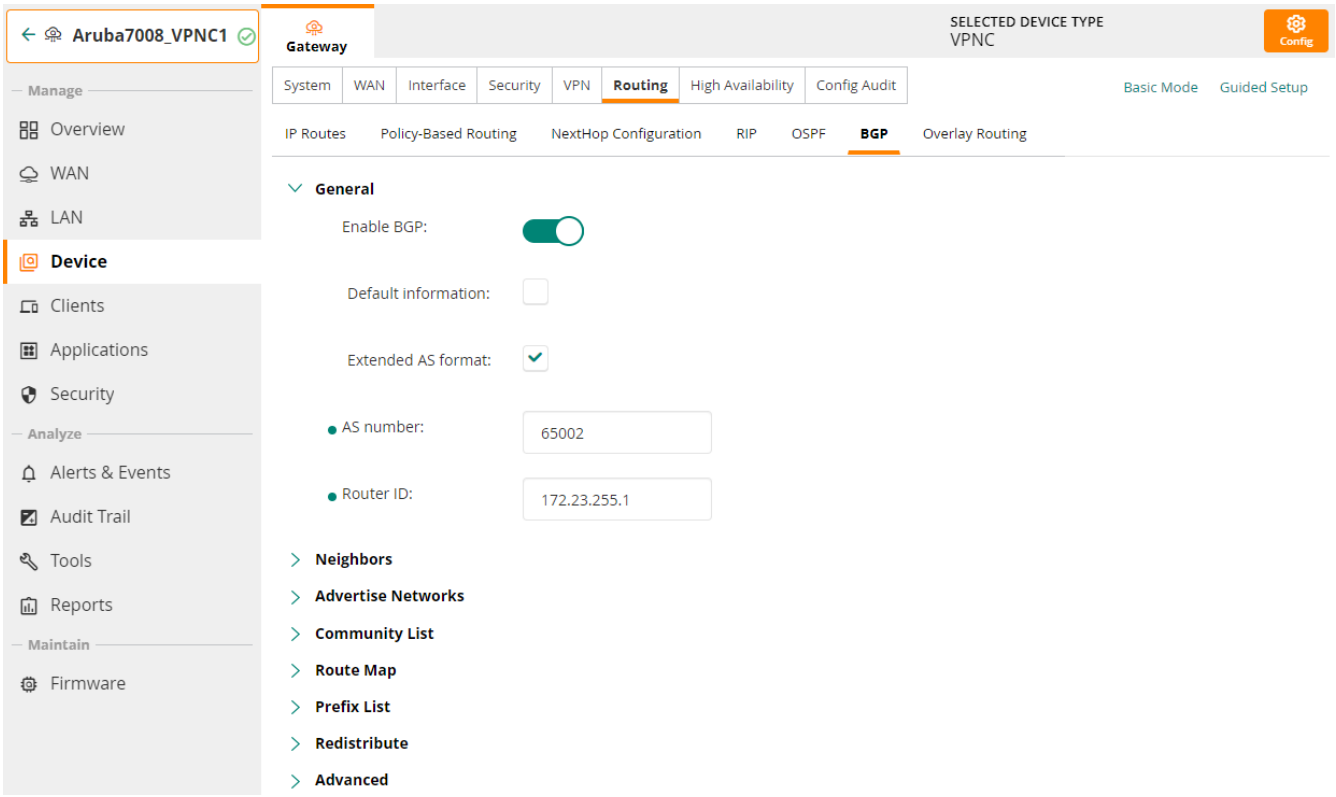
```
MicroBranch1# ping 10.44.44.17 source-address 10.44.44.81
Press 'q' to abort.
PING 10.44.44.17 (10.44.44.17): 56 data bytes
64 bytes from 10.44.44.17: icmp_seq=0 ttl=63 time=231.2 ms
64 bytes from 10.44.44.17: icmp_seq=1 ttl=63 time=274.3 ms
64 bytes from 10.44.44.17: icmp_seq=2 ttl=63 time=312.5 ms
64 bytes from 10.44.44.17: icmp_seq=3 ttl=63 time=271.2 ms
64 bytes from 10.44.44.17: icmp_seq=4 ttl=63 time=97.1 ms

--- 10.44.44.17 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 97.1/237.2/312.5 ms

MicroBranch1#
```

