



Service Manager Bulletin

TITLE:

Volvo Cars Global WiFi Service

GROUP: 00	NO: 355	ISSUING DEPARTMENT: Service Operations	CAR MARKET: United States and Canada	
REFERENCE BULLETINS:			ISSUE DATE: 2016-10-14	STATUS DATE: 2016-11-22
Service Personnel: Read and initial	SERVICE MANAGER	SERVICE WRITER	WARRANTY ADMINISTRATOR	Page 1 of 20

“Right first time in Time”

OVERVIEW

The **Volvo Cars Global WiFi service** is a service developed by Volvo Cars. From start, three service offerings are available within the service:

- Volvo Cars Diagnostic WiFi (VCCarDW)
- Volvo Cars Vehicle Connectivity WiFi (VCVCW)
- Volvo Cars Guest WiFi

The **Volvo Cars Diagnostic WiFi** will be detected by the vehicle when arriving at the dealership. When the vehicle connects it will be visible in VIDA and the system works as if the vehicle was connected by a cable.

The **Volvo Cars Vehicle Connectivity WiFi** will provide access to Internet for the vehicles. The network can be used for the following:

- demonstration of vehicle connectivity functionality in the showroom
- sales personnel can load apps and other data to vehicles in the showroom
- service technicians can load apps and other data into vehicles in the workshop
- fault tracing requiring connection to the Internet in the vehicle

The **Volvo Cars Guest WiFi** is offered to give a harmonized “retail experience” for Volvo customers visiting a dealership (Phase 2, 2017).



DESIGN REQUIREMENTS

- The solution must be scalable.
 - 1 connection per second year 2020.
 - 7000000 SPA cars 2028.
- The solution must be secure.
 - Radius certificates need to be contained within Volvo premises.
 - Car certificate shall be possible to revoke.
 - Car shall only be able to connect to valid Volvo Car dealer or Importer.
- The solution must deliver high availability.
 - The authentication chain (RADIUS server + OSCP) shall be available 24 hours, 7 days per week.
 - Reliability of 99.5%
- The solution must be manageable.
 - 2700 Dealer and importers at start.
 - Up to 10000 AP worldwide.
- The solution should be consistent, high quality for all workshops.
 - Order process, provide consistent installation in ALL sites.

SOLUTION OVERVIEW

The purpose of the Volvo Cars Global WiFi service is to provide a predictable, stable and secure wireless environment for the cars in a workshop scenario.

The solution consists of two main parts:

Central wireless environment

Central radius

Central wireless environment

The architecture is based on a cloud-managed solution from Cisco Meraki. It allows for central management of access points and easy deployment of new sites.

Central radius

The central radius will allow the solution to scale for several thousand sites and still be easy to administrate. It offers high availability and a secure environment for server side certificates.



