

AO EXCELENTÍSSIMO SENHOR AGENTE DE CONTRATAÇÃO DA CONTROLADORIA-GERAL DA UNIÃO – CGU.

PREGÃO ELETRÔNICO Nº 90001/2026

PROCESSO Nº 00190.100931/2025-83

Objeto: Registro de preços para aquisição de solução de conectividade de rede sem fio (WLAN), incluindo a aquisição de equipamentos, licenciamento, serviços de instalação, configuração, transferência de conhecimento, garantia e suporte técnico, visando atender as necessidades de modernização e expansão da rede Wi-Fi da CGU.

Assunto: Contrarrazões ao recurso apresentado pela **TELESUL TELECOMUNICAÇÕES LTDA.**, contra à decisão que declarou vencedora do certame a empresa **3CORP TECHNOLOGY INFRAESTRUTURA DE TELECOM LTDA.**

A **3CORP TECHNOLOGY INFRAESTRUTURA DE TELECOM LTDA.**, inscrita sob o CNPJ nº 04.238.297/0004-21, doravante designada “**3CORP**”, com fulcro na Lei Federal nº 14.133/2021, e demais legislação aplicável e, ainda, de acordo com as condições estabelecidas no Edital, vem tempestivamente e respeitosamente, apresentar **CONTRARRAZÕES** ao **RECURSO** interposto pela empresa **TELESUL TELECOMUNICAÇÕES LTDA.**, doravante designadas “**TELESUL**” em face da decisão que a declarou vencedora, conforme segue:

1) DA TEMPESTIVIDADE

A presente resposta é tempestiva, uma vez que a empresa Recorrente **TELESUL** poderia apresentar suas razões recursais até o dia 01/04/2026 (quarta-feira) e considerando o prazo para apresentação das contrarrazões de 03 (três) dias úteis, o prazo se esgotará no dia 07/04/2026 (terça-feira), portanto, verifica-se a sua tempestividade, conforme subitem 13.7. do Edital.

2) PRELIMINARMENTE

Ao elaborar a proposta, a **3CORP** fez no mais estrito cumprimento aos princípios gerais do Direito, atendendo aos preceitos que regem as licitações públicas, no que tange a modalidade de licitação denominada pregão, na forma eletrônica, além de garantir a observância dos princípios da legalidade, da impessoalidade, da moralidade, da publicidade, da eficiência, do interesse público, da probidade administrativa, da igualdade, do planejamento, da transparência, da eficácia, da segregação de funções, da motivação, da vinculação ao edital, do julgamento objetivo, da segurança jurídica, da razoabilidade, da competitividade, da proporcionalidade, da celeridade, da economicidade e do desenvolvimento nacional sustentável, insculpidos na nova lei de licitações de contratos administrativos.

Conforme alegações a seguir, a **3CORP** demonstrará que a decisão do Agente de Contratação e de sua equipe de apoio foi assertiva, pois fundamentada em princípios basilares da licitude e de acordo com o disposto no Edital.

3) DOS FATOS E DOS FUNDAMENTOS JURÍDICOS

Trata-se de licitação na modalidade de pregão eletrônico, tipo menor preço, modo de disputa aberto e fechado, com valor estimado de R\$ 4.069.074,23 (quatro milhões, sessenta e nove mil e setenta e quatro reais e vinte e três centavos), visando o registro de preços para aquisição de solução de conectividade de rede sem fio (WLAN), incluindo a aquisição de equipamentos, licenciamento, serviços de instalação, configuração, transferência de conhecimento, garantia e suporte técnico, visando atender as necessidades de modernização e expansão da rede Wi-Fi da CGU.

Após a etapa de envio de lances, a empresa Recorrida **3CORP**, restou classificada em 1º lugar com o menor lance de R\$ 2.579.500,00 (dois milhões, quinhentos e setenta e nove mil, quinhentos reais), sendo convocada para envio da proposta de preço ajustada e documentação de habilitação.