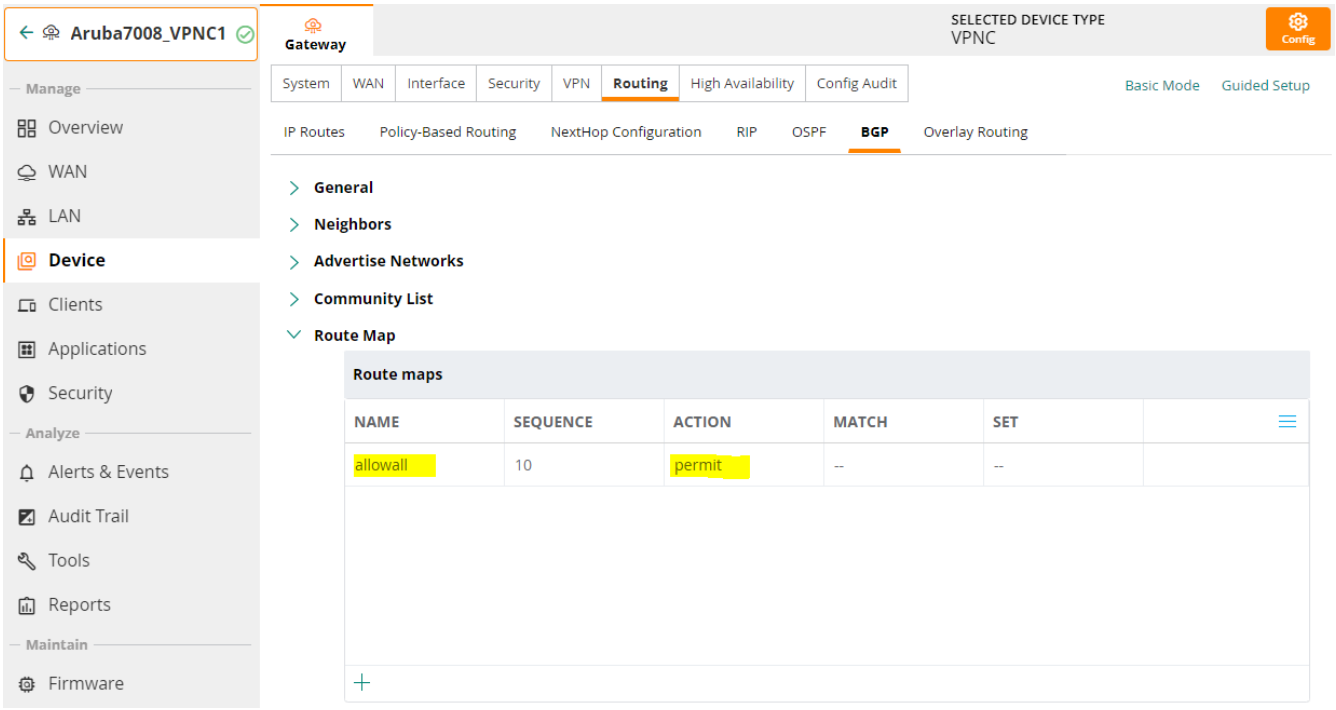
Now checking the route datapath cache entries

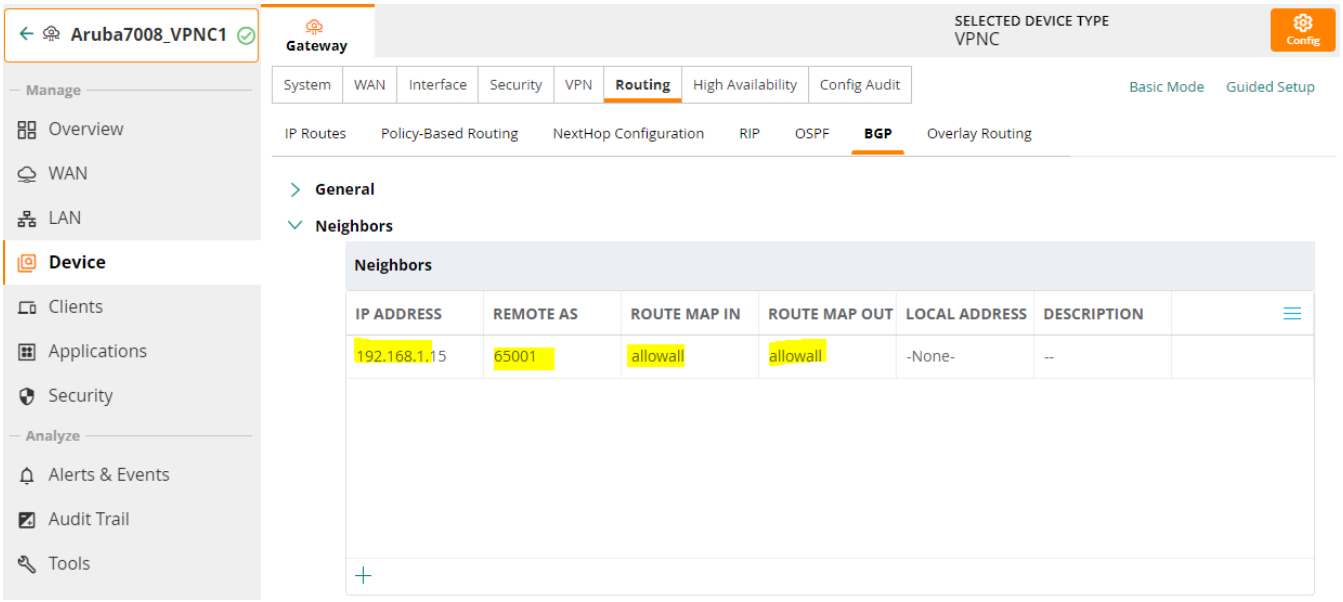
```
MicroBranch1#  sh datap route
Route Table Entries
-------------------

Flags: L - Local, P - Permanent,  T - Tunnel, Y - Dirty, I - IPsec, M - Mobile, A - ARP,
D - Drop, U - Use Default Gateway, G - PPPoE/3G/4G Gateway

       IP             Mask           Gateway       Cost  VLAN  Flags
---------------  ---------------  ---------------  ----  ----  -----
0.0.0.0          0.0.0.0          192.168.2.1         0  4092
10.44.44.16      255.255.255.240  192.168.1.57        0     0  T
10.44.44.80      255.255.255.240  10.44.44.81         0    44  LP
10.64.0.0        255.255.0.0      192.168.1.57        0     0  T
10.99.99.4       255.255.255.255  192.168.1.57        0     0  T
169.254.0.0      255.255.0.0      169.254.1.1         0  4092  LP
172.31.98.0      255.255.254.0    172.31.98.1         0  3333  D
192.168.2.0      255.255.255.0    192.168.2.50        0  4092  LP

Route Cache Entries
-------------------
Flags: L - local, P - Permanent,  T - Tunnel, I - IPsec, M - Mobile, A - ARP, D - Drop, G
- 3G/4G

       IP              MAC              VLAN      Flags      TunIdx
---------------  -----------------  -----------  ---------  ------
192.168.1.57     00:00:00:00:00:00  tunnel   31  PT              1
192.168.2.1      B0:B9:8A:A6:CA:3A         4092  A
192.168.2.50     20:4C:03:5C:05:6E         4092  LP
10.99.99.7       20:4C:03:5C:05:6E         4092  LP
10.44.44.81      20:4C:03:5C:05:6E           44  LP
10.44.44.17      00:00:00:00:00:00  tunnel   31  T               1
172.31.98.1      20:4C:03:5C:05:6E         3333  LP
169.254.1.1      20:4C:03:5C:05:6E         4092  LP

MicroBranch1#
```

