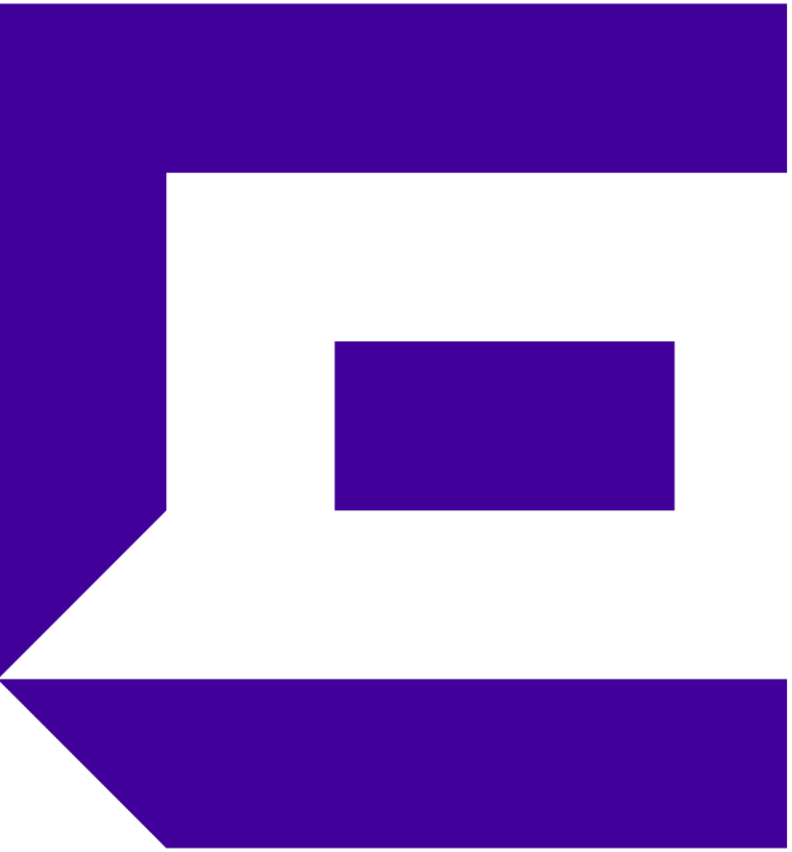
Extreme Wireless WiNG Quick Start Guide

Version 4 - 29/09/2017

Slava Dementyev
Corporate Systems Engineer

Extreme®
Connect Beyond the Network



WiNG - Quick Start Guide

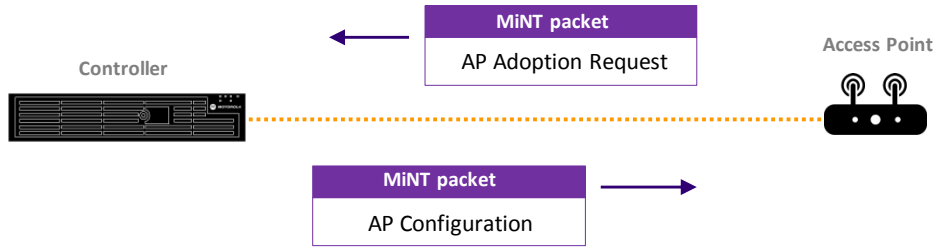
Part 1 – What is MiNT?
..or how WiNG devices talk to each other

Extreme®
Connect Beyond the Network

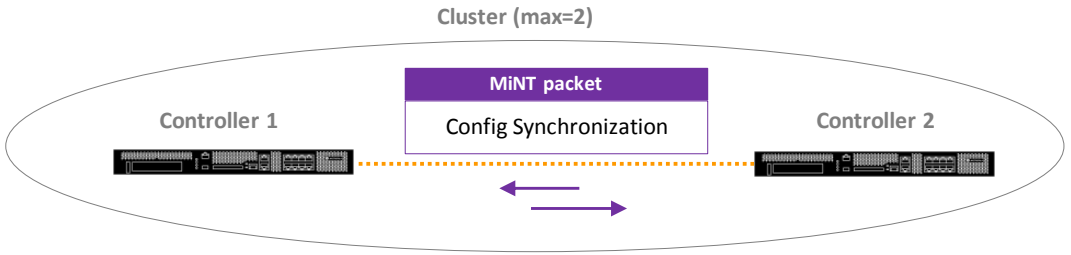
MiNT Protocol

- MiNT protocol is the means of communication between WiNG 5 devices

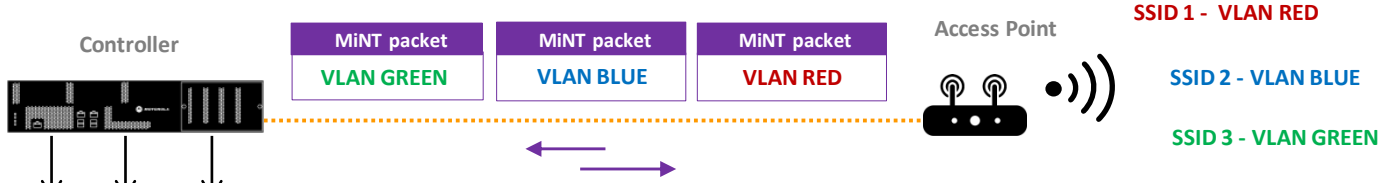
MiNT is used for Access Points Adoption and Provisioning



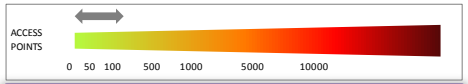
MiNT is used for Clustering



MiNT is used for Traffic Tunneling

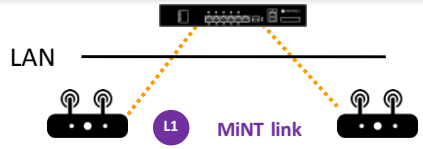


MiNT Protocol



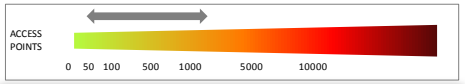
One Building / One VLAN
no IP address on APs
Single RF Domain

Automatic adoption @ Layer 2



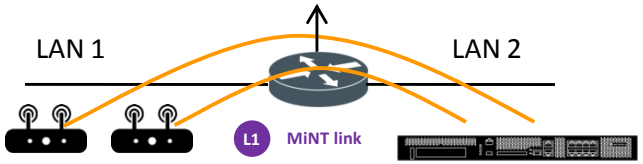
- Adoption and Provisioning using Ethertype 0x8783
- Layer 2 adoption
- MiNT links are « **Level 1** » (default)

As a best practice: - for more than 64 Single Radio access points, layer 3 adoption is recommended
- for more than 128 Dual / Tri Radio access points, layer 3 adoption is recommended

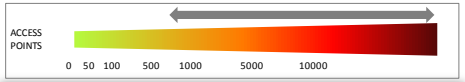


Campus / Several LANs
APs with IP addresses
Single RF Domain

DHCP option 191: pool1=192.168.0.1

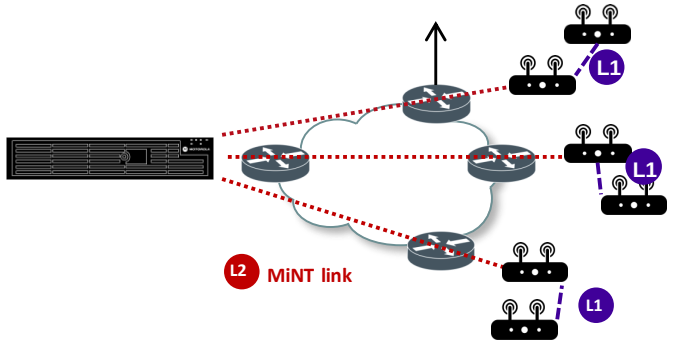


- Adoption and Provisionning using IP/UDP (port 24576)
- Layer 3 adoption
- Using DHCP option 191, APs get controller's IP address for adoption
- MiNT links are « **Level 1** » (default)



APs among several remote sites
Several RF Domains

DHCP option 191: pool1=192.168.0.1;level=2



- Adoption and Provisioning using IP/UDP (port 24576)
- Layer 3 adoption
- Using DHCP option 191, APs get controller's IP address and MiNT level for adoption
- MiNT links are « **Level 2** ».
- Level 2 MiNT links provides MiNT routes isolation
- **Level 2 MiNT links provides scalability !**

AP have mint level 1 at layer 2 between them

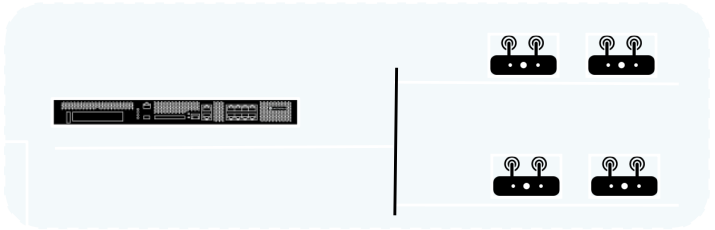
RF Domains - Introduction

- RF Domain concept – When do I need to create rf-domains ?

RF Domain allows administrators to assign configuration data to multiple devices deployed in a common coverage area

One Single Site
One building / One Campus

One coverage area is deployed
⇨ Only one RF Domain is needed
⇨ The default RF Domain can be used



RF Domain default

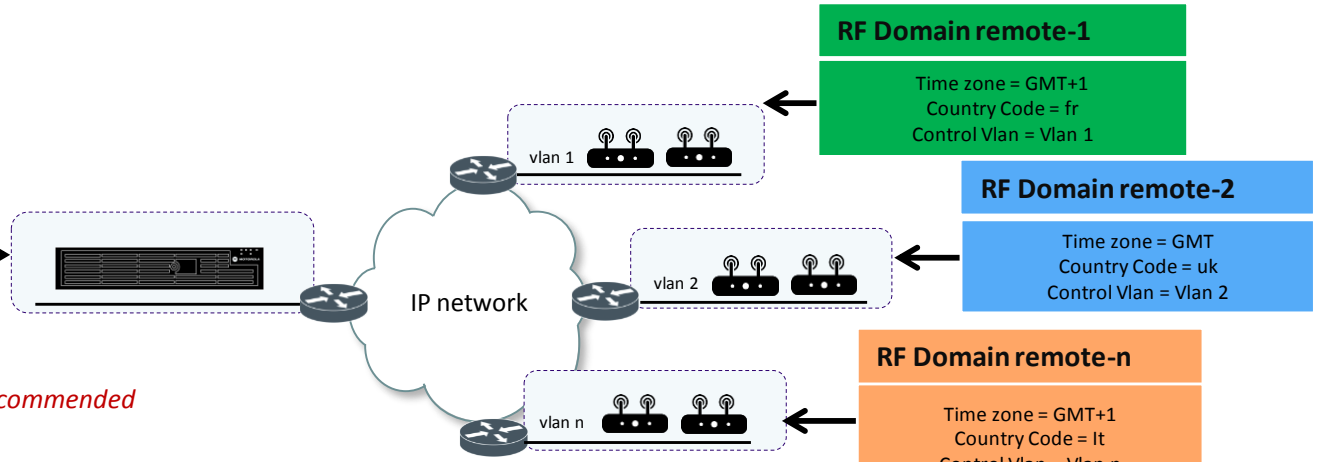
Time zone = GMT
Country Code = gb

MiNT Level 1 deployment

Large Deployments or
One or several remote sites

RF Domain noc

Time zone = GMT+7
Country Code = us



RF Domain remote-1

Time zone = GMT+1
Country Code = fr
Control Vlan = Vlan 1

RF Domain remote-2

Time zone = GMT
Country Code = uk
Control Vlan = Vlan 2

RF Domain remote-n

Time zone = GMT+1
Country Code = It
Control Vlan = Vlan n

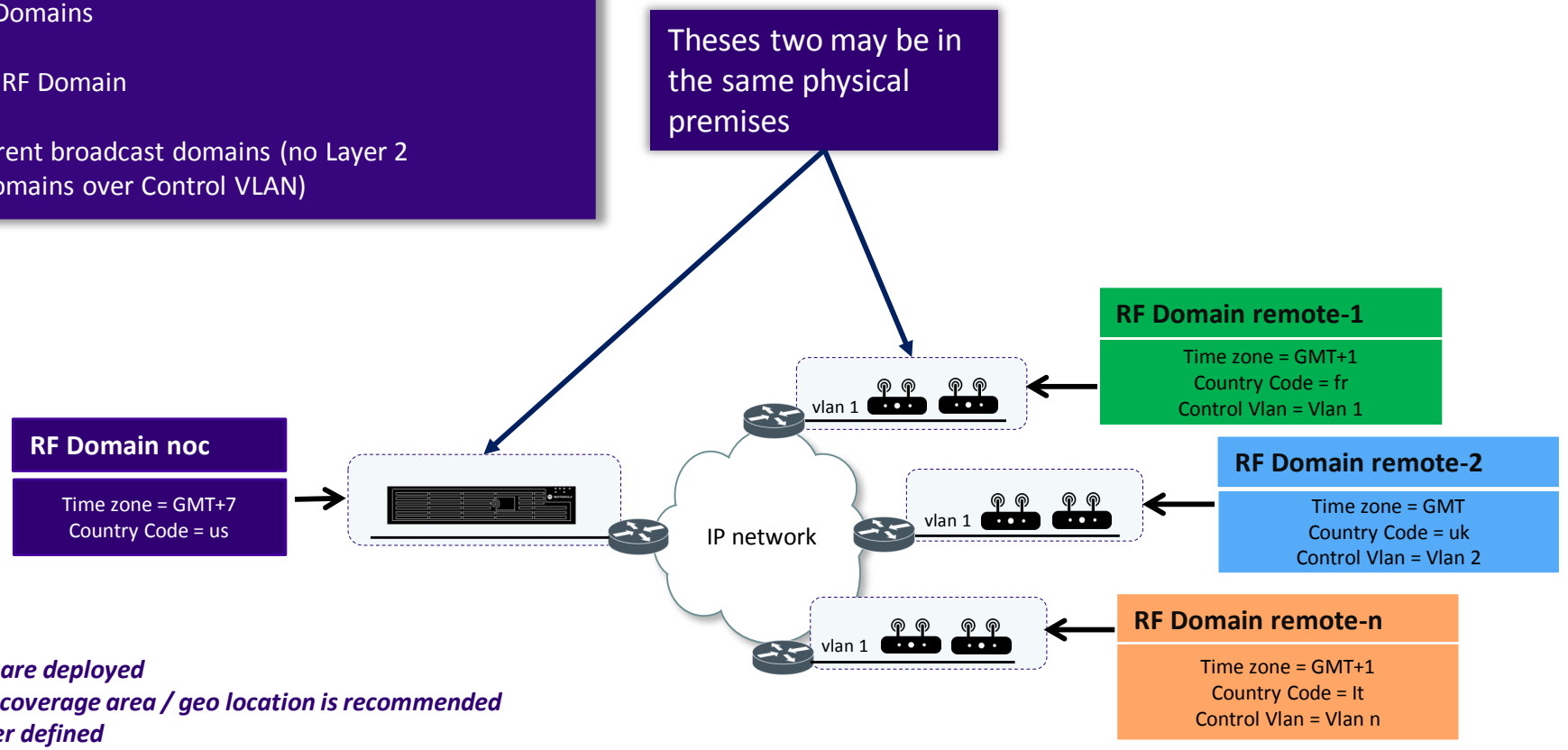
Several coverage area are deployed
⇨ One RF Domain per coverage area is recommended
⇨ RF Domains are user defined

MiNT Level 2 deployment

RF Domains – Centralized Controller with Remote Sites

- When there is more than one site, MINT Level 2 must be used
- All AP must have controller host IP;level=2
  - With DHCP option 191 or
  - Static Profile setting
- Control VLAN is set for AP RF Domains
- Controller is always in its own RF Domain
- RF Domains should be in different broadcast domains (no Layer 2 communication between RF Domains over Control VLAN)

MINT L1 and MINT L2 cannot be mixed on the NOC Controller



Several coverage area are deployed
- ⇨ *One RF Domain per coverage area / geo location is recommended*
- ⇨ *RD Domains are user defined*
- ⇨ *NOC Controller must be placed into their own RF Domain*

How to setup MINT Level 2 ?