A proposta da Recorrida **3CORP** foi aceita, consoante o parecer da área técnica, que afirmou que as especificações técnicas contidas nos documentos apresentados cumprem os requisitos do Termo de Referência.

Ocorre que, a empresa Recorrente **TELESUL**, irredimida com o resultado, interpôs recurso administrativo, e por qualquer ângulo que se observe, outra conclusão não se chegará, a não ser que o recurso é protelatório, sem fundamento técnico e jurídico, visando apenas retardar o processo, e como via de consequência, a decisão deve ser pela improcedência.

4) DAS CONTRARRAZÕES RECURSAIS

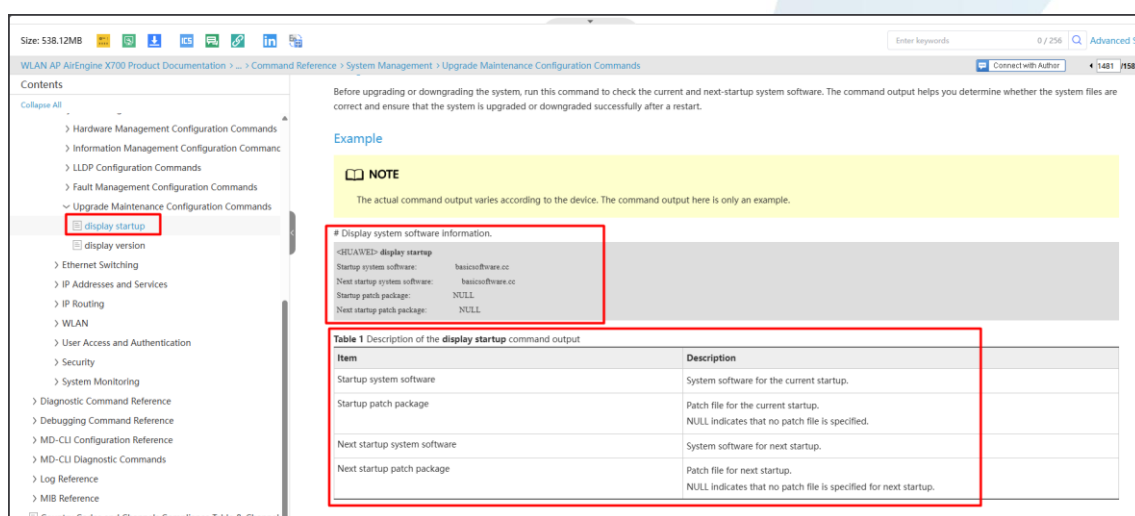
4.1) Do suposto não atendimento ao subitem 1.2.8. do Anexo I – Especificação Técnica

Aduz a Recorrente **TELESUL** que a Recorrida **3CORP**, não comprovou que a memória não volátil acomoda duas versões de firmware, requisito essencial para a segurança e resiliência do equipamento, não comprovando o subitem abaixo.

- 1.2.8. Possuir memória não volátil (flash) para armazenamento do software interno e da última configuração válida enviada pela controladora. Deve comportar, no mínimo, 2 (duas) imagens do sistema operacional simultaneamente, permitindo que seja realizada atualização de software e a imagem anterior seja mantida;

No entanto, esclarecemos que, a comprovação enviada demonstra o comando para verificação das imagens disponíveis no Acesso Point, conforme abaixo:

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100510642&id=EN-US_CLIREF_0000002190148852



Before upgrading or downgrading the system, run this command to check the current and next-startup system software. The command output helps you determine whether the system files are correct and ensure that the system is upgraded or downgraded successfully after a restart.

Example

NOTE

The actual command output varies according to the device. The command output here is only an example.

Display system software information.