3.5 BGP Routing Configuration

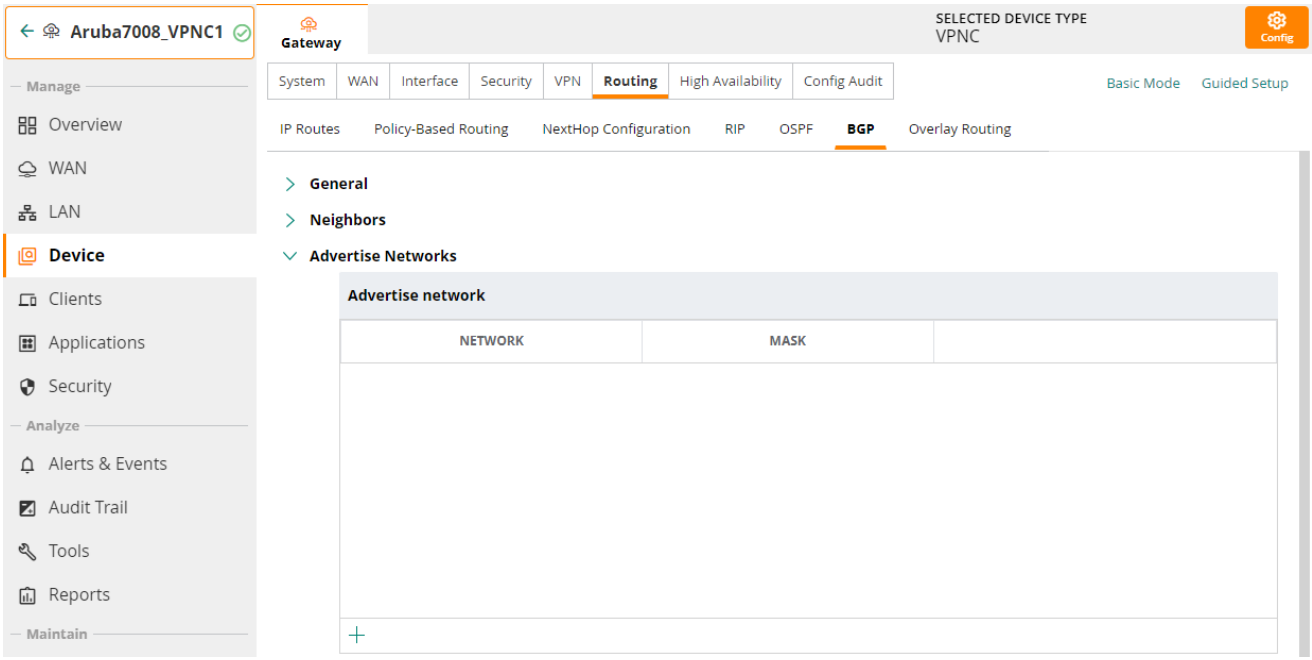
Here we'll configure the VPNC1 for a simple eBGP routing.