- Controller

Centralized controller in a RF Domain with no APs

- Cluster of centralized controllers with MINT L2 Active/Standby only
- AP RF Domains with Control VLAN set to match AP Native VLAN
- All AP with DHCP option 191

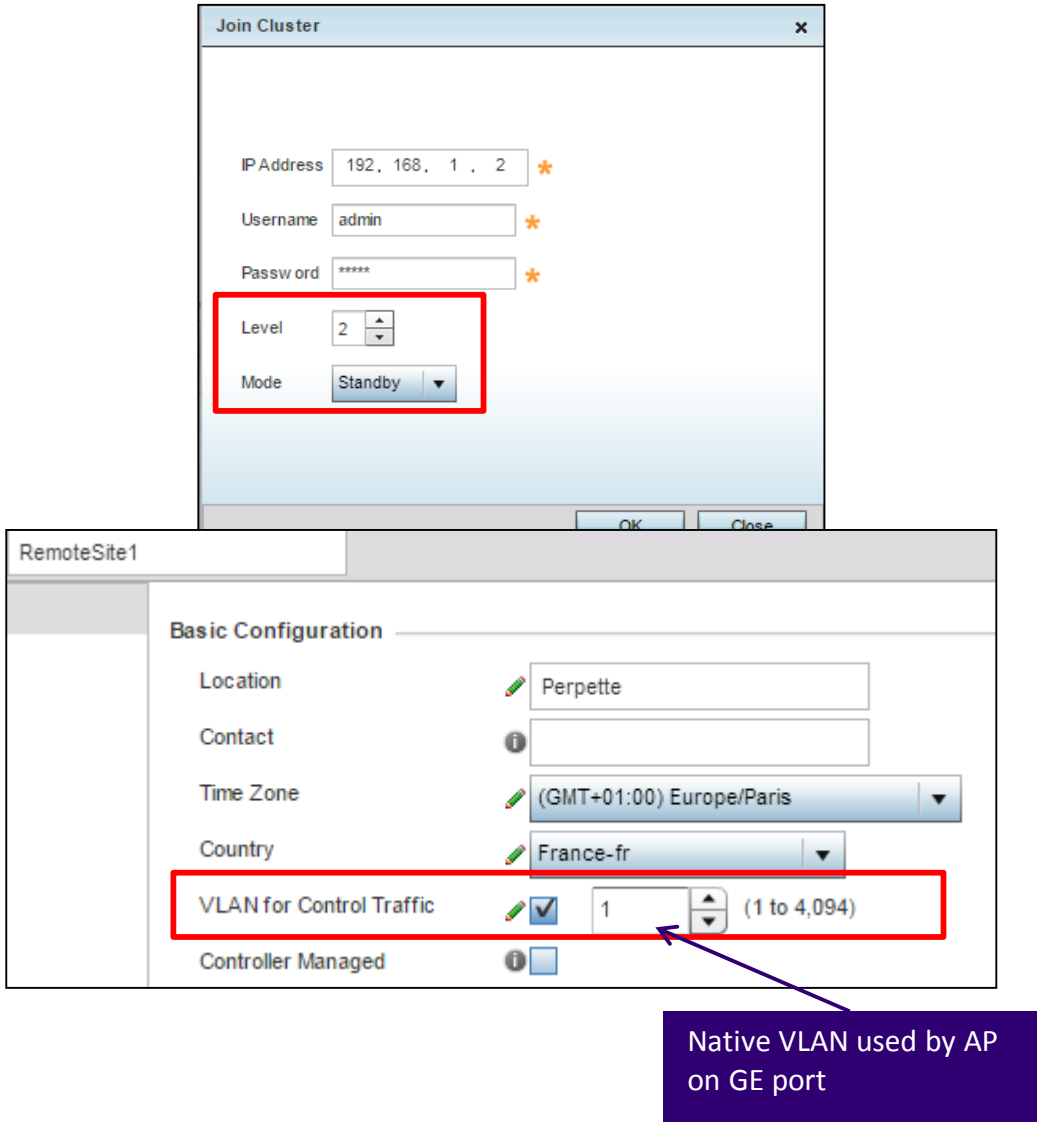
  `"pool1=IP-Ctrl1,IP-Ctrl2;level=2"`
- Static Configuration under Profile or Device Overrides:

```
ap7532 84-24-8D-18-85-E4
 use profile MyAnyAP
 use rf-domain default
 hostname ap7532-1885E4
 controller host 192.168.1.1 pool 1 level 2
rfs4000-1AE686(config-device-84-24-8D-18-85-E4)#
```

- Check what AP has received from DHCP server:

`#show ip dhcp-vendor-options`

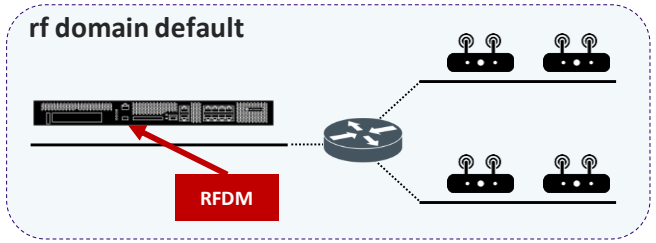
This will tell you what option 191 AP has received



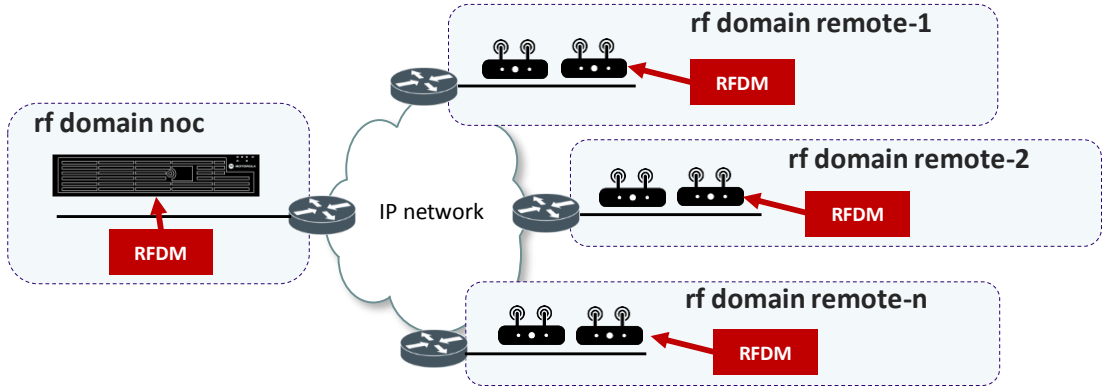
What is a RF Domain Manager ?

For each RF Domain, one device is elected to be the RF Domain Manager (RFDM)

One single RF Domain



Several RF Domains



What does the RF Domain Manager do?

- The RF Domain Manager is responsible for:
  - Collecting Statistics
  - SMART-RF & WIPS coordination
  - Remote Troubleshooting
  - Data tunneling aggregation (optionally for MINT/L2TPv3 tunnels)
  - Distributing firmware & config to other Access Points in the RF Domain

How RF Domain Manager is elected?

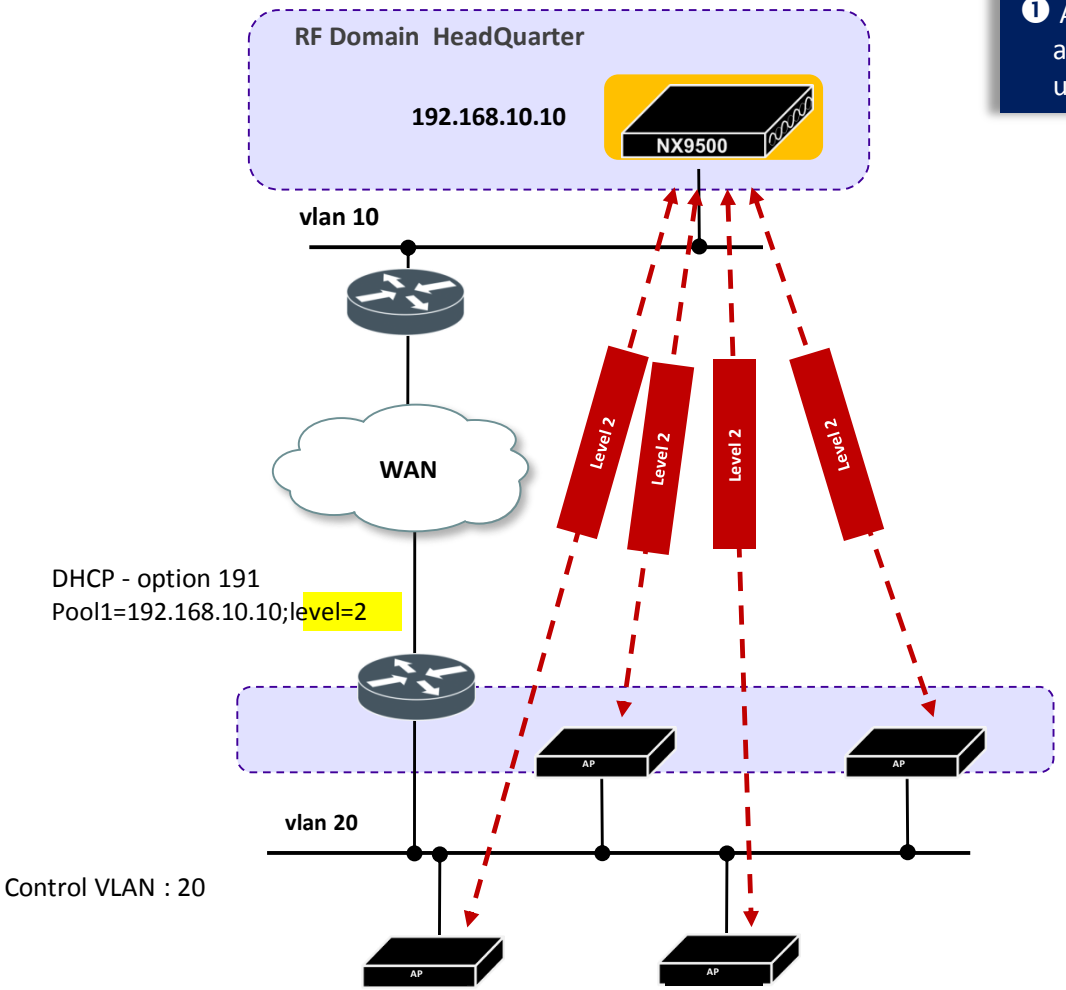
- Automatically elected with automatic failover:
  - If it has the highest RFDM priority
    rf-domain-manager priority [1 – 255]
  - If it has the highest CPU
    (eg. NX9600 > NX5500 > AP8533 > AP6522)
  - If it has the lowest MiNT ID (show mint id)
    (eg. when all devices are the same type)

AP as RFDM scaling

	AP	Access Point RF Domain Manager WiNG 5.5+
Low Tier	AP 6511	24
	AP 621 / 6521	24
	AP7602 | 7622	128
Mid/High Tier	AP 622 / 6522	128
	AP 650 / 6532	128
	AP 6562	128
	AP 71X1	128
	AP 7161	128
	AP 7181	128
	AP 81XX	128
	AP 82XX	128
	AP75X2	128
	AP7612 | AP7632 | AP7662	256
	AP8432	256
	AP8533	256

MiNT Protocol in a NOC model deployment – Step 1

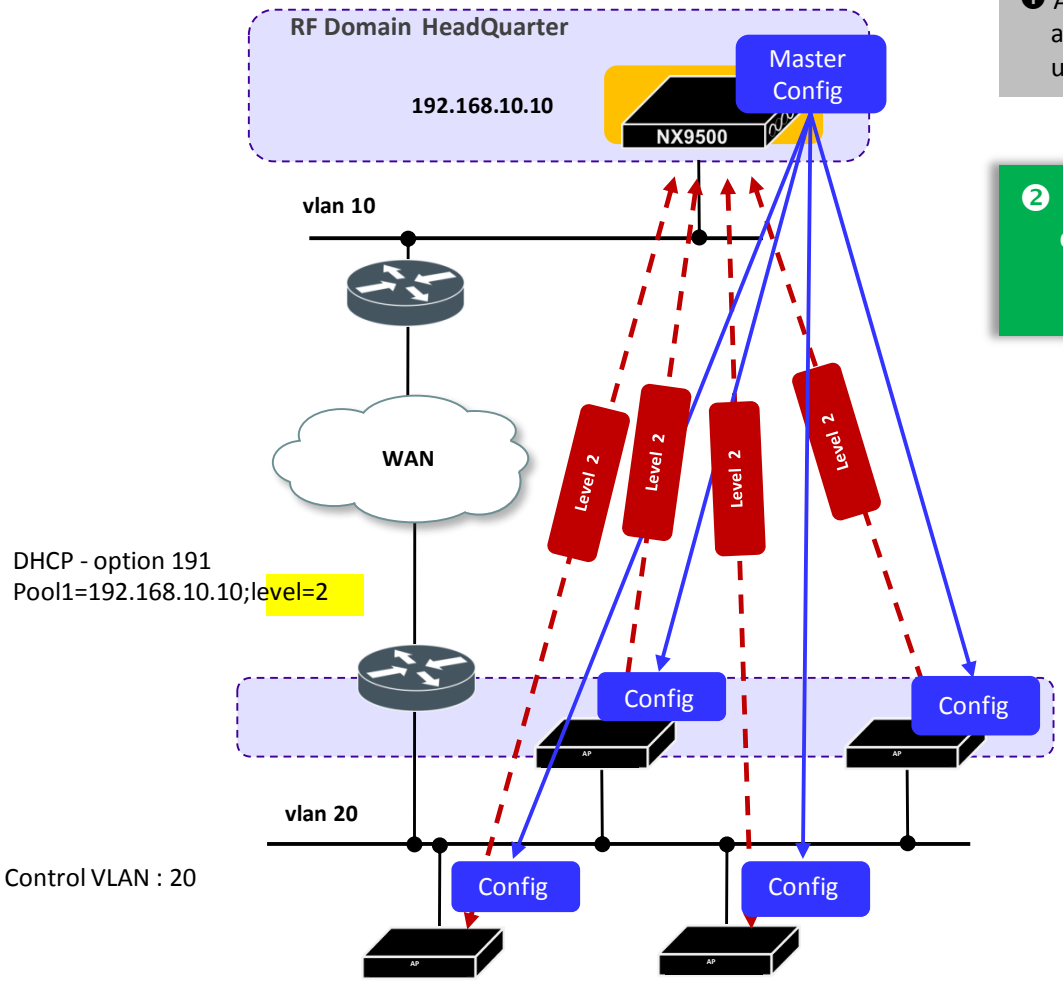
- How MINT Level 2 works



❶ Access Points on the Remote RF Domain are ***« level 2 » adopted*** by NX controller using the DHCP option 191