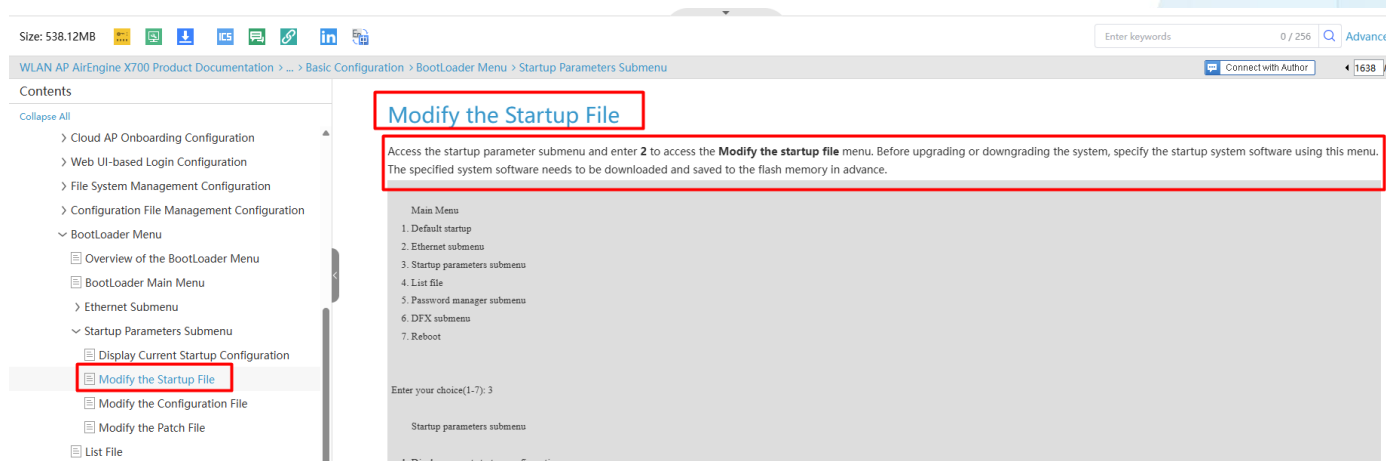
```
>HUAWEI> display startup
Startup system software:  basicsoftware.cc
Next startup system software:  basicsoftware.cc
Startup patch package:  NULL
Next startup patch package:  NULL
```

Table 1 Description of the display startup command output

Item	Description
Startup system software	System software for the current startup.
Startup patch package	Patch file for the current startup. NULL indicates that no patch file is specified.
Next startup system software	System software for next startup.
Next startup patch package	Patch file for next startup. NULL indicates that no patch file is specified for next startup.

Adicionalmente, demonstramos abaixo procedimento de alteração do arquivo de inicialização do Access Point, comprovando o atendimento ao item 1.2.8. do Anexo I – Especificação Técnica.

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100510642&id=EN-US_TOPIC_0000001402335846