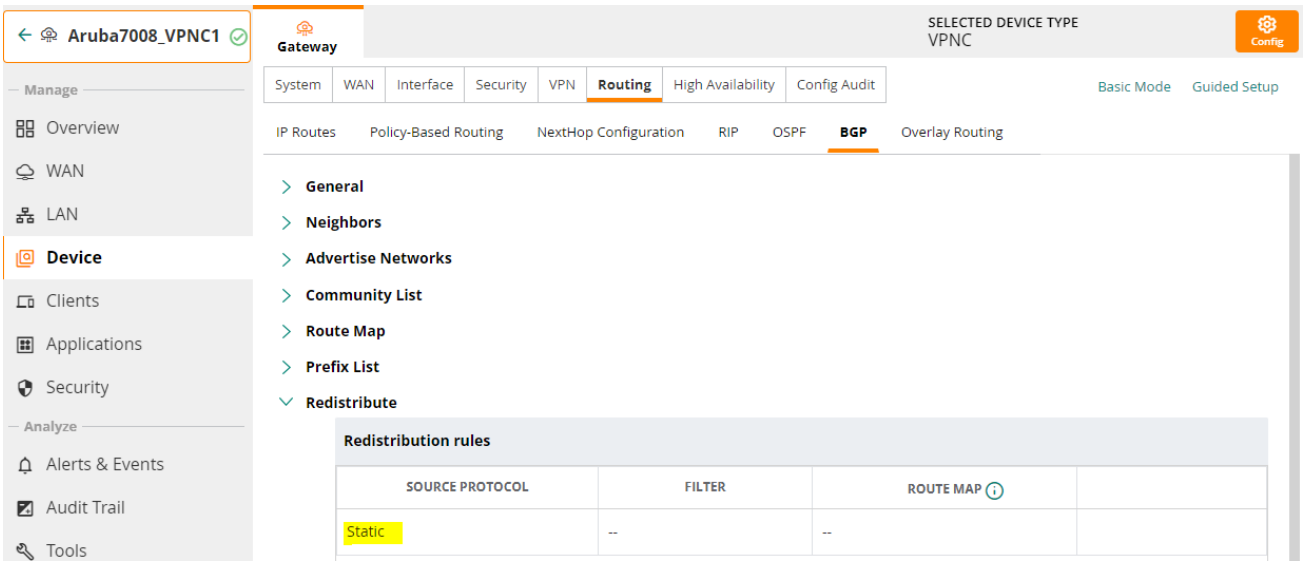

Aruba7008_VPNC1
Gateway
SELECTED DEVICE TYPE
VPNC
Config
Manage
Overview
WAN
LAN
Device
Clients
Applications
Security
Analyze
Alerts & Events
Audit Trail
Tools
Reports
Maintain
Firmware
System
WAN
Interface
Security
VPN
Routing
High Availability
Config Audit
Basic Mode
Guided Setup
IP Routes
Policy-Based Routing
NextHop Configuration
RIP
OSPF
BGP
Overlay Routing
General
Enable BGP:
Default information:
Extended AS format:
AS number:
65002
Router ID:
172.23.255.1
Neighbors
Advertise Networks
Community List
Route Map
Prefix List
Redistribute
Advanced


Aruba7008_VPNC1
Gateway
SELECTED DEVICE TYPE
VPNC
Config
Manage
Overview
WAN
LAN
Device
Clients
Applications
Security
Analyze
Alerts & Events
Audit Trail
Tools
Reports
Maintain
Firmware
System
WAN
Interface
Security
VPN
Routing
High Availability
Config Audit
Basic Mode
Guided Setup
IP Routes
Policy-Based Routing
NextHop Configuration
RIP
OSPF
BGP
Overlay Routing
General
Neighbors
Advertise Networks
Community List
Route Map
Route maps
NAME
SEQUENCE
ACTION
MATCH
SET
allowall
10
permit
--
--

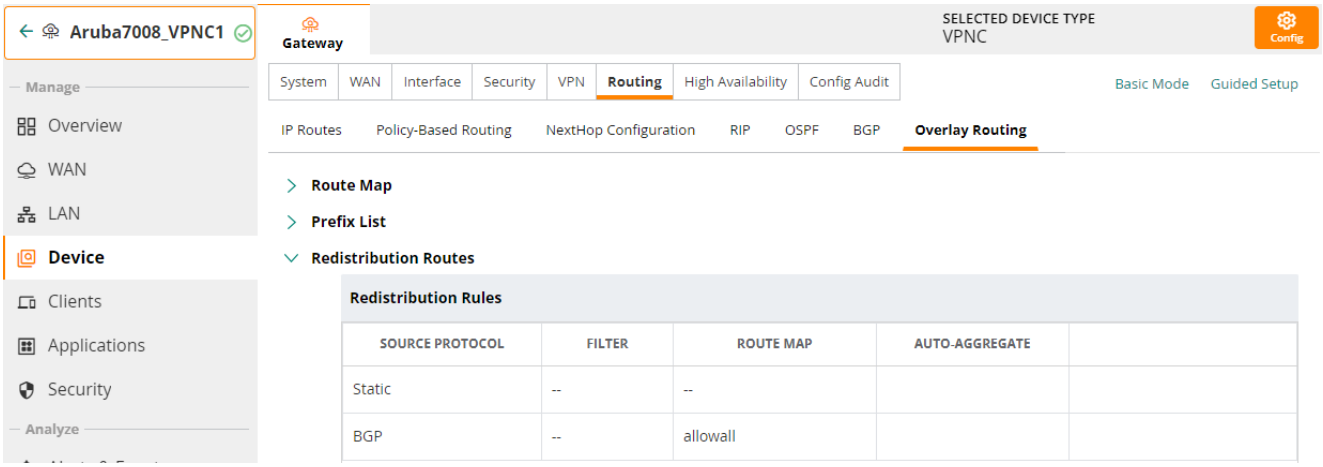


Here we are not advertising any routes directly, but we are redistributing the existing static routes.





And then we'll redistributed the learnt BGP routes in overlay so that microbranches can get to them.