MiNT Protocol in a NOC model deployment – Step 2

- How MINT Level 2 works

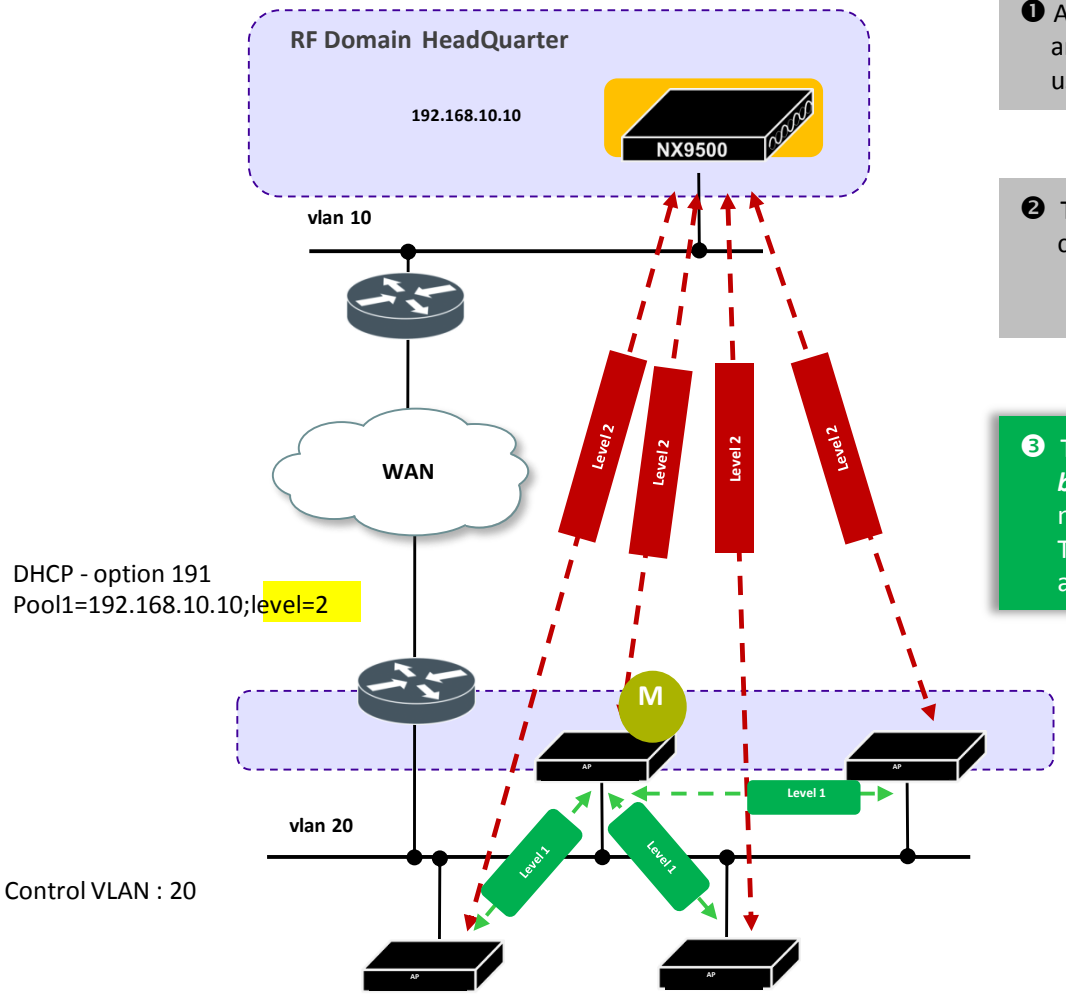


❶ Access Points on the Remote RF Domain are ***« level 2 » adopted*** by NX controller using the DHCP option 191

❷ The access points receive their configuration from the NX controller:
- ► Profile & Associated Policies
- ► RF Domain

MiNT Protocol in a NOC model deployment – Step 3

- How MINT Level 2 works



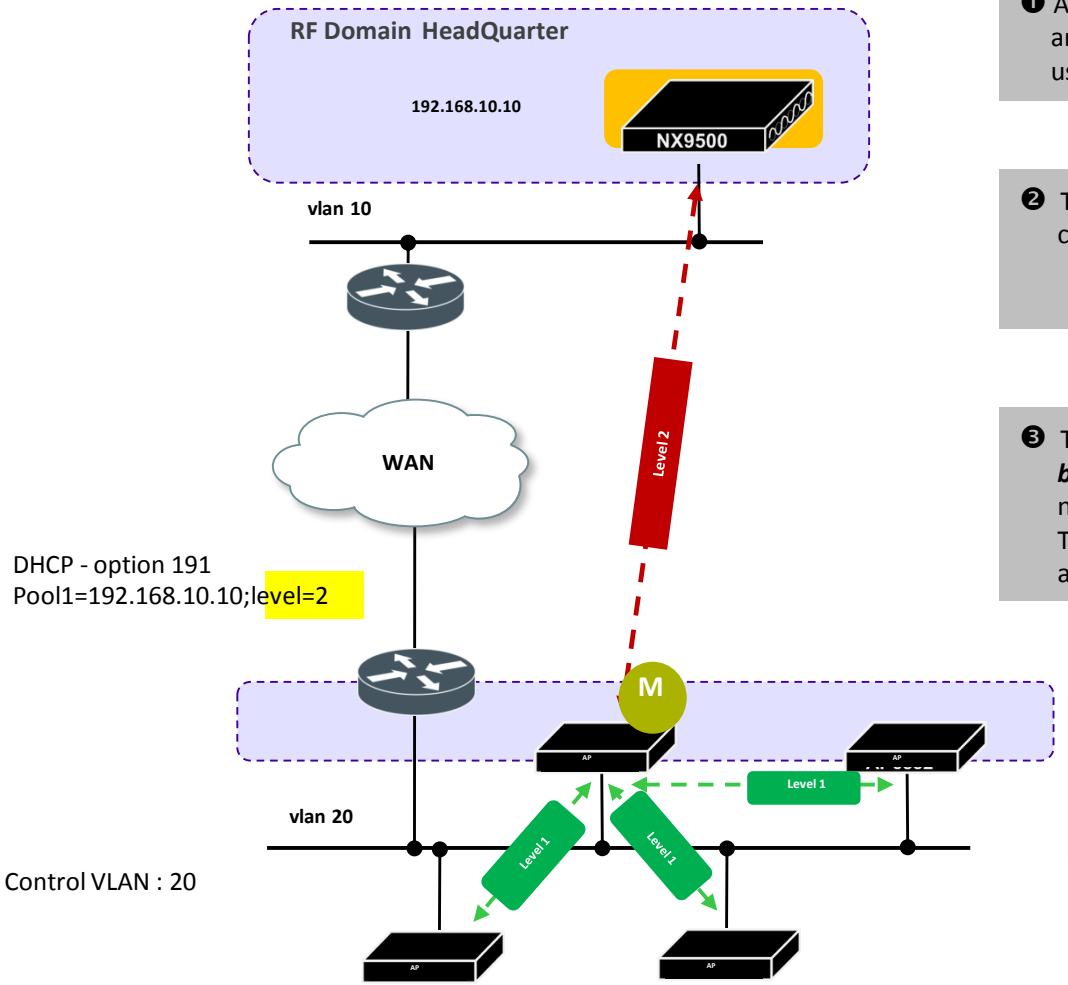
❶ Access Points on the Remote RF Domain are ***« level 2 » adopted*** by NX controller using the DHCP option 191

❷ The access points receive their configuration from the NX controller:
- ► Profile & Associated Policies
- ► RF Domain

❸ The access points establish a ***Level 1 VLAN based MINT link*** to discover all the neighboring access points at the remote site
The access points then elect one of the access points as the ***RF Domain Manager***

MiNT Protocol in a NOC model deployment – Step 4

- How MINT Level 2 works



❶ Access Points on the Remote RF Domain are ***« level 2 » adopted*** by NX controller using the DHCP option 191

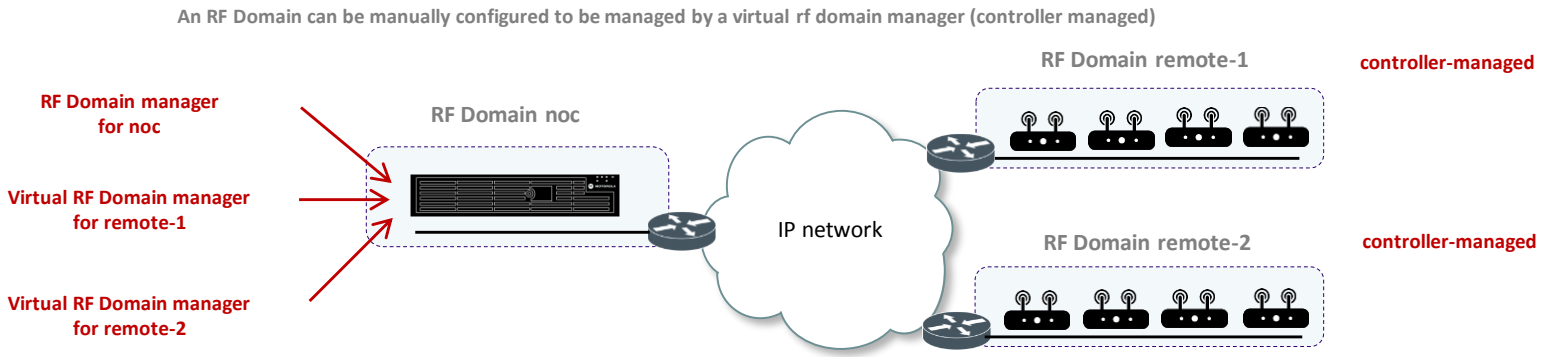
❷ The access points receive their configuration from the NX controller:
- ► Profile & Associated Policies
- ► RF Domain

❸ The access points establish a ***Level 1 VLAN based MINT link*** to discover all the neighboring access points at the remote site The access points then elect one of the access points as the ***RF Domain Manager***

❹ All the Access Points except the elected RF Domain Manager close their Level 2 IP based MINT links to their NX Controller at the Headquarter. They keep MiNT Level 1 at layer 2 to their neighbors

Virtual RF Domain Manager

WiNG concept of «Virtual RF Domain Manager» as Campus solution for large HQ locations



- *Virtual RF Domain Manager should be used for particular cases only:*
  - ⇨ *Where remote RF Domain contains more than 256 high tier APs with no local controller*
  - ⇨ *Where remote RF Domain contains more than 24 single radio access points with no local controller*
  - ⇨ *Where high bandwidth LAN links are existing between Virtual RF Domain manager and remote RF Domain (no WAN links with limited bandwidth)*

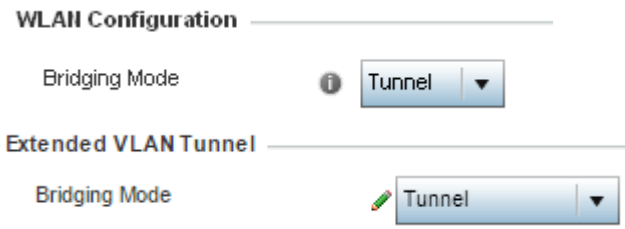
Number of RF Domains controlled by « Virtual RF Domain Manager » varies by platform model

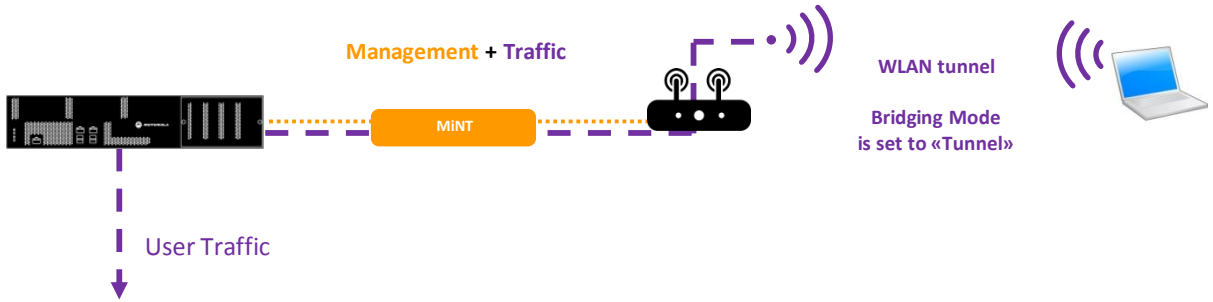
	VX9000	NX 95XX	NX75XX	NX5500	RFS6000	RFS4000
Multiple RF Domains Manager Capacity	200	200	40	20	5	2

WiNG: tunnel or local bridging mode WLANs ?

- Bridging Mode: «Tunnel» or «Local»?

Bridging Mode = Tunnel

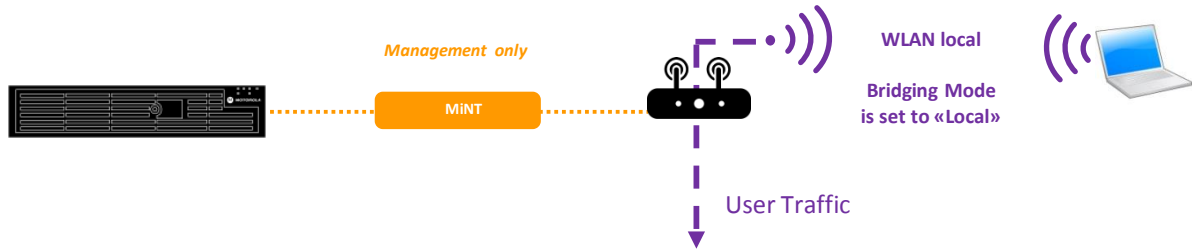




When bridging mode is set to «Tunnel», wireless LAN users traffic is tunneled from AP to the Wireless controller

Note: There is no traffic tunneling support on the NX9000 / NX9500 , VX9000 platforms (no dataplane)

Bridging Mode = Local



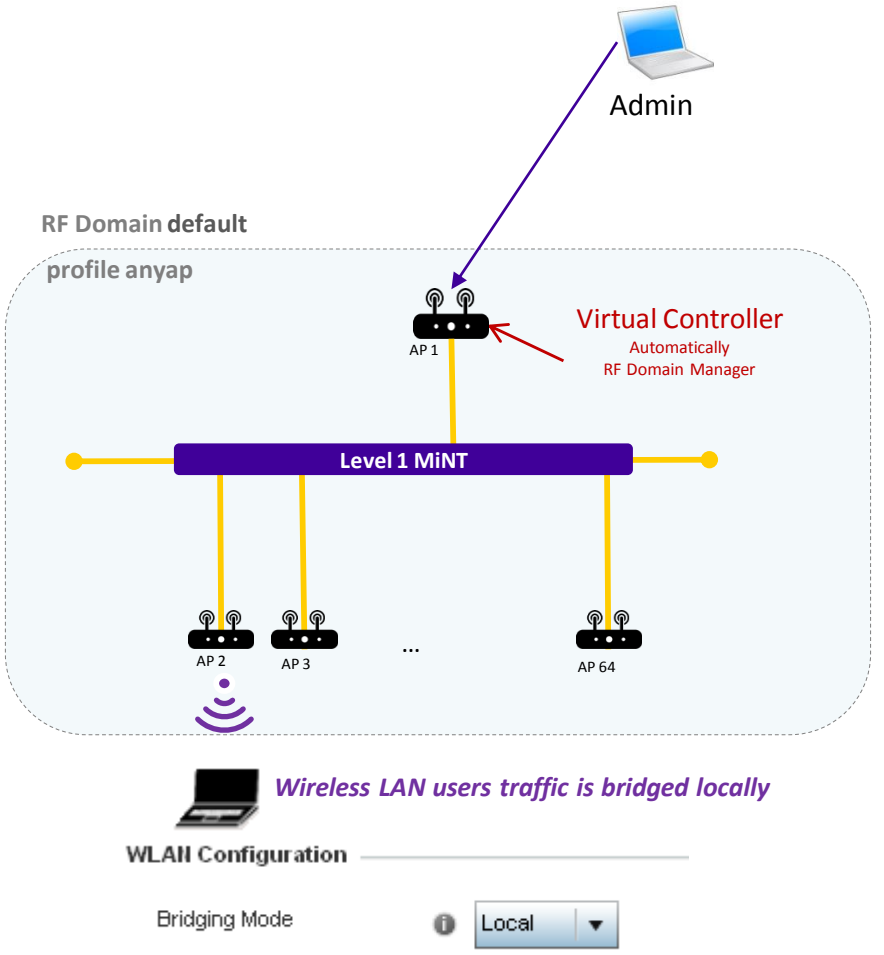
When bridging mode is set to «Local», traffic is locally switched by the AP

Do NOT use same VLAN as locally bridged and tunneled as this will introduce network loops!

MINT Level 1 usage – AP set as Virtual Controller.