VERIFICATION TOOL

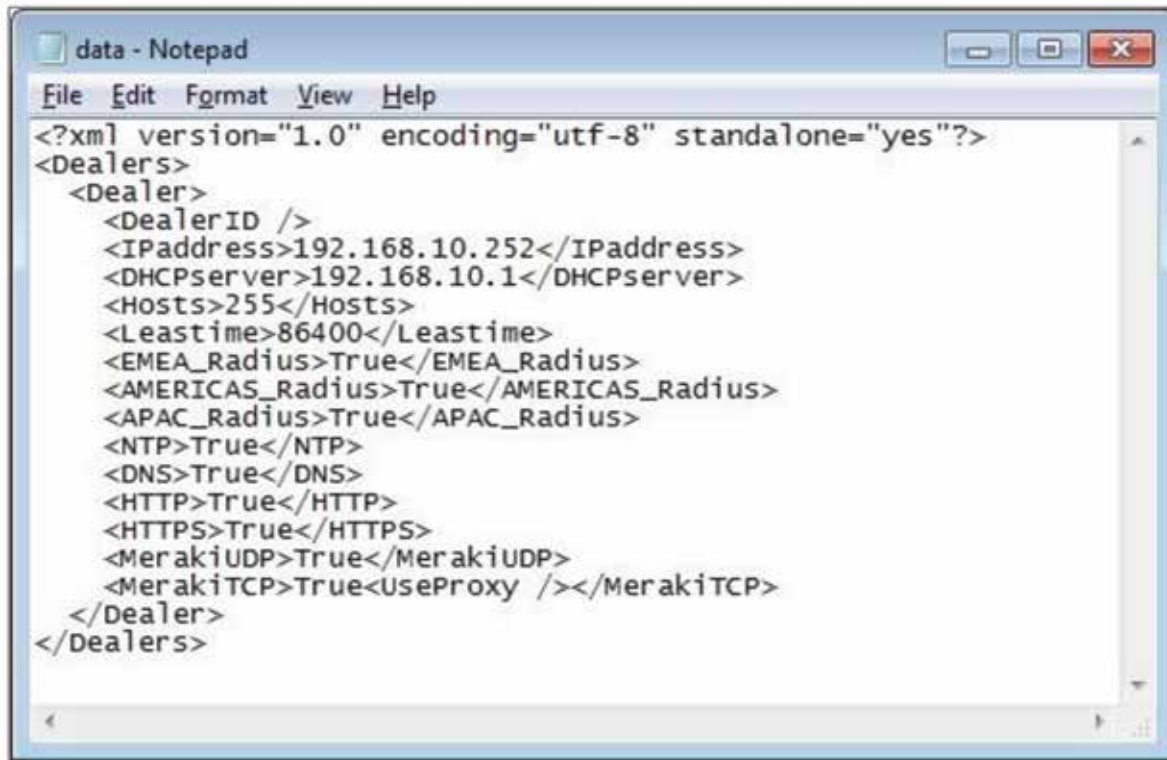
- Run in switchport used or intended to be used by the access points.
- Check to verify all ports and IP requirement is fulfilled.
- Can be used as a fault tracing tool at dealer.



Fig. 1



- Result file can be attached if support is needed.



```
data - Notepad
File Edit Format View Help
<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<Dealers>
  <Dealer>
    <DealerID />
    <IPAddress>192.168.10.252</IPAddress>
    <DHCPserver>192.168.10.1</DHCPserver>
    <Hosts>255</Hosts>
    <Leasetime>86400</Leasetime>
    <EMEA_Radius>True</EMEA_Radius>
    <AMERICAS_Radius>True</AMERICAS_Radius>
    <APAC_Radius>True</APAC_Radius>
    <NTP>True</NTP>
    <DNS>True</DNS>
    <HTTP>True</HTTP>
    <HTTPS>True</HTTPS>
    <MerakiUDP>True</MerakiUDP>
    <MerakiTCP>True<UseProxy /></MerakiTCP>
  </Dealer>
</Dealers>
```

Fig. 2

VOLVO CARS DIAGNOSTIC WIFI

Access Security

WPA2 Enterprise using certificate to authenticate against central radius.

Access

Local LAN

IP Addressing

The car uses DHCP to get an IP address. This needs to be provided by the dealer infrastructure.



VOLVO CARS DIAGNOSTIC WIFI – USE CASE EXAMPLE

The use case starts when the vehicle sees a valid workshop WLAN and the driver accepts that a connection will be made.

1. The Workshop AP asks the Vehicle for identity.
2. The Vehicle sends its identity.
3. The Authenticator (access point) sends an access request to RADIUS server.
4. The RADIUS server initiates TLS handshake with Workshop AP.
5. The Authenticator sends server certificate to Vehicle.
6. The Vehicle verifies server certificate.
7. The Vehicle sends client certificate to Authenticator.
8. The Authenticator sends client certificate to RADIUS server.
9. The RADIUS server verifies client certificate against CA server.
10. The RADIUS server validates that client certificate is still valid against OCSP server.
If the OCSP server is unavailable the car will gain access. Only if the OCSP rejects the certificate will the car be rejected.
11. The RADIUS server accepts Vehicle.
12. The Workshop AP accepts Vehicle.
13. The Workshop LAN DHCP assigns an IP address to the Vehicle.
14. The Vehicle HMI display shows connection is made.
15. The Vehicle starts to broadcast DOIP announcements.

VOLVO CARS VEHICLE CONNECTIVITY WIFI

Access Security

WPA2-PSK with unique PSK for each workshop.

Access

Sandboxed inside AP, only external Internet access.

IP Addressing

Client will get dummy IP address from AP.



VOLVO CARS GUEST WIFI

Access Security

Click thru access with AUP.