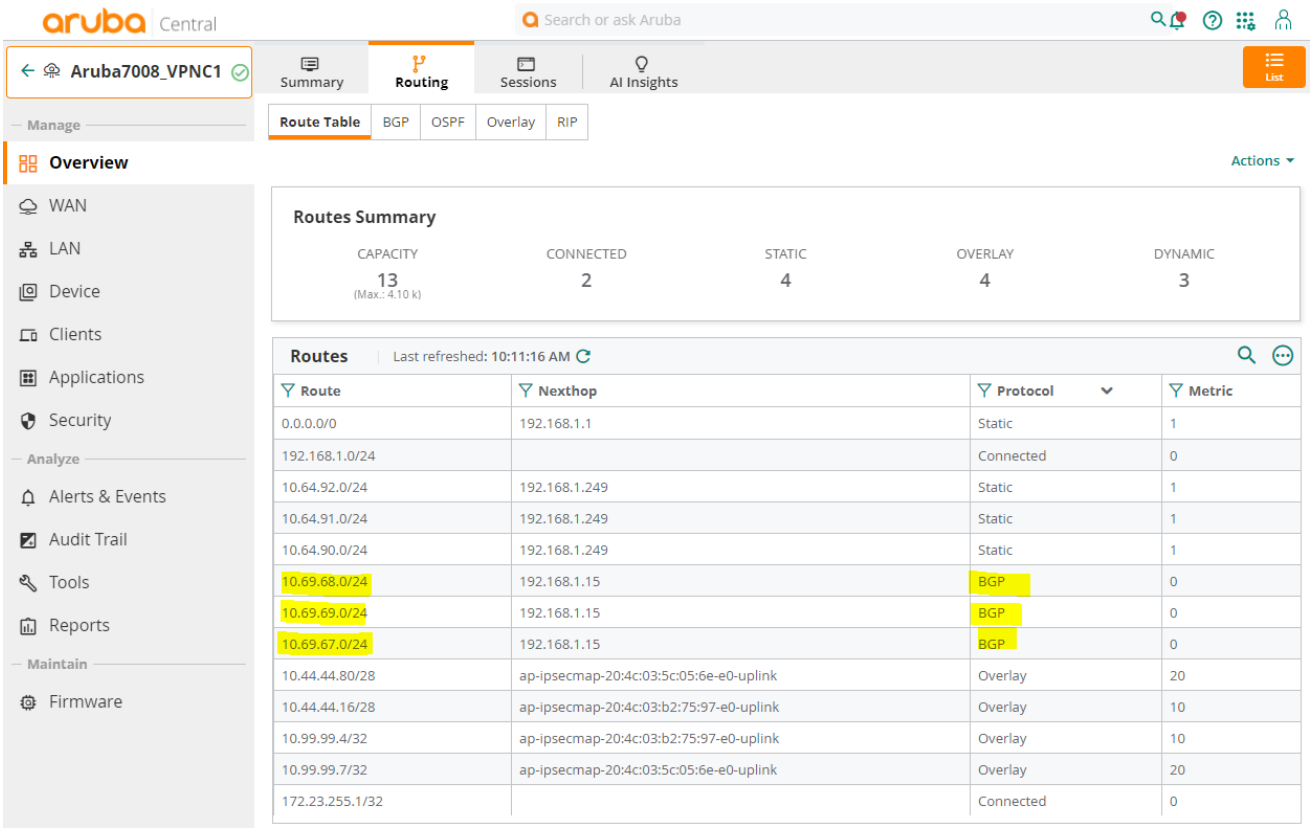


3.6 BGP Routing Testing

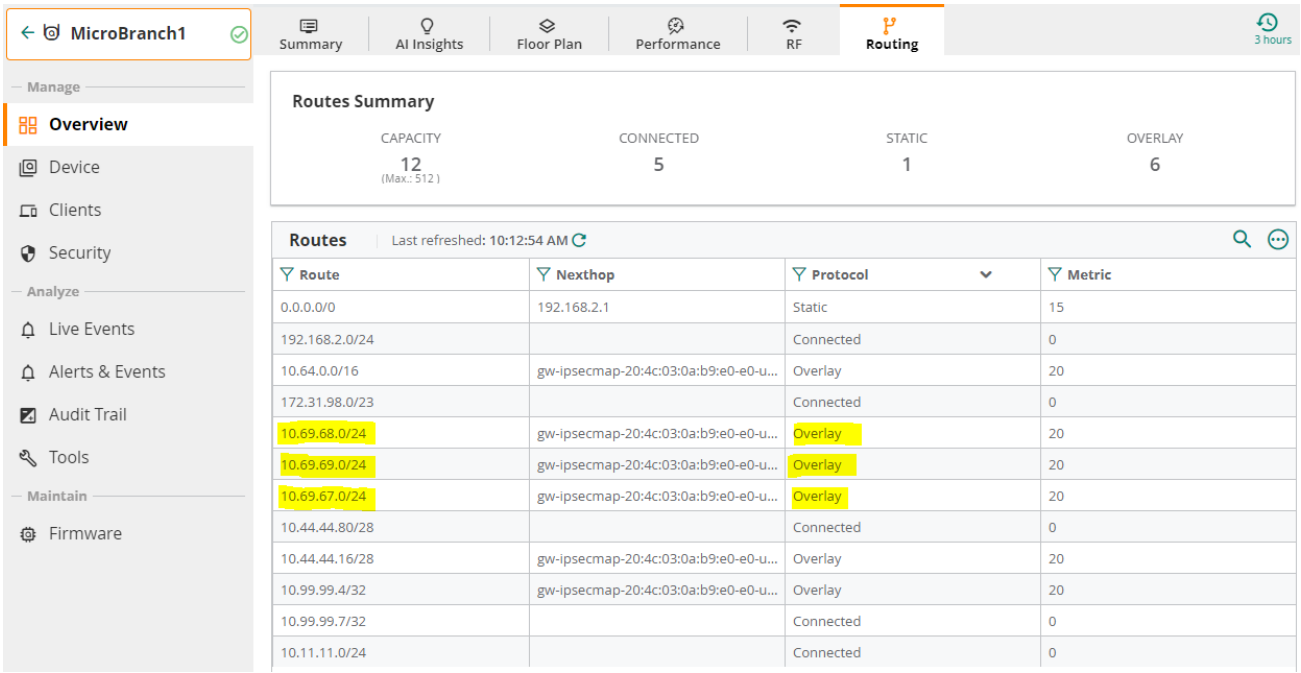
Here we'll check the VPNC1's routing table.

```
(Aruba7008_VPNC1) #show ip bgp summary

BGP Router identifier 172.23.255.1, local AS number 65002
Total Neighbors 1 Neighbors UP 1 Neighbors DOWN 0
Total Number of Network Entries 3
BGP Neighbor Information
------------------------
Neighbor        V  AS      MsgRcvd  MsgSent  InQ  OutQ  UpTime  State        PfxRcd
--------        -  --      -------  -------  ---  ----  ------  -----        ------
192.168.1.15    4  65001   3        13       0    0     29m20s  Established  3
(Aruba7008_VPNC1) #
```

```
(Aruba7008_VPNC1) #show ip route

Codes: C - Connected, O - OSPF, IA - OSPF Inter Area, E1 - OSPF External Type 1, R - RIP
       E2 - OSPF External Type 2, N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External
Type 2
       B I - BGP Interior, B E - BGP Exterior, S - Static
       U - BGW Peer Uplink, M - Management, Ru - Route Usable, * - Candidate Default
       V - RAPNG VPN/Branch, I - Crypto-Cfgset, N - Not Redistributed, Bc - Cloud Overlay
Protocol

S*     0.0.0.0/0   [50/1] via 192.168.1.1
C      192.168.1.0/24 is directly connected, VLAN192
S      10.64.92.0/24   [50/1] via 192.168.1.249
S      10.64.91.0/24   [50/1] via 192.168.1.249
S      10.64.90.0/24   [50/1] via 192.168.1.249
B     10.69.68.0/24   [100/0] via 192.168.1.15(E)
B     10.69.69.0/24   [100/0] via 192.168.1.15(E)
B     10.69.67.0/24   [100/0] via 192.168.1.15(E)
Bc     10.44.44.80/28   [90/20] ipsec map ap-ipsecmap-20:4c:03:5c:05:6e-e0-uplink
Bc     10.44.44.16/28   [90/10] ipsec map ap-ipsecmap-20:4c:03:b2:75:97-e0-uplink
Bc     10.99.99.4/32   [90/10] ipsec map ap-ipsecmap-20:4c:03:b2:75:97-e0-uplink
Bc     10.99.99.7/32   [90/20] ipsec map ap-ipsecmap-20:4c:03:5c:05:6e-e0-uplink
C      172.23.255.1/32 is directly connected, Loopback

(Aruba7008_VPNC1) #
```