- AP in Virtual Controller mode

- Single RF Domain
- Local Bridging
- Heterogeneous VC management is supported for 8432 and 8533
- Same AP family management supported for 7522/32/62 and 7612/32/62
- Other APs only same AP model management
- VC redundancy with Dynamic VC feature
- Max 64AP (24 AP with 802.11n APs)
- Level 1 VLAN MiNT links (default)



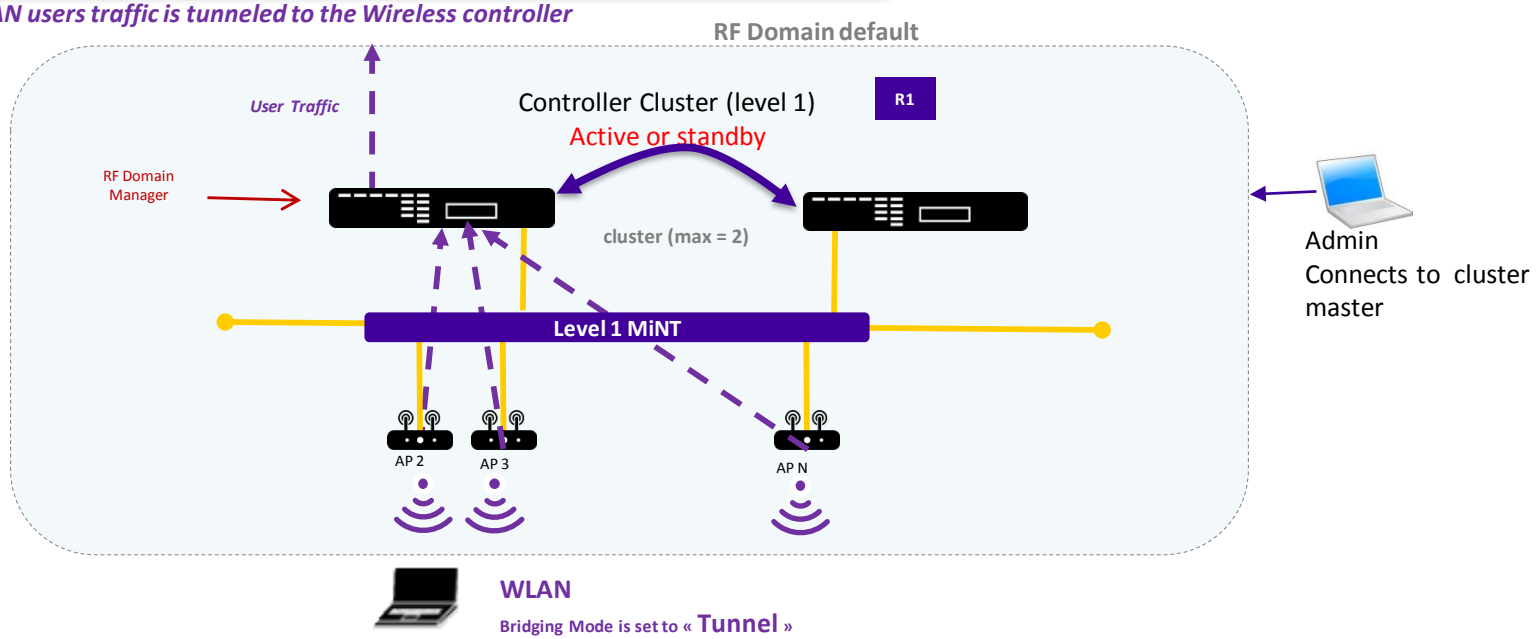
MINT Level 1 usage – WLAN mode tunnel

- Small/Medium Campus architecture – Tunneled / Mixed traffic forwarding

• Single RF Domain • WLAN bridging mode = Tunnel • Level 1 MiNT links (default)	Recommended *	NX75xx - 512 AP NX5500 – 256 AP
		NX9510 - 512 AP NX9610 - 512 AP

➢No more than 500 AP** should be deployed with MiNT L1 architecture
MiNT routing table is shared across all AP with MiNT L1

Wireless LAN users traffic is tunneled to the Wireless controller



** Recommended values are provided as design guidelines ONLY. Officially supported numbers (check Release Notes) can be different.*

*** with Dual Radios Access Points ONLY. No more than 256 single radio APs should be deployed in one Level1 MiNT domain*

MINT Level 1 usage – Small Campus architecture

- Small/Medium Campus architecture – Local Bridging

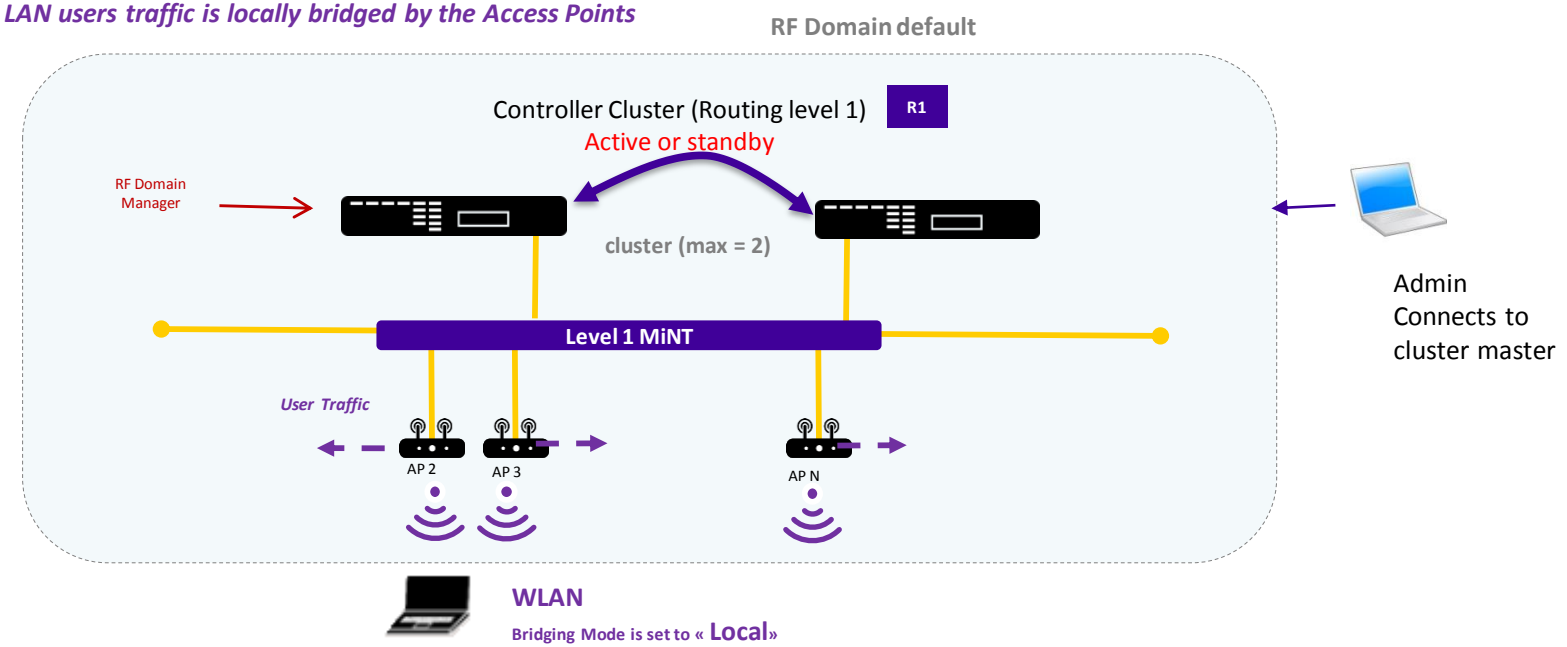
•Single RF Domain
• WLAN bridging mode = Local
• Level 1 MiNT links (default)

Recommended * RFS4000 - 144 AP
NX75xx - 512 AP **
VX9000 – 512 AP **

NX55xx - 512 AP
NX95xx - 512 AP **
NX96xx - 512 AP **

➢No more than 512 APs can be deployed with MiNT L1 architecture
MiNT routing table is shared accross all AP with MiNT L1

Wireless LAN users traffic is locally bridged by the Access Points

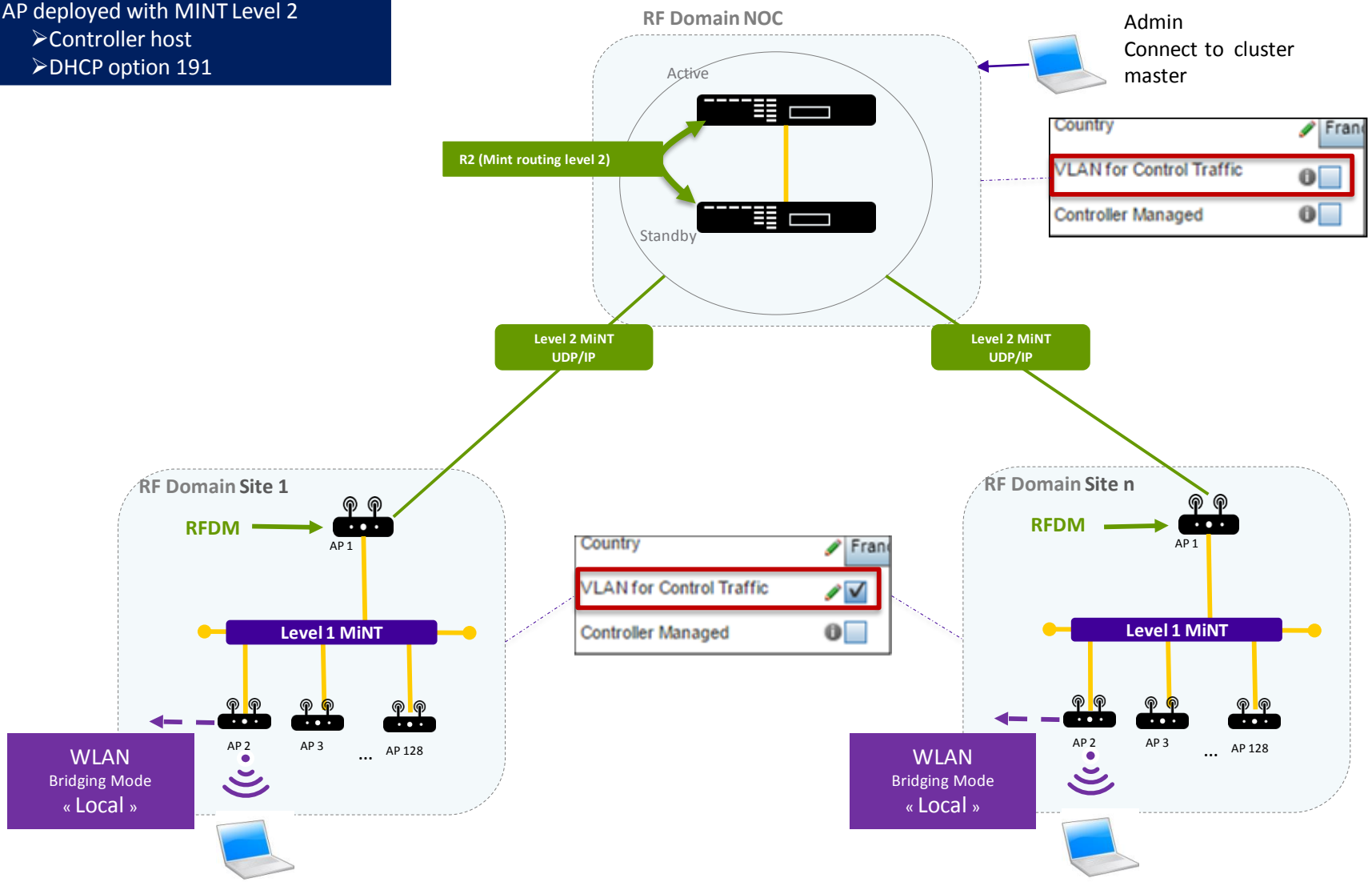


* *Recommended values are provided as design guidelines ONLY. Officially supported numbers (check Release Notes) can be different.*

** *with Dual Radios Access Points ONLY. No more than 256 single radio APs should be deployed in one Level1 MiNT domain*

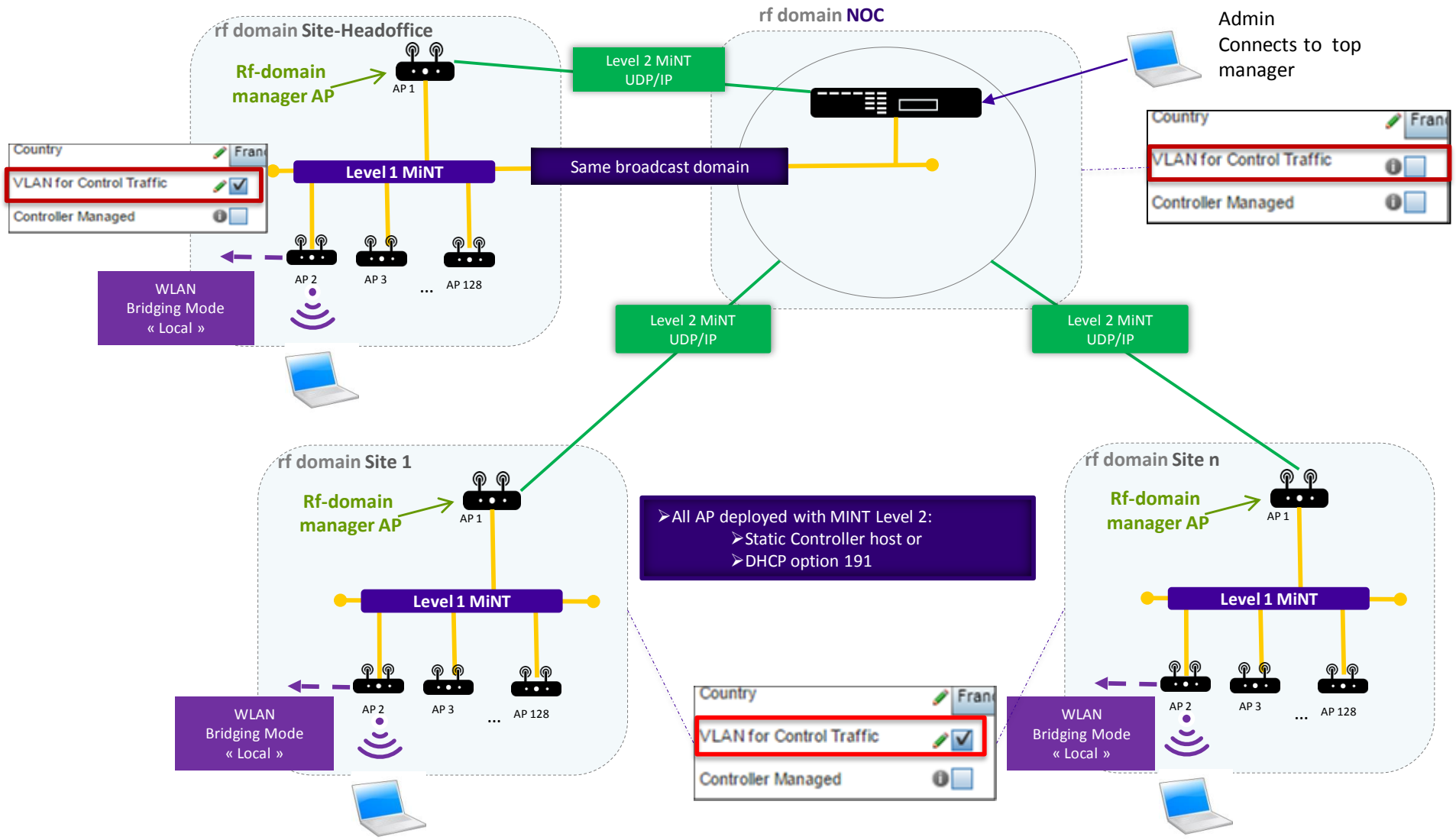
MINT L2 usage – Multi Site Centralized deploiyment