Access

Sandboxed inside AP, only external Internet access.

IP Addressing

Client will get dummy IP address from AP.

SANDBOXING (NAT-MODE)

- The DHCP server run by the Cisco Meraki AP provides addresses in the 10.0.0.0/8 subnet (10.x.x.x). Outbound connections will be initiated with the LAN IP address of the AP using Network Address Translation. Wireless clients that connect to the network will be given the following configuration via Meraki DHCP:
 - An IP address in the 10.x.x.x range. The IP address is created by running the client's MAC address through a hashing algorithm.
 - A gateway address of 10.128.128.128
 - A DNS address of 10.128.128.128

SANDBOXING (CLIENT ISOLATION)

- NAT mode with Meraki DHCP isolates clients. Devices with a Meraki DHCP address will be able to access external and internal resources, such as the Internet and LAN (if firewall rules permit). However, connected clients will be unable to contact each other.

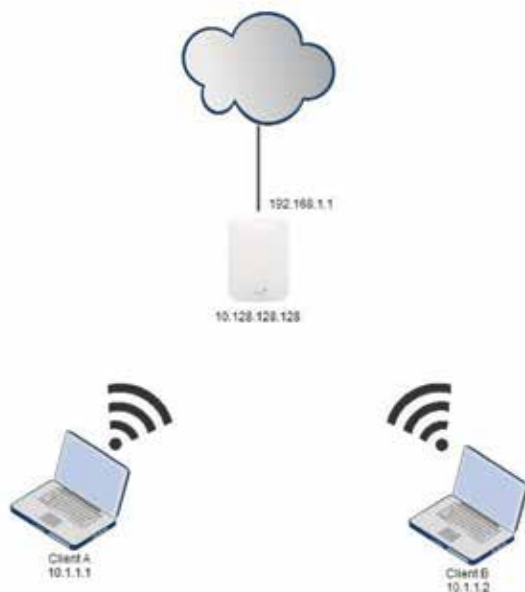


Fig. 3



- Client A and Client B can both access the Internet. When Client A wants to send traffic to Client B, the traffic will reach the AP. However, the AP will not forward this traffic to Client B. Therefore, the two clients are isolated from each other.

SANDBOXING (NETWORK ISOLATION)

- The **Deny Local LAN** function blocks access from Wireless clients on sandboxed SSIDs to the **Local LAN**.
- For the purposes of this firewall rule, **Local LAN** is described as any destinations in the following private address spaces:
 - 10.0.0.0/8
 - 172.16.0.0/12
 - 192.168.0.0/16
- *DNS traffic is exempt from this rule.*

CENTRAL WIRELESS

- The architecture is designed around a solution from Cisco Meraki which provides several benefits, such as:
 - Central management of network components.
 - Consistent deployment of new sites.
 - Authentication via RADIUS proxy from cloud controller.
 - Centralized logs and alarms.
 - Unified guest WiFi.

CENTRAL MANAGEMENT OF NETWORK COMPONENTS

- All the administration is done on the dashboard via a web browser. The support personnel can easily make changes on any AP wherever it is installed in the world.
- It's easy to deploy changes to the solution even if it consists of thousands of APs that are distributed around the world.
- Updates to the hardware are automatically distributed and you can easily deploy them during maintenance windows that best suit the specific workshop.



Fig. 4

AUTHENTICATION VIA RADIUS PROXY

- This feature dramatically reduces the number of RADIUS clients that have to be supported on the RADIUS server side.
- Every access point is connected to the cloud controller and it proxies the RADIUS request from the AP toward the RADIUS server.
- The number of RADIUS clients remains the same as the system grows.
- Only Volvo Cars Global WiFi service AP will have access to central radius.



CISCO MERAKI CLOUD CONTROLLER

- Cisco Meraki device typically utilizes 1 kb/s or less.
- Cisco Meraki's control tunnel supports seamless high availability.
 - Every Cisco Meraki network is backed by at least three independent data centers
- While the Cisco Meraki cloud is unreachable, management, monitoring, and hosted services are temporarily unavailable.