Now checking the microbranch1 to see if we see these routes.



4 WAN Health Check

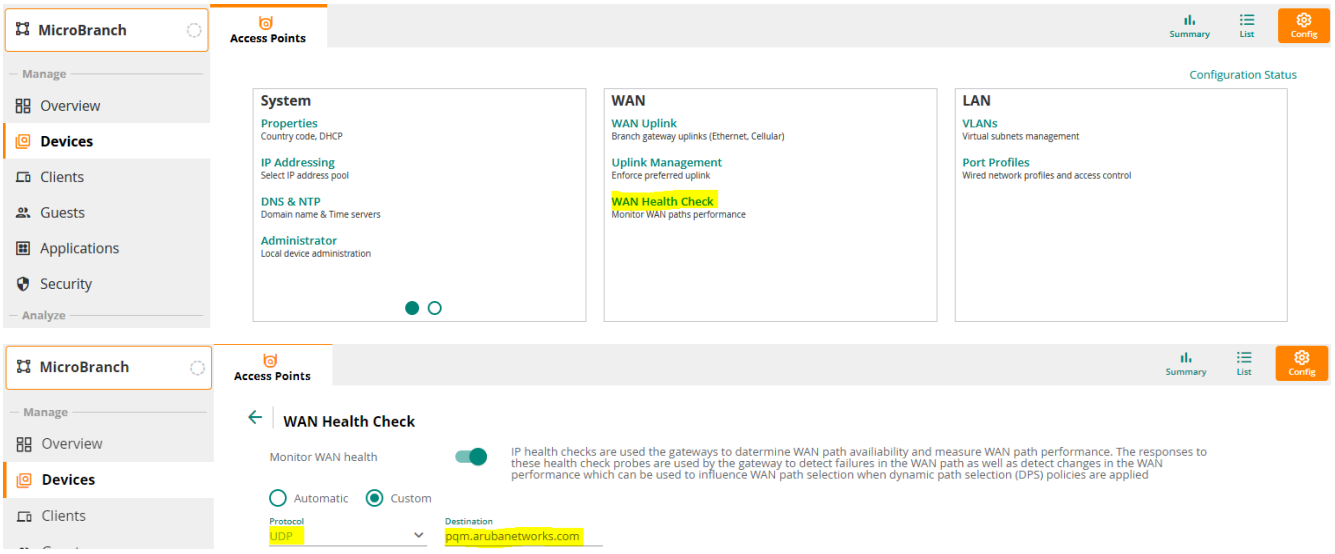
The WAN Health check is like the health check for the gateways. It sends probes to measure WAN availability and latency on selected uplinks. Based on probe response, gateways continue to use the primary uplink or failover to a backup link.

It's good practice to enable this feature on all Microbranch groups. When enabled, the probes are sent through the underlay at regular intervals to verify if the Internet is reachable over the uplink interfaces configured on Gateways. Based on the probe response, the uplink interface is marked as unavailable for the underlay traffic.