- All AP deployed with MINT Level 2
  - Controller host
  - DHCP option 191



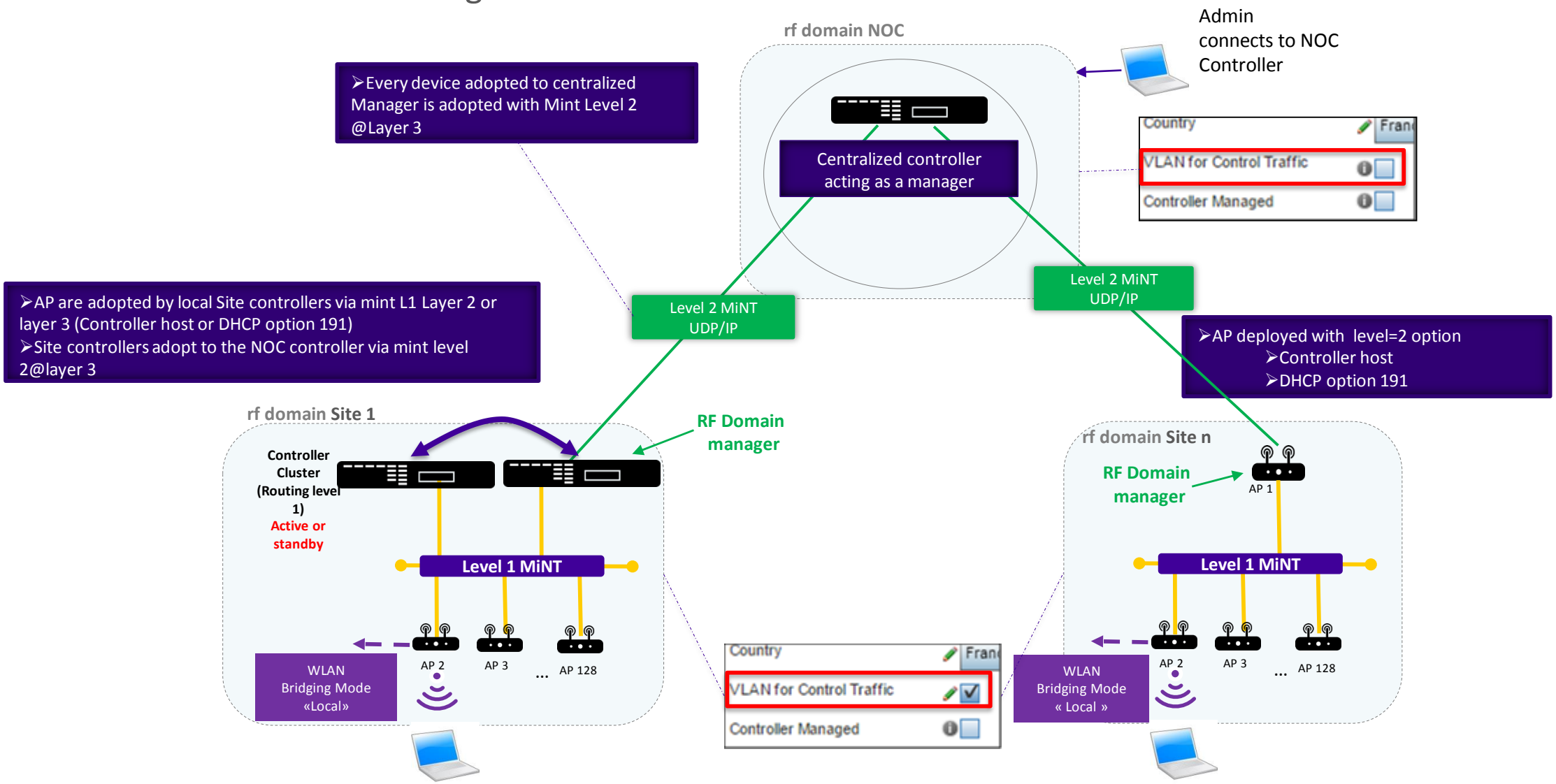
MINT L2 usage – Multi Site centralized deployment variation

APs can be in same network as NOC controller



MINT Level 2 usage – Multi Site Hierarchical Management

- Multi Site Hierarchical Management with Site Controllers

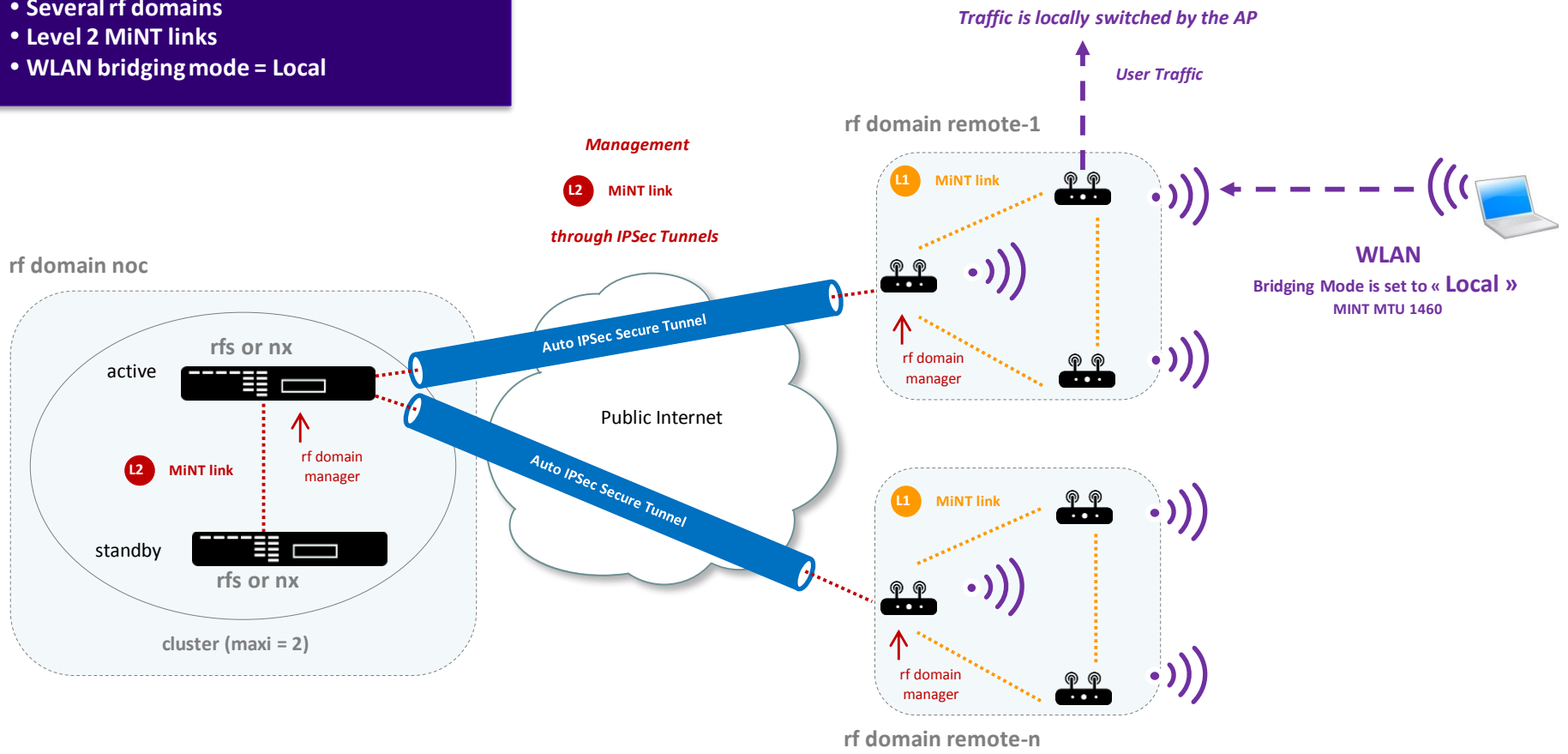


A Site Controller CANNOT adopt other Controllers and itself be adopted
AAP licenses are used to adopt both Access Points and Site Controllers

WiNG 5 Architecture with remote sites over unsecured network

2.2

- Several rf domains
- Level 2 MiNT links
- WLAN bridging mode = Local



IPSec Tunnels Maximum	RFS4000 - 256 Tunnels	NX5500 - 512 NX75xx - 1000 Base / 2000(Adv sec) NX9510 - 1.000 (Base) / 8.000 (Adv Sec)

Note: There is no IPSec VPN support:
- with VX9000
- with single radio Access Points

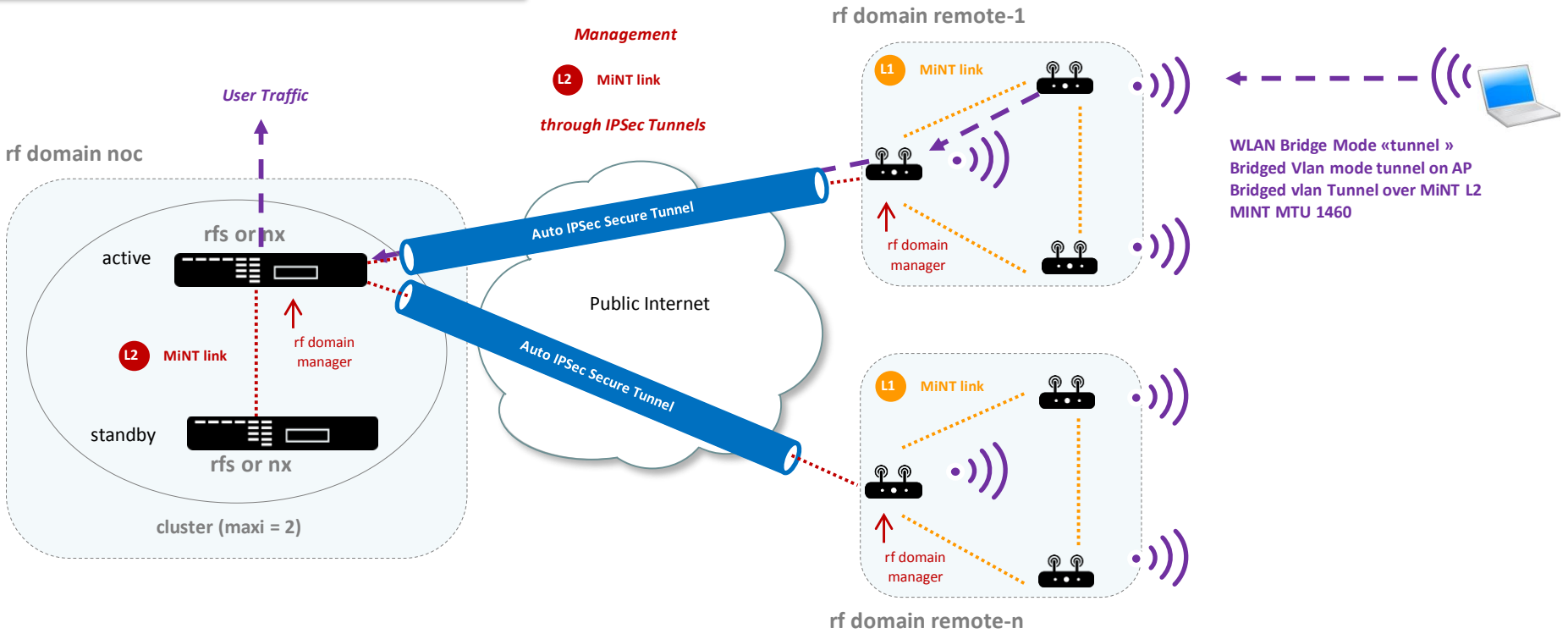
WiNG 5 Architecture with remote sites over unsecured network

2.2a

With MiNT tunnels

- Several rf domains
- Level 2 MiNT links
- WLAN bridging mode = Tunnel

Traffic is tunneled in MiNT to controller



IPSec+MiNT Tunnels Maximum	RFS4000 - 36 Tunnels NX5500 - 256 Tunnels NX75xx - 1024 Tunnels NX9510 - 4096 Tunnels

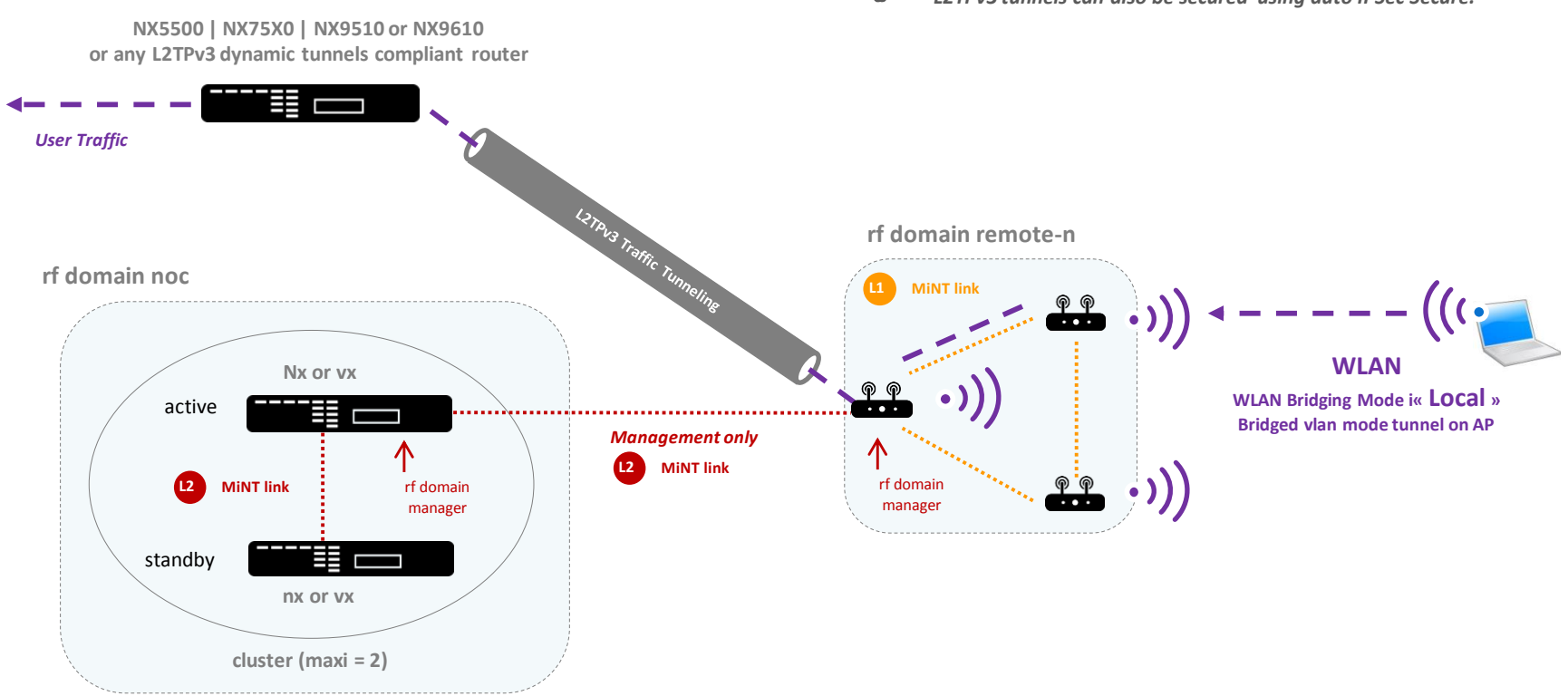
Note: There is no IPSec VPN support:
- with VX9000 platforms
- with single radio Access Points

WiNG 5 Architecture with remote sites & traffic tunneling 2.3

L2TPv3 Standard Protocol is used for Traffic Tunneling

Several criteria are available for L2TPv3 tunnels establishment. Please refer to the L2TPv3 How-To-Guide for details.

L2TPv3 tunnels can also be secured using auto IPSec Secure.