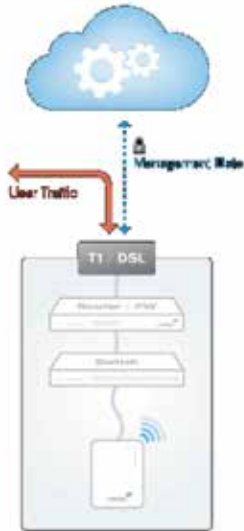


Fig. 5

CISCO MERAKI CLOUD CONTROLLER PORTS

- Meraki cloud communication.
 - UDP 7351 from Meraki cloud addresses.
- Backup Meraki cloud communication.
 - TCP 80 from Meraki cloud addresses.
- Backup configuration downloads, Backup firmware downloads, Throughput tests live tool, Splash pages.
 - TCP 80, 443, 7734, 7752
 - NTP UDP 123



CISCO MERAKI AP



Fig. 6

- Indoor AP MR32
 - 802.11AC
 - 3 radios: 2.4 and 5 GHz, dual-band WIDS/WIPS
 - 2-stream 802.11ac and 802.11n, up to 1.2 Gbps
 - PoE: Full functionality with 802.3af
 - Guest isolation firewall, restrict or block recreational traffic
- Outdoor AP MR72
 - IP67 rated, tested for dust, shock, vibration, and moisture
 - 3 radios: 2.4 and 5 GHz, dual-band WIDS/WIPS
 - 2-stream 802.11ac and 802.11n, up to 1.2 Gbps
 - PoE: Full functionality with 802.3af
 - Guest isolation firewall, restrict or block recreational traffic



CISCO MERAKI AP

- Need access to switchport.
- Need power.
 - Adapter.
 - PoE adapter.
 - PoE 802.3af capable switch.
- Gets IP from local DHCP server.
- Need working DNS (will connect without but with limited functions.)
- Connects to cloud controller.
- Gets configuration and starts to operate.

UNIFIED GUEST WIFI

- Same experience in all workshops.
- Will redirect to specific URL.
- Can be used for marketing purpose.



Fig. 7



UNIFIED GUEST WIFI REQUIREMENTS

- Guest WiFi bandwidth shall be max 4 Mbit/s.
 - If local dealer Internet access permits higher-speed bandwidth, it could be more even to the guest WiFi.
- Guest WiFi bandwidth shall be max 1 Mbit/s per user
- Guest WiFi bandwidth shall allow “bursts” up to 4 Mbit/s
- An AUP will be available by following link.
- Redirect after connect.
- Guest users will be sandboxed within the AP and will only be able to reach Internet.

PREDICTABLE WIRELESS ENVIRONMENT

- All updates and changes to the system can be tested in a test/QA environment before implementation.
- New car software can be tested and the result will apply to entire solution.

WHAT IS LOGGED

- When a client connects to an AP the system logs:
- Date/time
- What AP the car connects to
- Hostname (include VIN information for the cars)
- IP address
- MAC address

Time (CEST) ▼	Access point	SSID	Client
Aug 19 12:06:57	EMEA-SE-SAA-AP1	VCCarDW	DolP-VCCYV1PSA8BDH1000286
Aug 19 11:46:21	EMEA-SE-SAA-AP1	VCCarDW	DolP-VCCYV1PSA8BDH1000286
Aug 19 11:46:21	EMEA-SE-SAA-AP1	VCCarDW	DolP-VCCYV1PSA8BDH1000286

Fig. 8



MERAKI DASHBOARD

- Log in using functional e-mail address.
- Get access to specific markets' networks.

The screenshot shows the Meraki Dashboard Login interface. At the top left, the Cisco Meraki logo is displayed. The main heading is 'Dashboard Login'. Below this, there are two text input fields: 'Email' and 'Password'. Under the 'Password' field, there is a green 'Log in' button and a checkbox labeled 'Stay logged in'. At the bottom of the login form, there are two links: 'I forgot my password' and 'Create an account'.

Fig. 9



NSC/BSC/IMPORTER AND DEALER ACCESS TO DASHBOARD

- Support personnel at NSC/BSC and Importers will have limited access to dashboard.
- Will only see networks for the market they assist.
- Basic fault tracing is possible.
- (NEW) Dealer can get monitor access to its workshop APs.