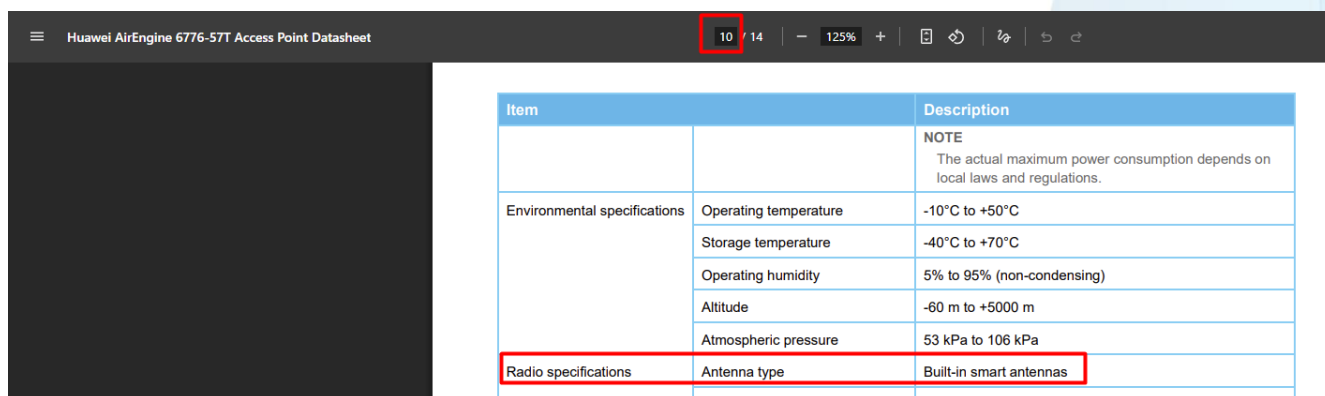


4.2) Do suposto não atendimento ao subitem 1.3.3. do Anexo I – Especificação Técnica

Aduz a Recorrente **TELESUL** que a Recorrida **3CORP**, não comprovou que a antena do produto ofertado é omnidirecional, característica fundamental para a cobertura de sinal esperada, não comprovando o subitem abaixo.

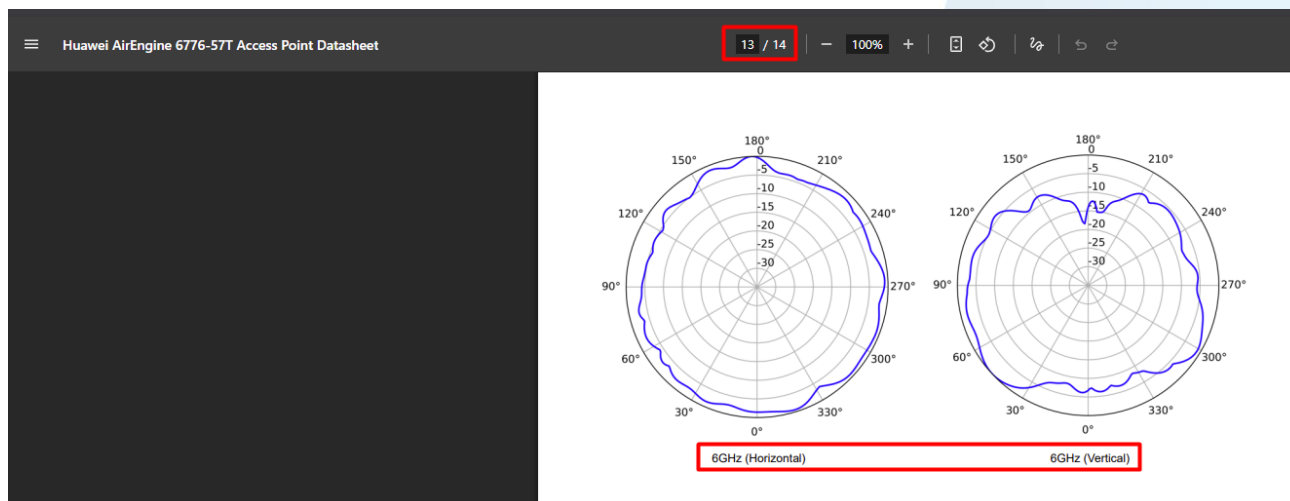
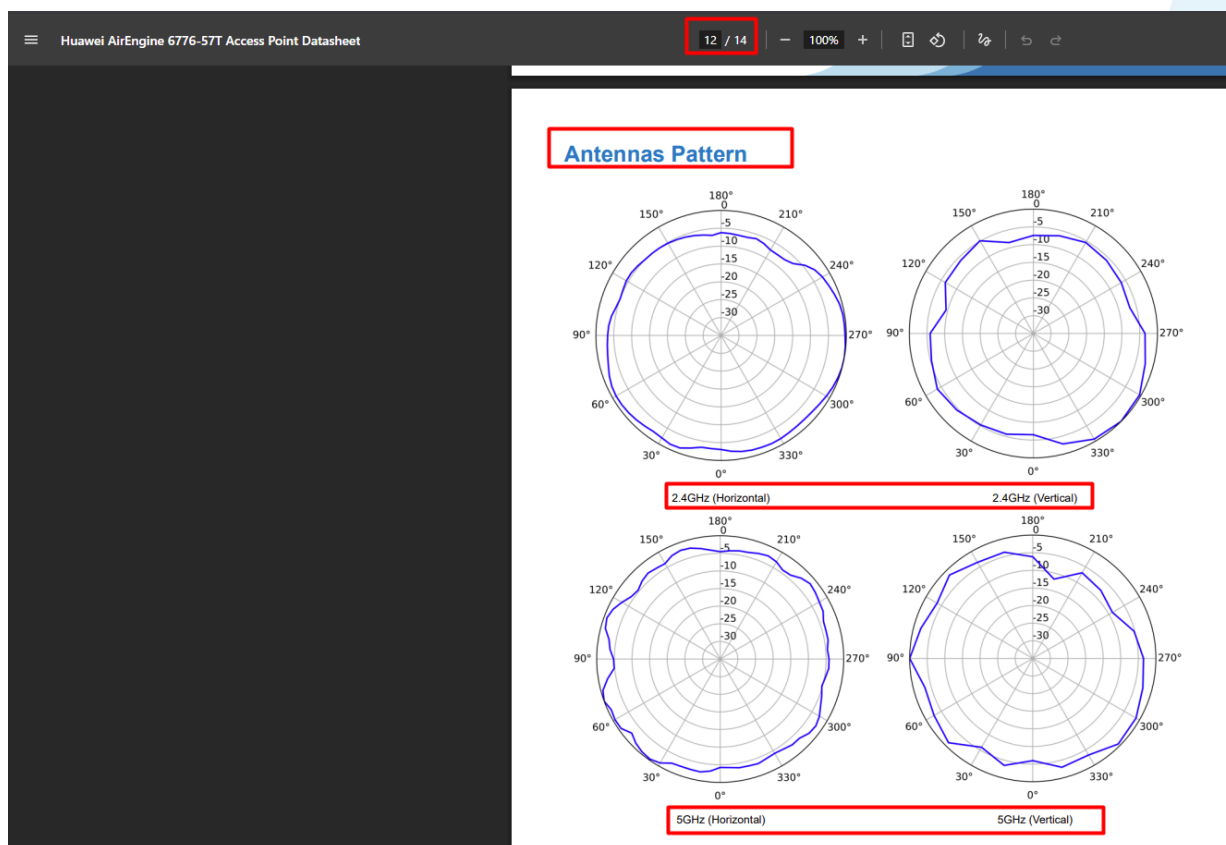
1.3.3. Possuir antenas omnidirecionais, integradas e internas;