L2TPv3 Dynamic Tunnels	RFS4000 - 63 Tunnels
	NX5500 - 256 Tunnels
	NX75xx - 2000 Tunnels
Maximum	NX9510 - 16.383 Tunnels

WiNG Quick Start Guide
Part 2 – Configuration Steps

Extreme®
Connect Beyond the Network

WiNG 5 – Quick Start Guide

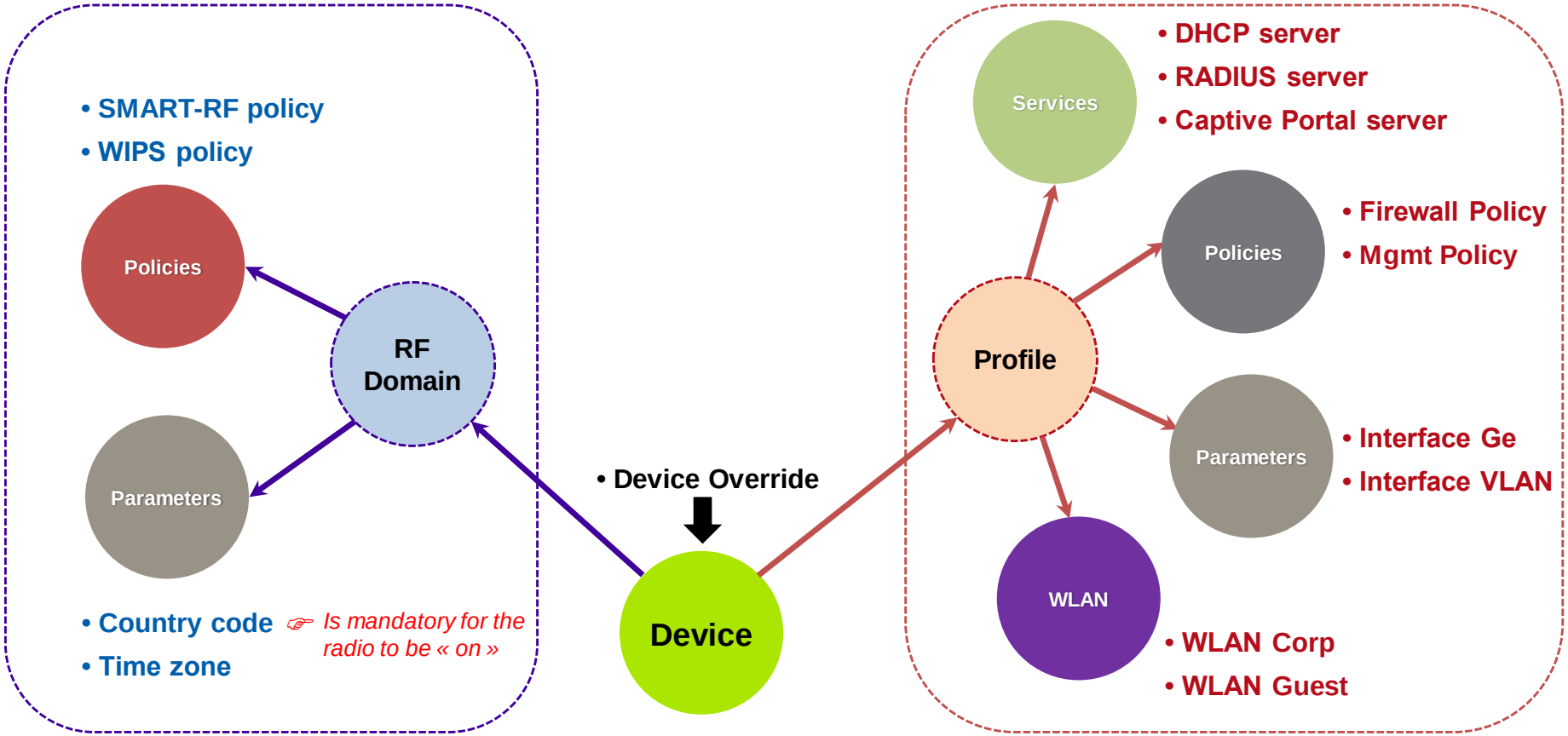
Understanding WiNG 5 Concepts and Configuring the main Features

- WiNG 5 Key Concepts
- DHCP Server (Distributed)
- DHCP Server (Centralized)
- Provisioning Policy
- WLAN with PSK security
- WLAN with 802.1x Authentication (Internal RADIUS)
- Captive Portal (Centralized)
- Captive Portal (Distributed)
- Captive Portal (MAC Registration)
- Level 2 MiNT architecture
- AutoIPsec Secure
- L2TPv3 Tunneling
- Clustering
- Mesh Legacy
- MeshConnex ™

☞ *Note: This document describes the main steps for configuring most used features.*
For advanced configurations, please refer to the How-To-Guide documents available for each topic.

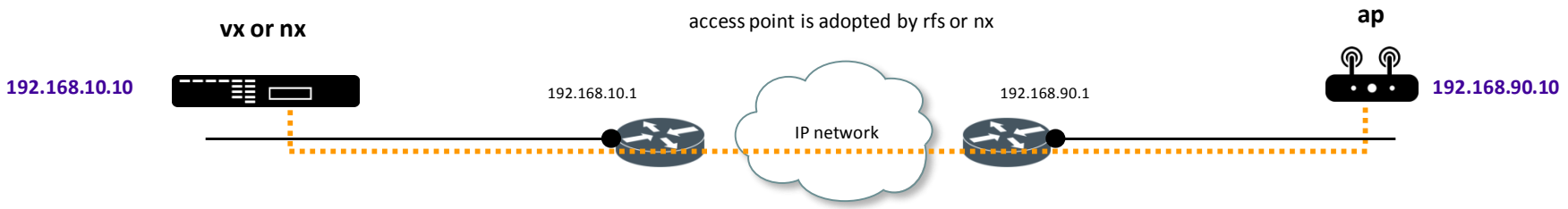
WiNG 5 – Quick Start Guide

- Key Concepts
  - WiNG 5 provides a ***hierarchical configuration model*** that allows enterprises to manage large number of devices from a single point of management.
  - Each physical device (AP, RFS or NX or VX) is assigned to one ***RF-Domain*** and one ***Profile***



WiNG 5 – Quick Start Guide

- Configuring a DHCP Service (Distributed on Access Point)



1 Set a Virtual Interface on AP

Configuration > Devices > ap > Interface > Virtual Interfaces

- Add
  - VLAN = 90
  - IP addresses / Primary IP address = 192.168.90.10/24

2 Create a DHCP Server Policy

Configuration > Services > DHCP Server Policy > Add

- DHCP Server Policy
  - DHCP Server Policy Name = dhcp_srv_on_ap
- DHCP Pool
  - DHCP Pool Name = subnet_90
    - Subnet = 192.168.90.0/24
    - Lease Time = 86400
    - Default routers = 192.168.90.1
    - DNS Servers = 8.8.8.8
    - IP address ranges = 192.168.90.100 to 192.168.90.200

3 Statistics

- *Check if your DHCP server is running*

Statistics > Select your ap > DHCP Server > General

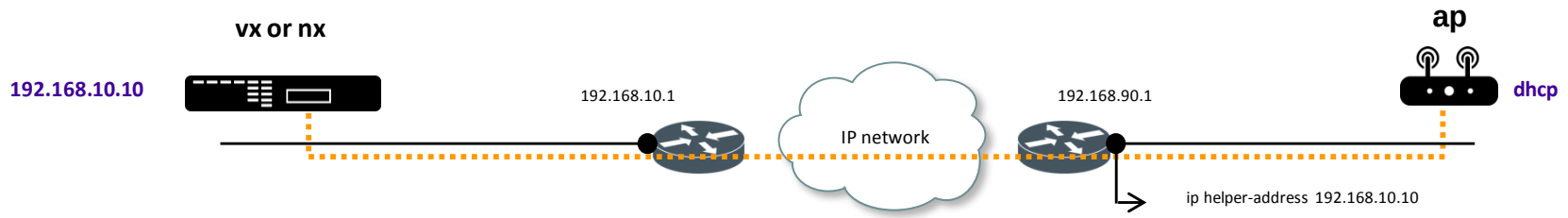
2b Assign the DHCP Server Policy to the device (ap)

Configuration > Devices > ap > Services > DHCP Server

☞ *Note: In this configuration, the DHCP service for the IP Subnet can be « running » on a device if this device owns a Virtual Interface in this IP Subnet.*

WiNG 5 – Quick Start Guide

- Configuring a DHCP Service (Centralized on RFS)



1 Virtual Interface on the controller

Configuration > Devices > <Controller> > Interface > Virtual Interfaces

- Add
  - VLAN = 10
  - IP addresses
    - Primary IP address = 192.168.10.10/24
  - DHCP Relay
    - Respond to DHCP Relay Packets ☑

2b Assign the DHCP Server Policy to the device (rfs)

Configuration > Devices > controller > Services > DHCP Server

3 Statistics

- *Check if your DHCP server is running*

Statistics > Select your RFS > DHCP Server > General

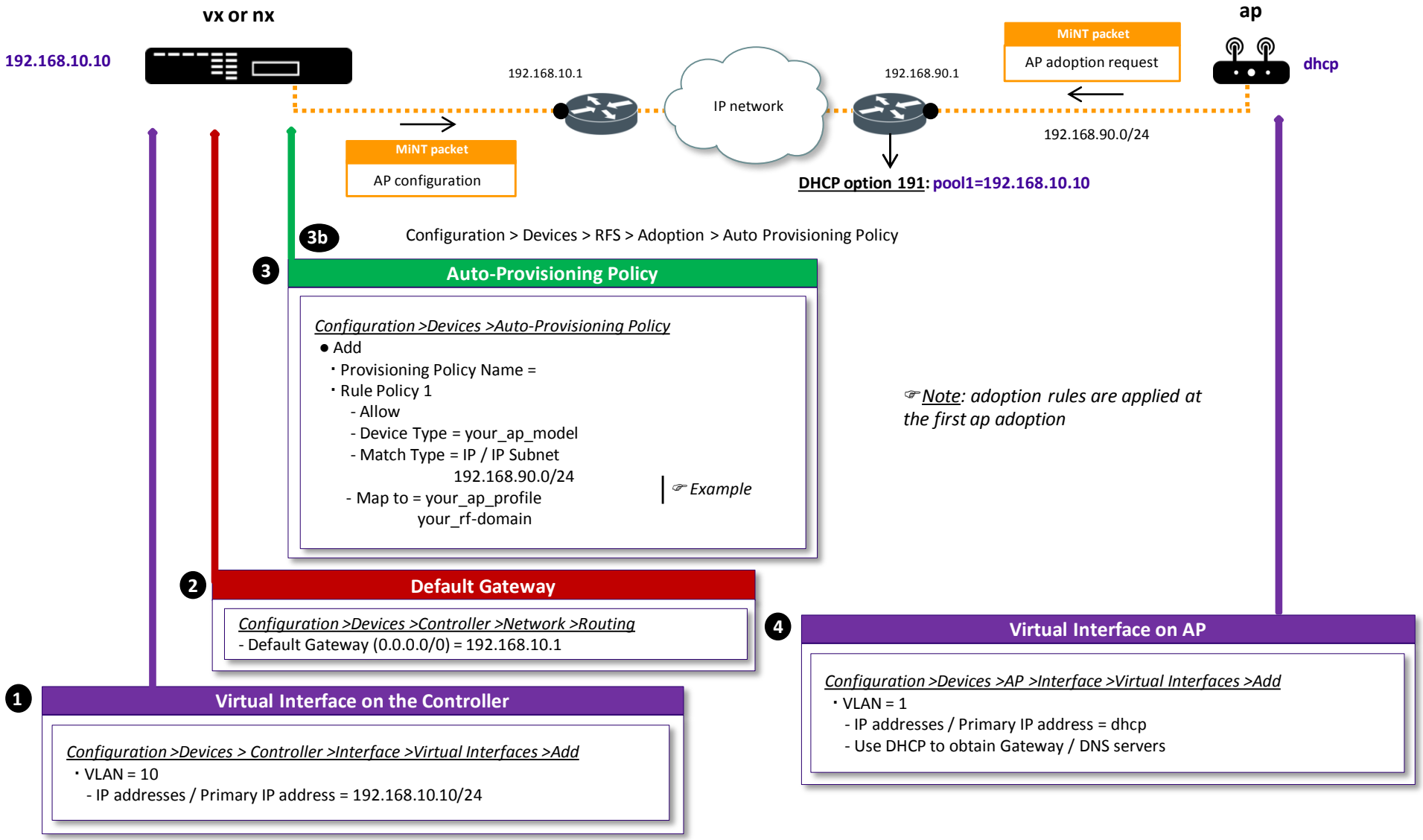
2 Create a DHCP Server Policy

Configuration > Services > DHCP Server Policy > Add

- DHCP Server Policy
  - DHCP Server Policy Name = dhcp_srv_on_rfs
- Global Settings > Add Row
  - Name = option191
  - Type = ASCII
  - Code = 191
- DHCP Pool > Add
  - DHCP Pool Name = pool_90
  - Basic Settings
    - Subnet = 192.168.90.0/24
    - DNS Servers = 8.8.8.8
    - Lease Time = 86400
    - Default routers = 192.168.90.1
    - IP address ranges = 192.168.90.100 to 192.168.90.200
  - Advanced
    - DHCP Options Values > Add Row
      Global DHCP Option Name = option191
      Value = pool1=192.168.10.10

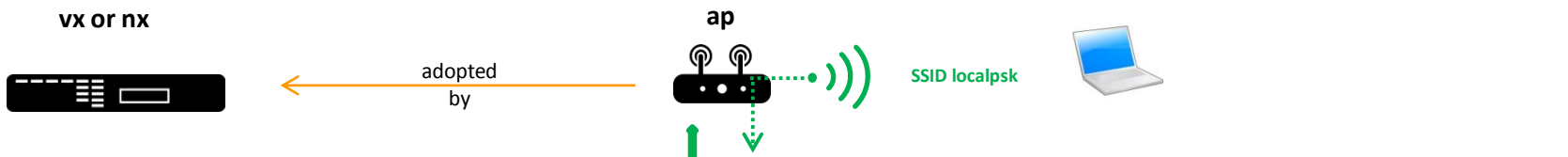
WiNG 5 – Quick Start Guide

- Auto Provisioning Policy (aka Adoption Rules)



WiNG 5 – Quick Start Guide

- WLAN with PSK security



When bridging mode is set to « local », traffic is locally switched by the AP

1b Configuration > Device > AP > Interface > Radio > Radio 1 > WLAN Mapping

1 Wireless LAN

Configuration > Wireless > Wireless LANs

- Basic Configuration
  - WLAN Name = localpsk
  - SSID Name = localpsk
  - Bridging Mode = Local
- Security
  - Select Authentication = PSK / None
  - Select Encryption = WPA2-CCMP
  - Pre Shared Key = 12345678

2 Statistics

- *Check if your radio state is « on »*

Statistics > Select your AP > Radio > Status

- *Check if your WLAN is « Advertised »*

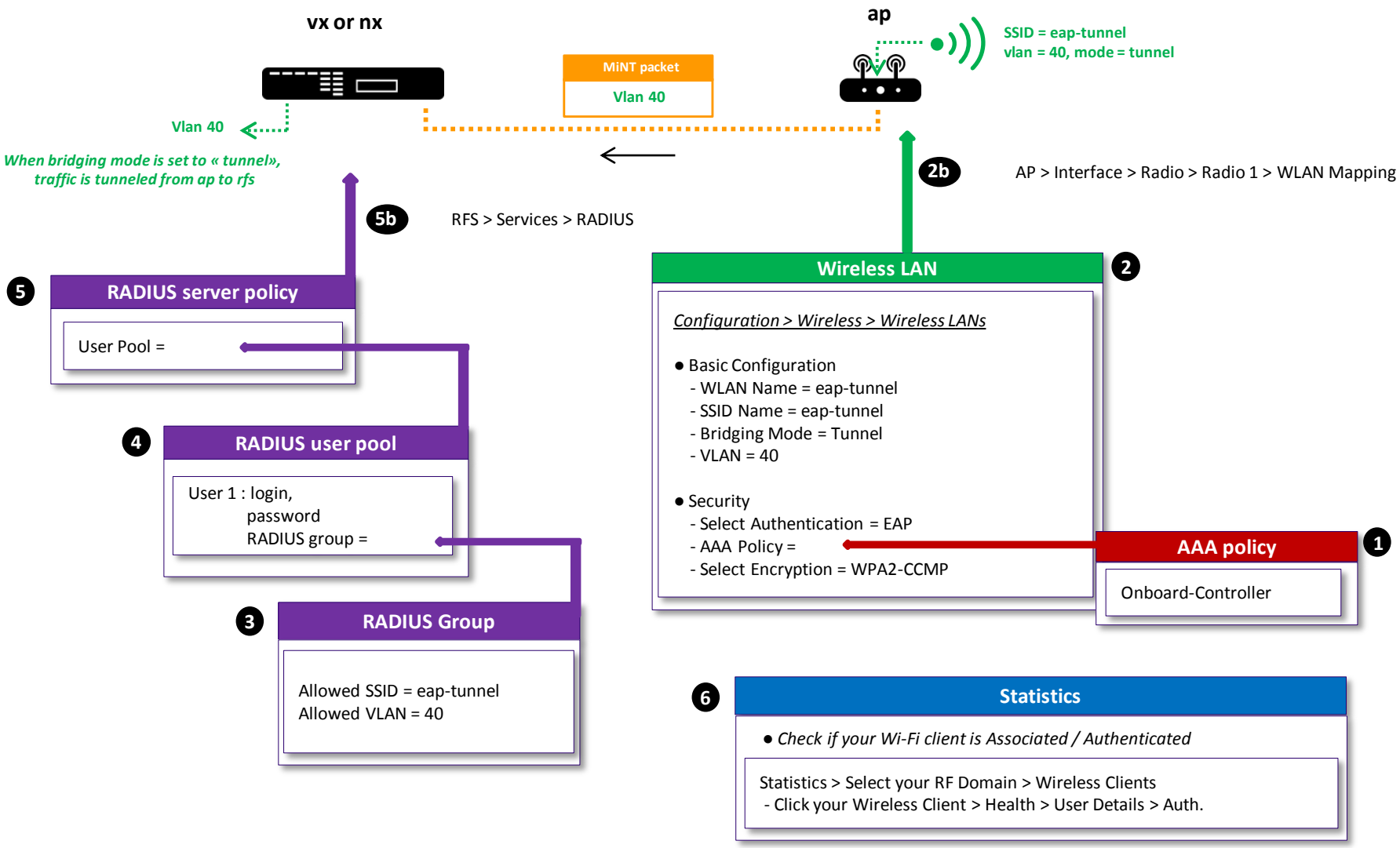
Statistics > Select your AP > Radio > Status
- Click on the apxxxx:R1 or apxxxx:R2
- Select « Wireless LANs »