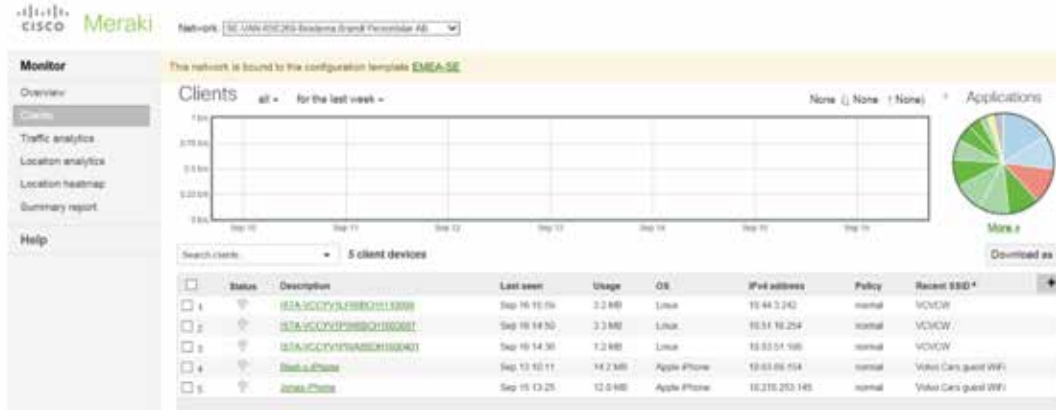


Fig. 10

CENTRAL RADIUS

- The central RADIUS solution provides benefits, such as:
 - Scalability
 - High availability
 - Manageability
 - Security

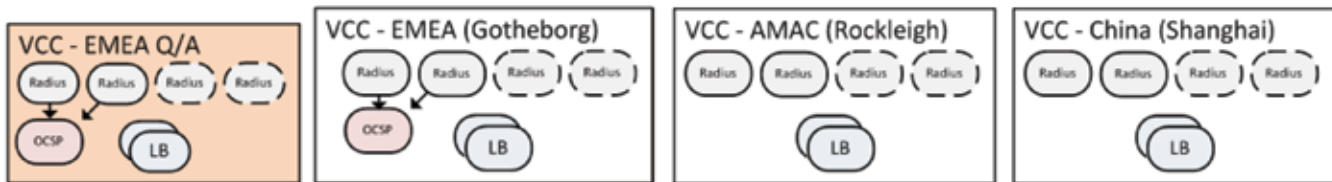


Fig. 11

OCSP (ONLINE CERTIFICATE STATUS PROTOCOL)

- The certificate that the car use needs to be checked against an OCSP-server.
- If the certificate is revoked the car will not be able to connect.
- All radius clusters will use the OCSP servers in Gothenburg.
- If the OCSP does not respond, the car will be allowed access.



DESIGN OVERVIEW

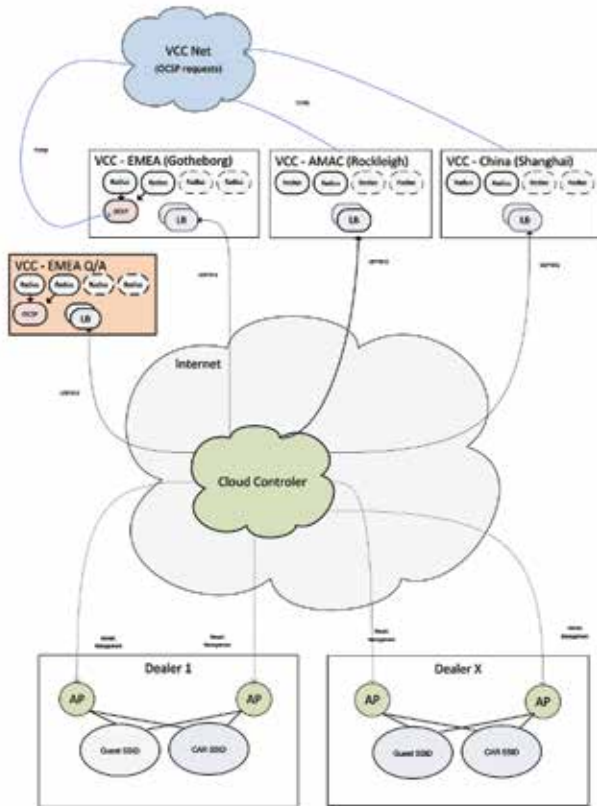


Fig. 12

DEALER NETWORK TOPOLOGIES

- Local consideration when you install Volvo Cars Global WiFi solution:
 - Current dealer infrastructure
 - ◆ Network size (AP and Car will consume IP addresses)
 - ◆ IP assignment method (will only work with DHCP)
 - ◆ Firewall rules
 - ◆ Proxy solution
 - Local security policy
 - ◆ Network separation
 - ◆ Internet access policy



EXAMPLE 1 – NORMAL INSTALLATION SINGLE NETWORK

- No complexity.
- Works out of the box for VIDA.
- Security provided by AP.
- Local Internet rules might be applied on guest traffic.