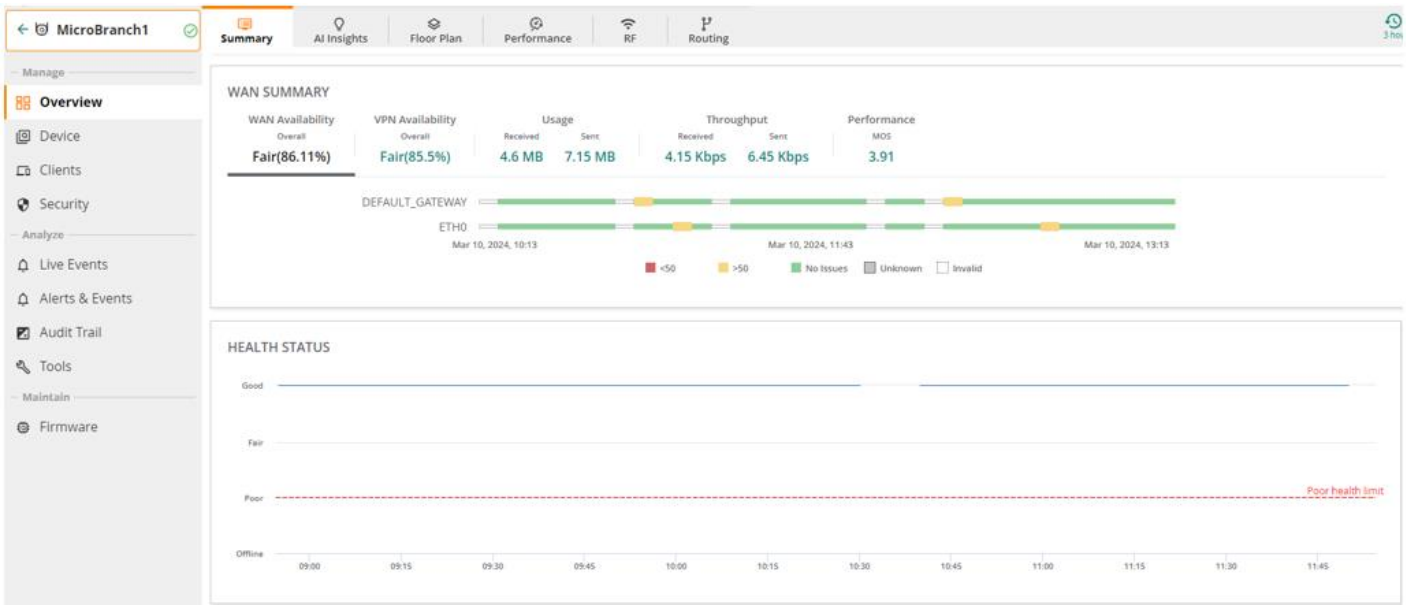
It sends 5x UDP or ICMP probes to a host every 10 seconds. The tunnel health is determined based if

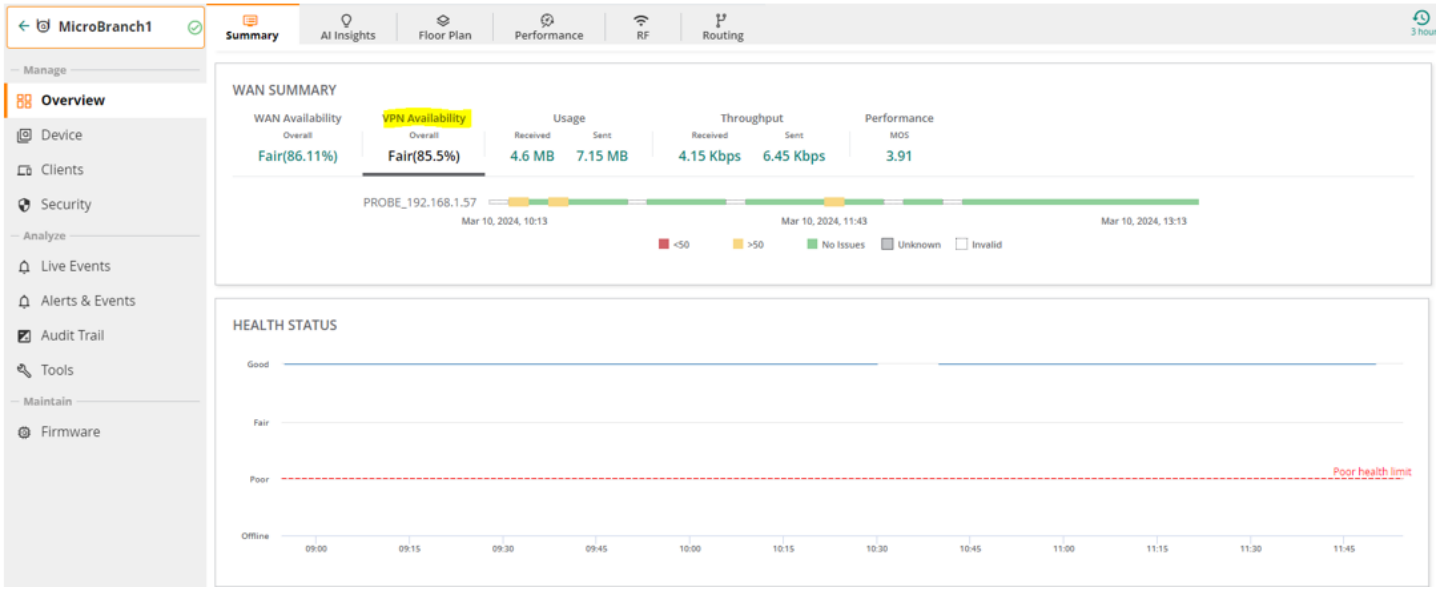
1. a probe is lost, then five probes are sent every two seconds to the host.
2. a probe is lost in the first two seconds, then the aggressive mode is enabled by default, and 25 probes are sent every two seconds for the next 10 seconds.
3. the probes don't reach the destination, then the tunnel is torn down, achieving faster tunnel age-out with min packet loss.