- *Check if your Wi-Fi client is associated*

Statistics > Select your RF Domain > Wireless Clients

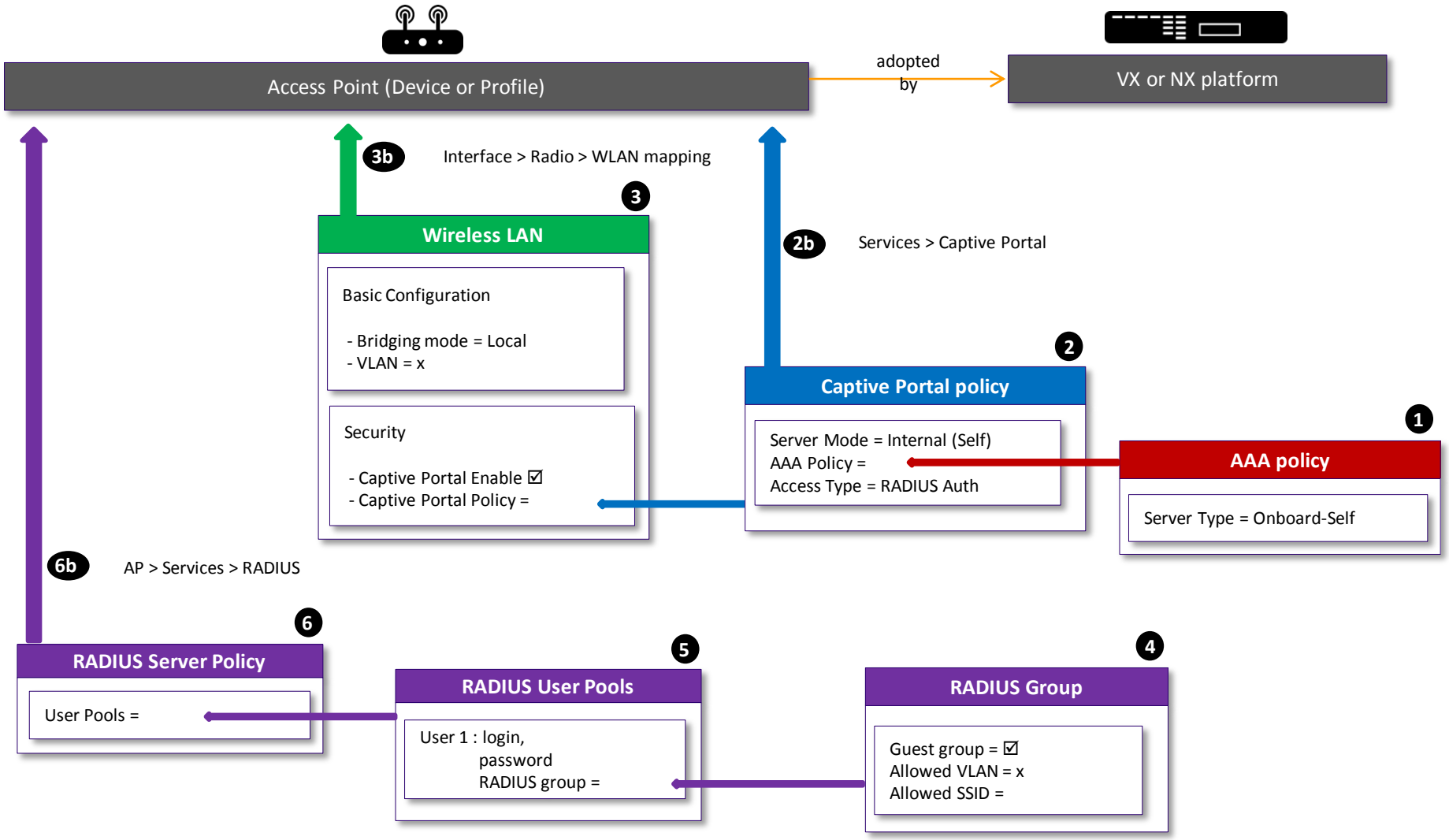
WiNG 5 – Quick Start Guide

- WLAN with Internal RADIUS Authentication (EAP-PEAP)



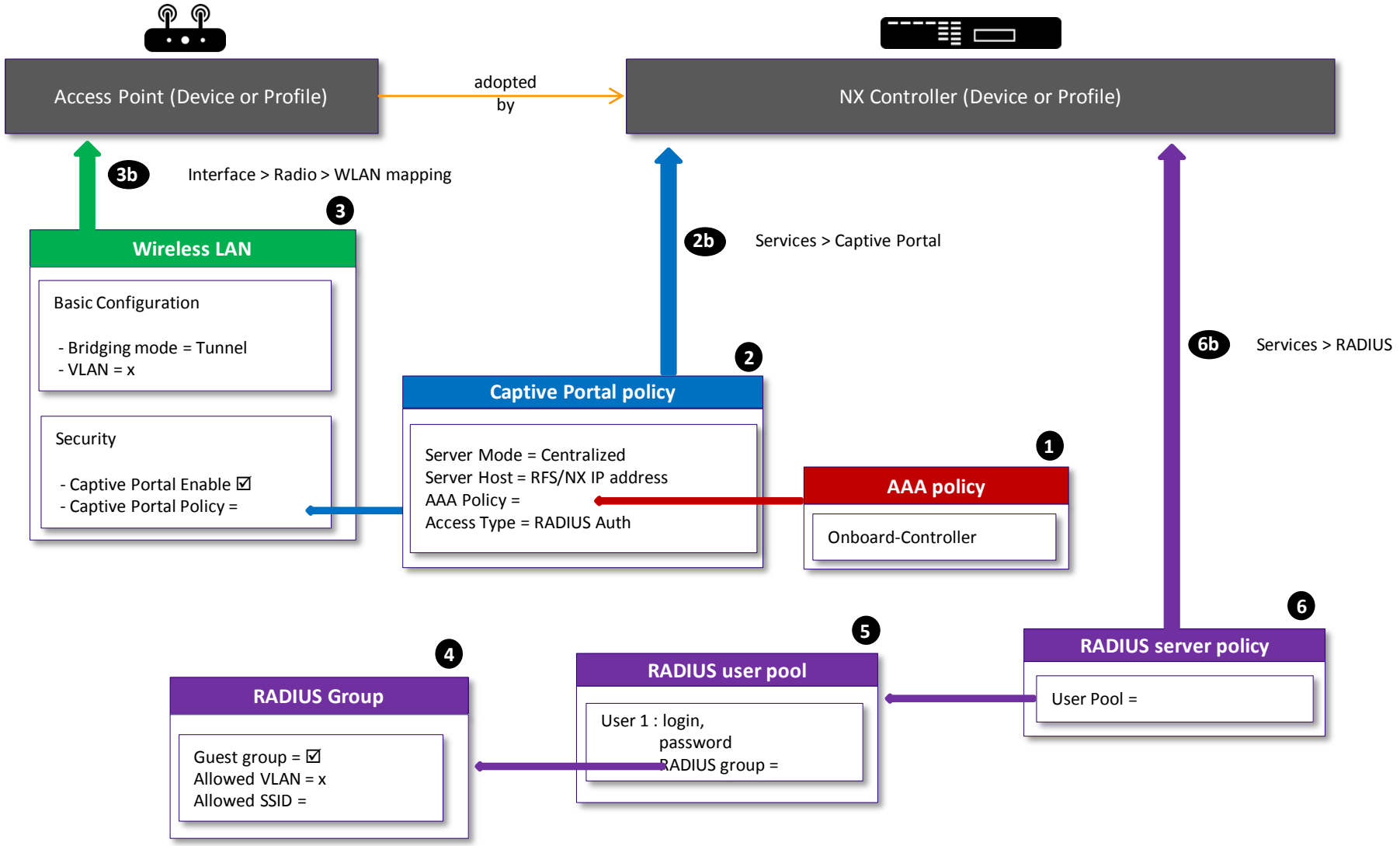
WiNG 5 – Quick Start Guide

- Captive Portal (Distributed) - RADIUS Authentication



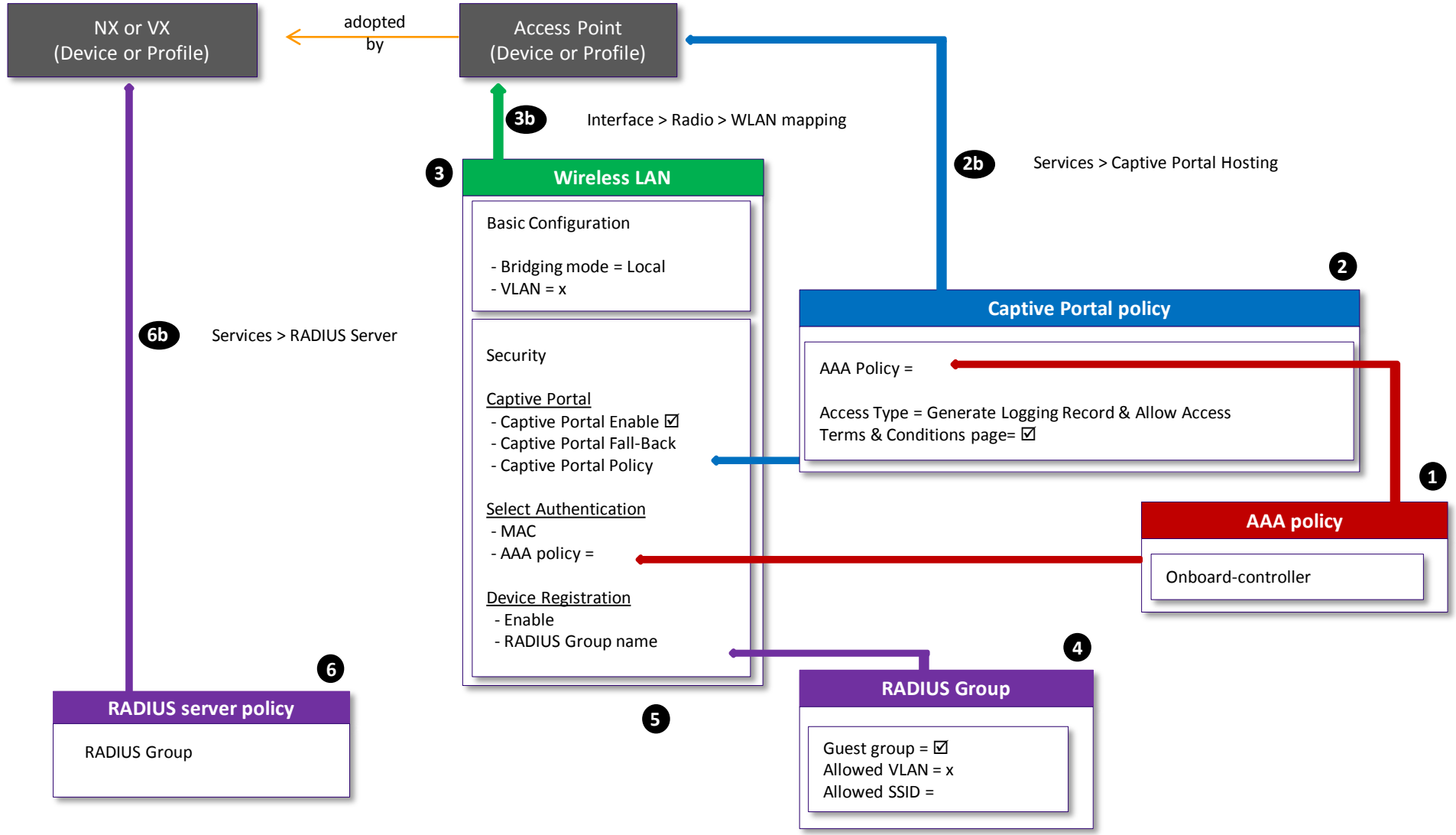
WiNG 5 – Quick Start Guide

- Captive Portal (Centralized) - RADIUS Authentication



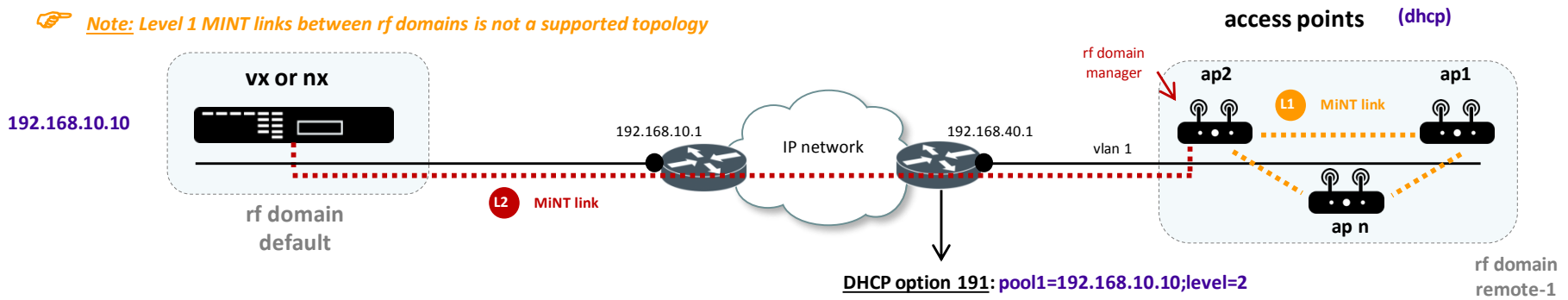
WiNG 5 – Quick Start Guide

- Onboard Self Guest Registration (VX9000 or NX9XX0)



WiNG 5 – Quick Start Guide

- Configuring a level 2 MiNT link architecture



1 RF Domain

Configuration > RF Domain > Add

- RF Domain name = remote-1
- Time Zone = GMT+01:00
- Country = France-fr
- VLAN for Control Traffic ☑ = 1

2 Assign remote APs to created RF Domain

Configuration > Device > ap1 > Edit

- Basic Configuration > RF Domain
  - RF Domain Name = remote-1

Configuration > Device > ap2 > Edit

- Basic Configuration > RF Domain
  - RF Domain Name = remote-1

3 Statistics

- *Check if all access points are assigned to the remote rf domain*

Statistics > remote-1 > Devices
ap1, ap2, ap n should be displayed

- *Check which ap is automatically elected « RF Domain Manager »*

Statistics > remote-1 > Health > Domain
RF Domain Manager = ap2 (example)

☞ *Note: The « VLAN for Control Traffic » configured in the RF Domain is used to establish level 1 MiNT links between APs in the remote rf domain.*