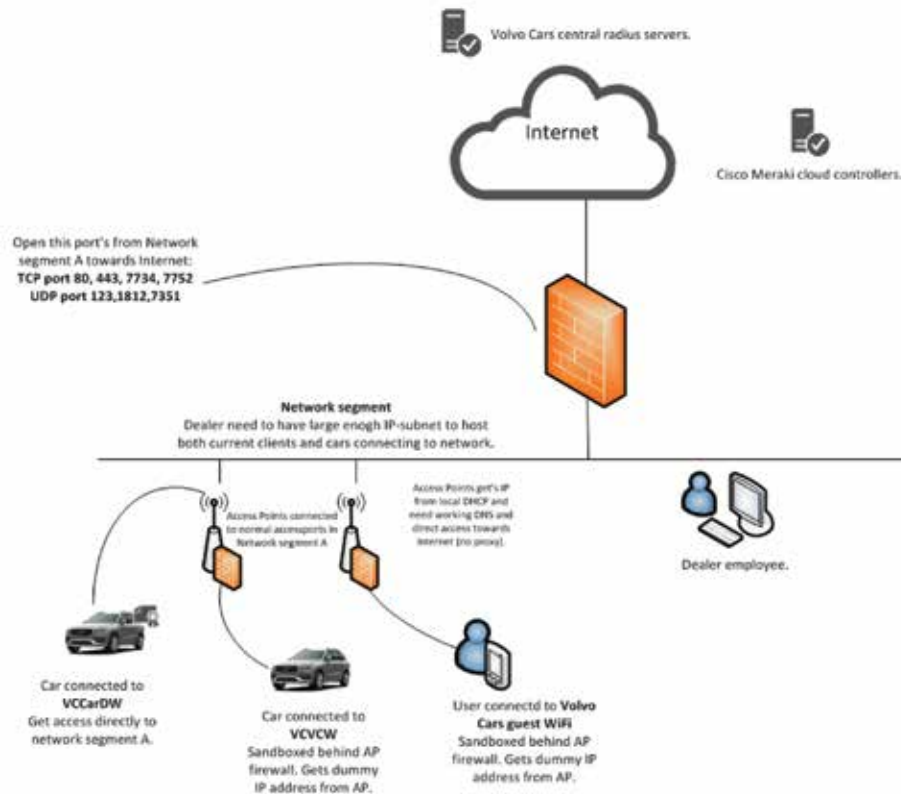


Fig. 13



EXAMPLE 2 – SEPARATE NETWORKS

- Higher complexity.
- Need to configure VIDA admin for network discovery.
 - Specify directed broadcast address or the network range for **Network segment A** in example 2.
- Security provided by dealer firewall and AP firewall.
 - Local firewall needs to permit DOIP traffic (UDP 13400) to pass from **Network segment B** to **Network segment A**.
- Local Internet rules might be applied on guest traffic.