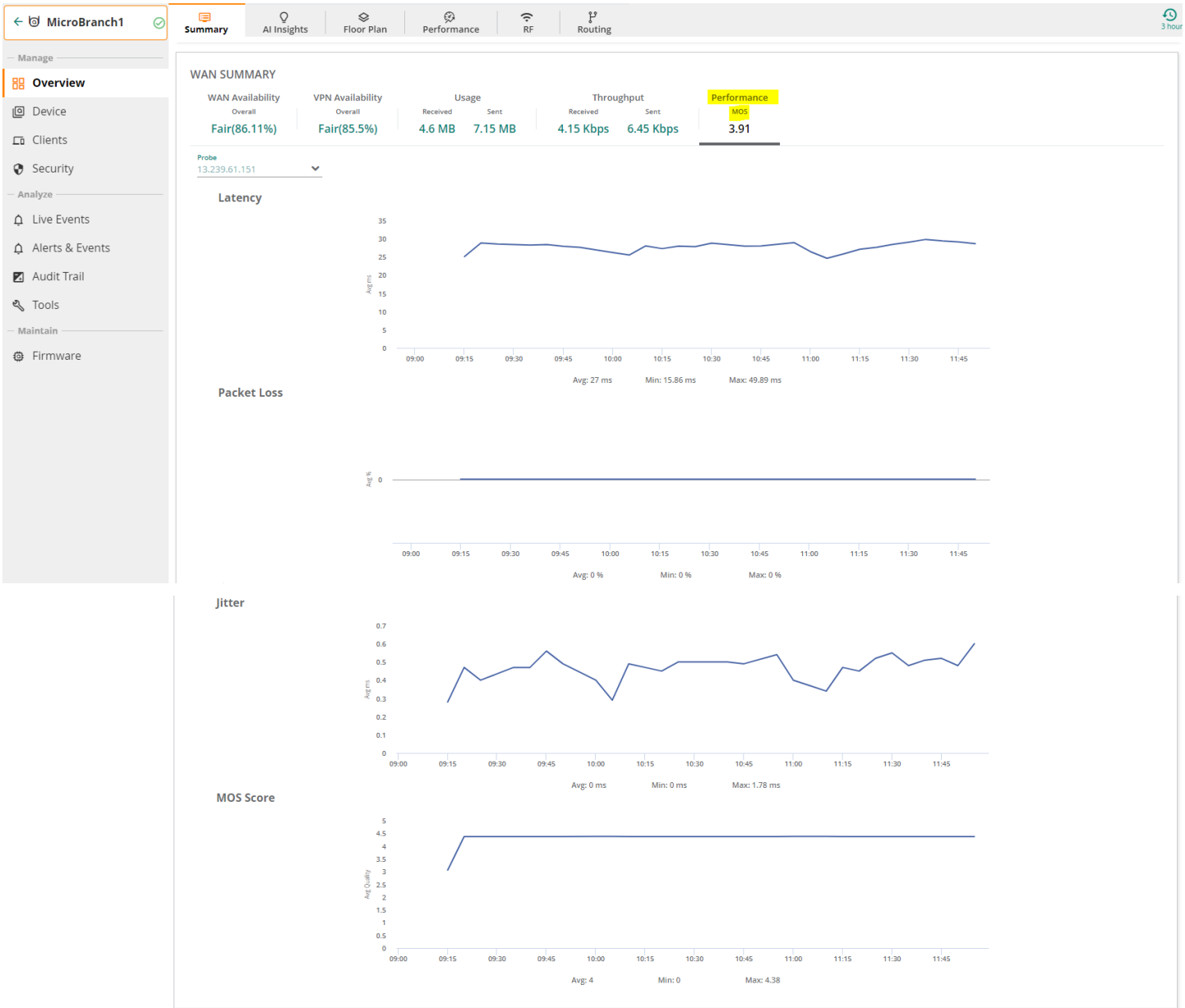
When probes are not lost, the Microbranch goes back to sending five probes every 10 seconds per uplink. In Basic mode, WAN health check can be configured at the group level for the Microbranch only



This feature requires Advanced licenses and not available in APs with Foundation licenses. The WAN health check configuration works in APs in Microbranch group starting with AOS 10.3 or later versions. Now we should be able to see the tunnel health from here.




MicroBranch1
Summary
AI Insights
Floor Plan
Performance
RF
Routing
3 hour
Manage
Overview
Device
Clients
Security
Analyze
Live Events
Alerts & Events
Audit Trail
Tools
Maintain
Firmware
WAN SUMMARY
WAN Availability
Overall
Fair(86.11%)
VPN Availability
Overall
Fair(85.5%)
Usage
Received
4.6 MB
Sent
7.15 MB
Throughput
Received
4.15 Kbps
Sent
6.45 Kbps
Performance
MOS
3.91
PROBE_192.168.1.57
Mar 10, 2024, 10:13
Mar 10, 2024, 11:43
Mar 10, 2024, 13:13
<50
>50
No Issues
Unknown
Invalid
HEALTH STATUS
Good
Fair
Poor
Offline
Poor health limit
09:00
09:15
09:30
09:45
10:00
10:15
10:30
10:45
11:00
11:15
11:30
11:45


MicroBranch1
Summary
AI Insights
Floor Plan
Performance
RF
Routing
3 hour
Manage
Overview
Device
Clients
Security
Analyze
Live Events
Alerts & Events
Audit Trail
Tools
Maintain
Firmware
WAN SUMMARY
WAN Availability
Overall
Fair(86.11%)
VPN Availability
Overall
Fair(85.5%)
Usage
Received
4.6 MB
Sent
7.15 MB
Throughput
Received
4.15 Kbps
Sent
6.45 Kbps
Performance
MOS
3.91
Probe
13.239.61.151
Latency
Avg ms
Avg: 27 ms
Min: 15.86 ms
Max: 49.89 ms
Packet Loss
Avg %
Avg: 0 %
Min: 0 %
Max: 0 %
Jitter
Avg ms
Avg: 0 ms
Min: 0 ms
Max: 1.78 ms
MOS Score
Avg Quality
Avg: 4
Min: 0
Max: 4.38
09:00
09:15
09:30
09:45
10:00
10:15
10:30
10:45
11:00
11:15
11:30
11:45