☞ *Note: The AP elected « RF Domain Manager » keeps established a single level 2 MiNT link between the remote rf domain and the management platform.*

WiNG 5 – Quick Start Guide

- Auto IPSec Secure

1 Configure IPSec Secure on RFS

Configuration > Device > Controller > Security > AutoIPSec Tunnel

- GroupID= your_id_name
- Authentication Type = PSK
- Authentication Key = 12345678
- IKE version = ikev2 (default)

2 Configure IPSec Secure on Access Point

Configuration > Device > AP > Security > AutoIPSec Tunnel

- GroupID= your_id_name
- Authentication Type = PSK
- Authentication Key = 12345678
- IKE version = ikev2 (default)

3 Configure Adoption with IPSec Secure on Access Point

Configuration > Device > AP > Adoption > Controller Hostnames

- Host (IP address) = rfs-ip-address
- Pool = 1 (default)
- Routing Level = 1 or 2
- IPSec Secure = Yes ☑

4 Statistics

- *Check adoption status*

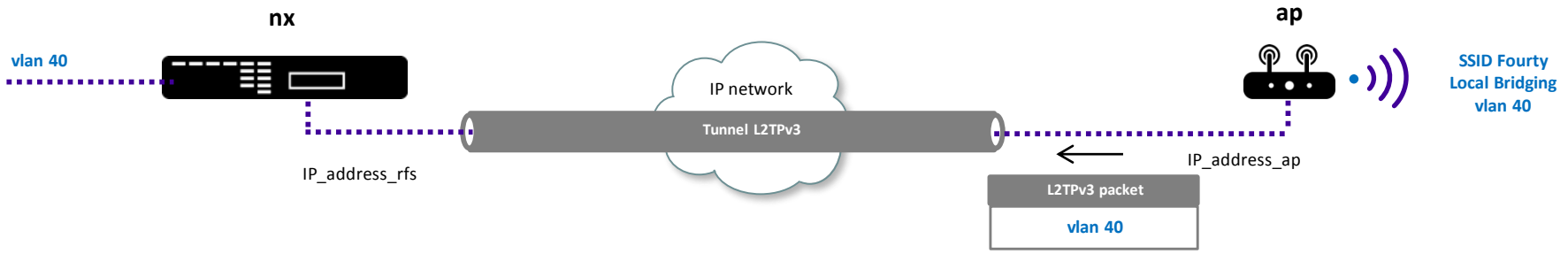
Statistics > Controller > Adoption > Adopted APs
Status = configured

- *Check AutoIPSec Secure*

Statistics > Controller > VPN > IKESA
State = established
Statistics > RFS > VPN > IPSec
State = VALID / Mode = Tunnel

WiNG 5 – Quick Start Guide

- Tunneling data via L2TPv3



1 Configure L2TPv3 on RFS

Configuration > Device > Controller > Network > L2TPv3

- General
  - Hostame = rfs

- L2TPv3 Tunnels > Add
  - Settings
    - Name = vlan40
    - Use Tunnel Policy = default
  - Peer > Add Row
    - Router ID = any
  - Session > Add Row
    - Name = Session40
    - Pseudowire = 40
    - Traffic source type = VLAN
    - Traffic source value = 40

2 Configure L2TPv3 on Access Point

Configuration > Device > AP > Network > L2TPv3

- General
  - Hostame =

- L2TPv3 Tunnels > Add
  - Settings
    - Name = vlan40
    - Use Tunnel Policy = default
  - Peer > Add Row
    - Peer IP address = IP_address_RFS
    - Hostname = rfs
    - Router ID = any
  - Session > Add Row
    - Name = Session40
    - Pseudowire = 40
    - Traffic source type = VLAN
    - Traffic source value = 40

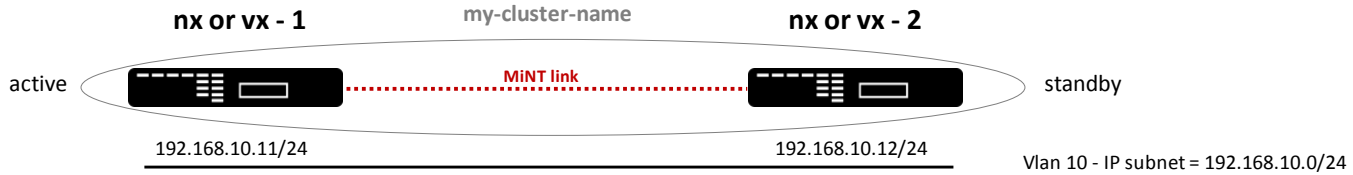
3 Statistics

- *Check L2TPv3 status* — *Statistics > Controller > L2TPv3 tunnels* Local = IP_address_rfs, Peer = IP_address_ap, Tunnel State = established

WiNG 5 – Quick Start Guide

- Establishing a Cluster using CLI and the « join-cluster » command

☞ *Only two (2) controllers in a cluster are supported*



1 Set a Virtual Interface on platform 1

- *Connect to platform 1 (via port Console or SSH or Telnet) and enter the Config Mode – at the Device level*

nx-1(config-device)#interface vlan 10
nx-1(config-device-if-vlan10)#ip address 192.168.10.11/24

3 Set a Virtual Interface on platform 2

- *Connect to platform 2 (via port Console or SSH or Telnet) and enter the Config Mode – at the Device level*

nx-2(config-device)#interface vlan 10
nx-2(config-device-if-vlan10)#ip address 192.168.10.12/24

2 Configure Cluster Settings on platform 1

- *Connect to platform 1 (via port Console or SSH or Telnet) and enter the Config Mode – at the Device level*

nx-1(config-device)#cluster name <my-cluster-name>
nx-1(config-device)#cluster mode <active>
nx-1(config-device)#cluster master-priority <1-255>

☞ *Note: Higher value has greater precedence* ↗

nx-1(config-device)#cluster member ip <192.168.10.11> level <1/2>
nx-1(config-device)#cluster member ip <192.168.10.12> level <1/2>

4 Establishing cluster using the join-cluster command

- *Connect to platform 2 (via port Console or SSH or Telnet) and enter the Enable Mode – Make sure connectivity to platform 1 is enabled first, then issue the join-cluster command*

nx-2#ping 192.168.10.11

nx-2#join-cluster <192.168.10.11> user <admin> password <superuser-pwd> level <1/2> mode <active/standby>
... connecting to 192.168.10.11
... applying cluster configuration
... committing the changes

5 Statistics

- *Check cluster status using CLI commands*

nx-x#show cluster status
nx-x#show cluster members
nx-x#show cluster configuration

- *Check cluster status using Web UI*

Statistics > cluster name > nx-x > Cluster Peers

WiNG 5 – Quick Start Guide

- MeshConnex ™

Configuration / Security

1 Firewall Policy default

- Denial of Service > Events = Disable All Events
- Advanced Settings > L2 Stateful Packet Inspection > Disable

Configuration / Wireless

2 MeshConnex Policy Add

** Control VLAN should be different from Allowed VLANs*

- Set a MeshPoint name, set a Mesh Id (same as the MeshPoint name)
  Beacon Format= mesh-point, **Do not check the « Is Root » box !**
  Configure the Control VLAN * and the Allowed VLANs *
- Security Tab > set the Security Mode to « PSK », and configure the PreShared Key

Configuration / Profiles

4 Add Root Profile

- Interface > Virtual Interfaces (static or DHCP)
  > Radios > Radio Settings > set RF Mode (2.4/5GHz), Channel= smart, DCS= disable
  set Radio Placement (indoor/outdoor)

  WLAN Mapping/Mesh Mapping Tab > Assign the MeshPoint to the radio
- MeshPoint > Add and Select the MeshConnex policy
  > Settings > is Root= True, Monitor Primary Port Link= Enable ☑
  Path Method= uniform

Assign then the Root Profile to the Root AP(s)

5 Add Non Root Profile

- Interface > Virtual Interfaces (static or DHCP)
  > Radios > Radio Settings > set RF Mode (2.4/5GHz), Channel= smart, DCS= disable
  set Radio Placement (indoor/outdoor)

  WLAN Mapping/Mesh Mapping Tab > Assign the MeshPoint to the radio
- MeshPoint > Add and Select the MeshConnex policy
  > Settings > is Root= False
  Path Method= uniform
- Advanced > Miscellaneous > RF Domain Manager Capable= No

Assign the Non-Root Profile to the Non-Root AP(s)

After commiting and saving, check if the configuration is correctly pushed (show Running Configuration - CLI or GUI) – Then unplug and deploy non-root MeshPoints

Statistics

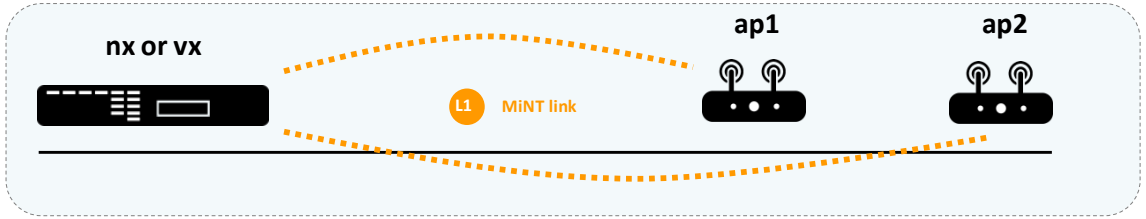
6 Verification

- Select the RF Domain > Statistics > MeshPoint > Select MeshPoint name > MCX Logical View

WiNG 5 Quick Start Guide
Part 3 – Firmware Upgrades

Extreme®
Connect Beyond the Network

Firmware Upgrades – Local Deployments



1 Disable the adopted device automatic firmware upgrade

vx or nx – CLI - configuration Mode
no device-upgrade auto

2 Management platform – firmware upgrading

vx or nx – CLI – enable Mode
upgrade tftp://ip-address/VX9000-5.x.x.x-0xx.img

3 Reload the management platform

vx or nx – CLI – enable Mode
reload

☞ *Note: After reload, adopted devices are now in a « version-mismatch » adoption status*
(show adoption status)

4 Upgrade adopted devices on the unused partition in the rf-domain default using the « no-reboot » option - devices can then be reloaded at a later time

vx or nx – CLI – enable Mode
device-upgrade rf-domain default all from controller no-reboot
> success – number of devices added for upgrade = 2

☞ *Note: Check upgrade using the following command:* show boot on ap6532-A429A0

5 Reload at a later time

- *Option 1*

Reload all devices

vx or nx – CLI – enable Mode
reload on default
> ap1 : OK
> ap2 : OK
> vx9k : OK

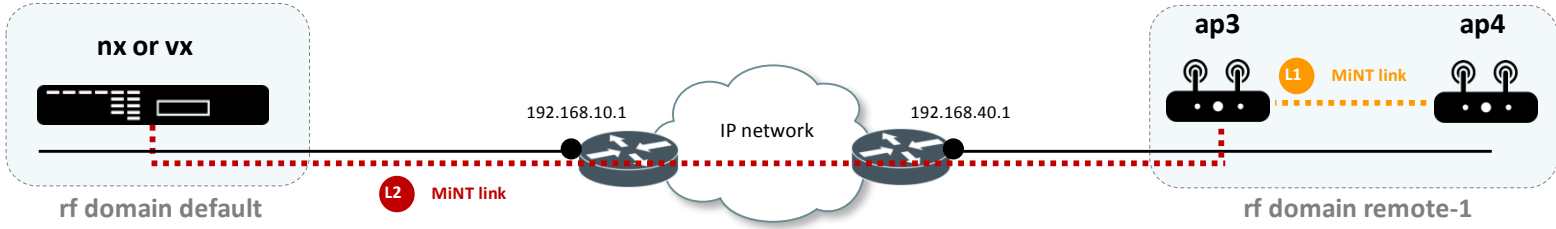
- *Option 2*

Reload adopted devices one by one

vx or nx – CLI – enable Mode
reload on ap6532-A429A0
> ap1 : OK
reload on ap6532-A42A30
> ap2 : OK

☞ *Note: After reload, adopted devices in the rf-domain default are now displaying a « configured » adoption status (* show adoption status)

Firmware Upgrade – NOC Deployments



1 Disable the adopted device automatic firmware upgrade

vx or nx – CLI - configuration Mode
no device-upgrade auto

2 Management platform – firmware upgrading

vx or nx – CLI – enable Mode
upgrade tftp://ip-address/VX9000-5.x.x.x-0xx.img

3 Reload the management platform

vx or nx – CLI – enable Mode
reload

☞ *Note: After reload, adopted devices are now in a « version-mismatch » adoption status* (show adoption status)

4 Upgrade adopted devices in the remote rf-domain – using the « no-reboot » option - Remote devices can then be reloaded at a later time

vx or nx – CLI – enable Mode
device-upgrade rf-domain remote-1 all no-reboot

☞ *Note: Check upgrade using the following command:* show boot on ap6532-A429A0

5 Reload devices at a later time in the remote rf-domain

vx or nx – CLI – enable Mode
reload on remote-1
ap3 : OK
ap4 : OK

☞ *Note: After reload, adopted devices in the remote rf-domain are now displaying a « configured » adoption status* (show adoption status)

WiNG - Quick Start Guide

Appendix – Feature Matrix

WiNG 5 Quick Start Guide

Controller Feature Matrix

Controller Type	Max Access Points (NOC Deployments)	Max Access Points (Campus deployments)	MiNT Tunneling	L2TPv3 Tunneling	Backplane for data tunneling
VX 9000	25,600	4,096	Not Supported	Not Supported	Not supported
NX 9500, NX9600	10,240	4,096	Not Supported	Not Supported	Not supported
NX9510, NX9610	10,240	4,096	4,096 tunnels	16,383 tunnels	Up to 40Gbps firewall throughput Up to 30Gbps HW crypto throughput
NX75XX	2,048	2,048	1,024 tunnels	2,048 tunnels	Up to 20Gbps firewall throughput Up to 8Gbps HW crypto throughput
NX5500	512	512	256 tunnels	255 tunnels	Up to 4Gbps firewall throughput Up to 1.4Gbps HW crypto throughput
RFS 6000 (EOS)	256	256	48 tunnels	511 Tunnels	Up to 2Gbps firewall throughput
RFS 4000	144	36	36 tunnels	63 Tunnels	1Gbps firewall throughput

WiNG 5 Quick Start Guide

Controller Feature Matrix

Controller	Number of AP	Tunneling support	VM based	As NOC controller	As Campus controller	As Site controller
VX9000	25,600 (from 5.9.1)	No	Yes (VMWare, Hyper-V, XenServer, Amazon EC2, KVM)	Yes	Yes	Yes
NX9600	10,240	No	No	Yes	Yes	No
NX9610	10,240	Yes	No	Yes	Yes	No
NX9500	10,240	No	No	Yes	Yes	No
NX9510	10,240	Yes	No	Yes	Yes	No
NX75X0	2,048	Yes	No	Yes	Yes	Yes
NX5500	512	Yes	No	Maybe	Yes	Yes
RFS4000	144	Yes	No	No	No	Yes

WiNG 5 Quick Start Guide

Access Points Use Cases

AP Type	Voice	High Density of clients	MeshConnex	Client Bridge	Location Based Services	WIPS
AP6522-6562	YES only radio 2	No	YES	Yes	Yes poor perf	Yes
AP7502	Yes	No	Yes (2.4GHz only)	No	No	No
AP7522	Yes	Yes	Yes	Yes	Yes	Yes with 2 radios
AP7532	Yes	Yes	Yes	Yes	Yes	Yes with 2 radios
AP7562	Yes	Yes	Yes	Yes	Yes	Yes with 2 radios
AP7602	Maybe	No	No	Yes	5.9.1	Yes
AP7622	No	No	No	Yes	5.9.1	Yes
AP7612	Yes	No	No	No	5.9.2	5.9.2
AP7632	Yes	Yes	No	No	5.9.2	5.9.2
AP7662	Yes	Yes	No	No	5.9.2	5.9.2
AP8432	Yes	Yes	No	No	Yes	Yes (borrow radio 1 or use radioshare)
AP8533	Yes	Yes	No	No	Yes	Yes (dedicated 3rd radio)

WWW.EXTREMENETWORKS.COM