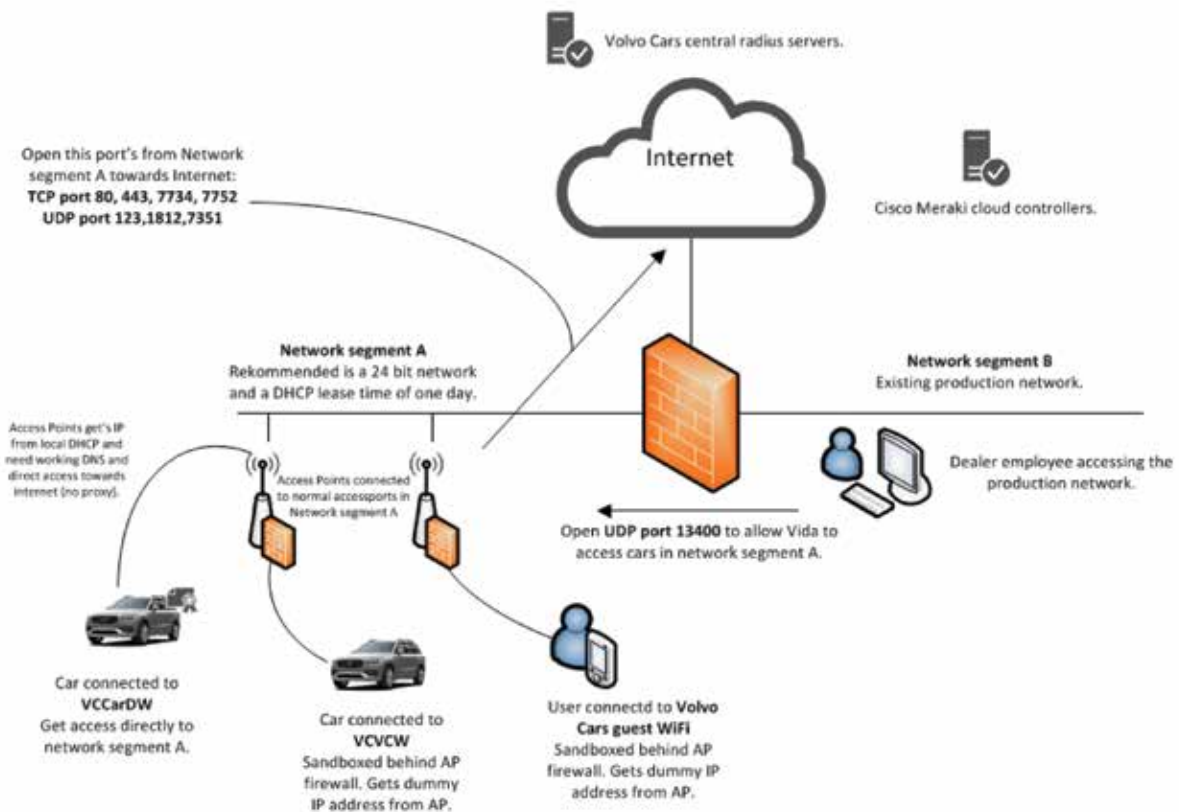


Fig. 14 Example 2 – Separate Networks

EXAMPLE 3 – SEPARATE NETWORKS (ADVANCED INSTALL)

- Can use different VLAN for guest traffic and connectivity traffic.
- AP traffic and diagnostic traffic will still go “untagged” and it’s possible for dealer to use any VLAN for this traffic.
- Make it possible to have different Internet provider for guest and production traffic.
- Can be ordered after successful installation of service.

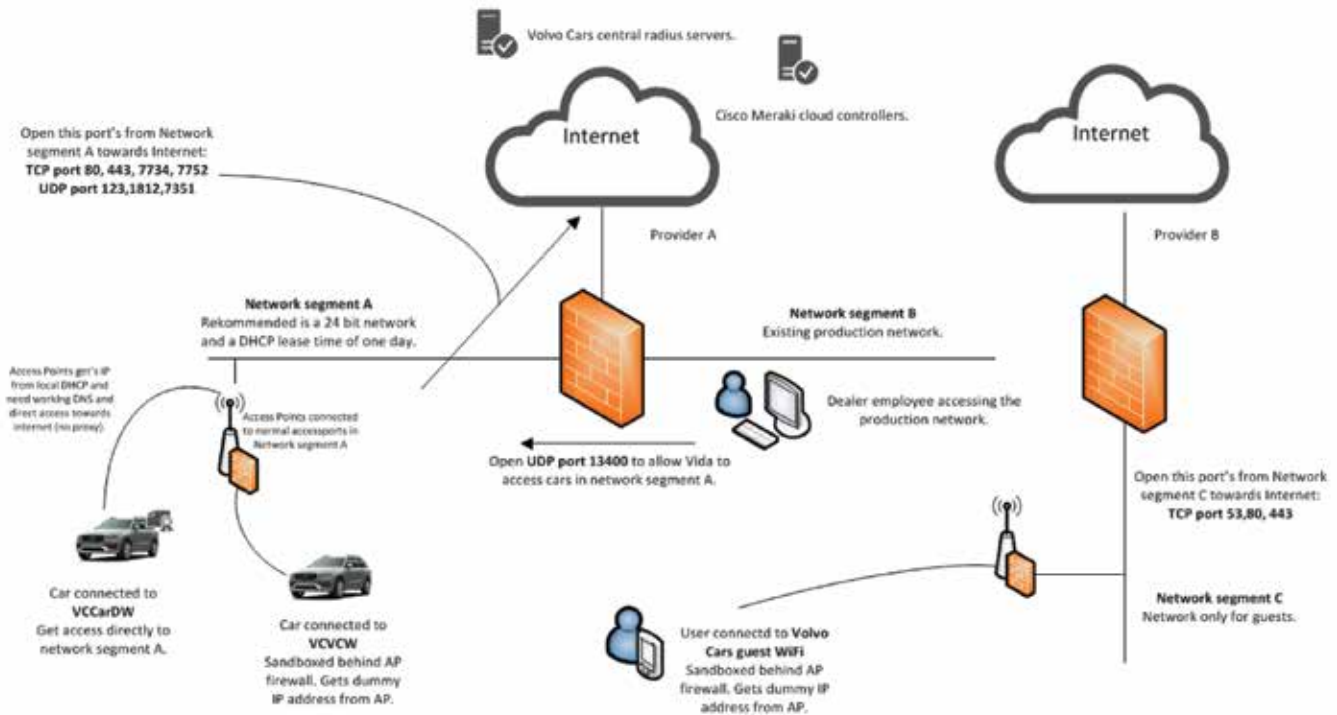


Fig. 15 Example 3 – Separate Networks (Advanced Install)

SETTINGS IN VIDA ADMIN

- Depending on the network design, the dealers have to configure VIDA admin accordingly.
- There are two different methods of detecting car on other networks:
 - Directed Broadcast.
 - Sequential Scanning.
- Traffic between VIDA client and cars will be TCP13400 (DOIP).



SETTINGS IN VIDA ADMIN (DIRECTED BROADCAST)

- You need to know the details about the network used by the car.
- IP address and subnet mask.
- The example is from network 192.168.131.0/24.
- The directed broadcast address for this subnet will be 192.168.131.255.
- Your firewall/router may block this type of traffic. If so, you need to use Sequential Scanning.

The screenshot shows the 'LAN vehicle discovery' settings in VIDA Admin. A checkbox labeled 'VIDA clients and vehicles exist in different IP subnets.' is checked. Below this, it states 'VIDA can discover vehicles using two different methods: 1. Sequential scanning (always works) 2. Directed Broadcast (better performance in LANs where routers support subnet directed broadcasts)'. It then asks to 'Specify which method should be used for each subnet.' There are five subnets listed. Subnet 1 is set to 'Directed Broadcast' and has a 'Broadcast address' of '192.168.131.255'. Subnets 2 through 5 are set to '-NotConfigured-'.

Fig. 16

SETTINGS IN VIDA ADMIN (SEQUENTIAL SCANNING)

- You need to know the details about the network used by the car.
- IP address and subnet mask.
- The example is from network 192.168.131.0/24.
- In this example we will scan all addresses in the network.
- It is possible to adjust this to match the scope in the DHCP server for the network.

The screenshot shows the 'LAN vehicle discovery' settings in VIDA Admin. A checkbox labeled 'VIDA clients and vehicles exist in different IP subnets.' is checked. Below this, it states 'VIDA can discover vehicles using two different methods: 1. Sequential scanning (always works) 2. Directed Broadcast (better performance in LANs where routers support subnet directed broadcasts)'. It then asks to 'Specify which method should be used for each subnet.' There are five subnets listed. Subnet 1 is set to 'Sequential Scanning' and has 'From' and 'To' IP address fields set to '192.168.131.1' and '192.168.131.254' respectively. Subnets 2 through 5 are set to '-NotConfigured-'.

Fig. 17



ADVANCED SECURITY

- No filter is applied on user traffic.
 - The dealer can restrict guest traffic in firewall as long as DNS, HTTP and HTTPS are working.
- URL-filtering and content inspection can be done at premises to increase security.
 - It's not possible to use proxy solutions for clients.
- Total separation of traffic can be done using advanced installation option.