No entanto, esclarecemos que, o modelo de Access Point ofertado (AirEngine 6776-57T) possui antenas integradas e internas, conforme descrito no datasheet (Huawei AirEngine 6776-57T Access Point Datasheet.pdf) página 10 e comprovado na imagem abaixo:



Huawei AirEngine 6776-57T Access Point Datasheet		
10 / 14 125% [Icons]		
Item		Description
		NOTE The actual maximum power consumption depends on local laws and regulations.
Environmental specifications	Operating temperature	-10°C to +50°C
	Storage temperature	-40°C to +70°C
	Operating humidity	5% to 95% (non-condensing)
	Altitude	-60 m to +5000 m
	Atmospheric pressure	53 kPa to 106 kPa
Radio specifications	Antenna type	Built-in smart antennas

No que tange à propagação, no mesmo documento (AirEngine 6776-57T), páginas 12 e 13 é demonstrado o padrão das antenas para 2,4GHz, 5GHz e 6GHz respectivamente:



As imagens apresentadas evidenciam que o padrão de radiação do sinal ocorre de forma essencialmente omnidirecional, caracterizado por uma distribuição uniforme da energia eletromagnética no plano horizontal (360°). Tal comportamento comprova o atendimento ao requisito estabelecido no item 1.3.3 do Anexo I – Especificação Técnica, no que se refere à cobertura omnidirecional do Access Point Modelo AirEngine 6776-57T.

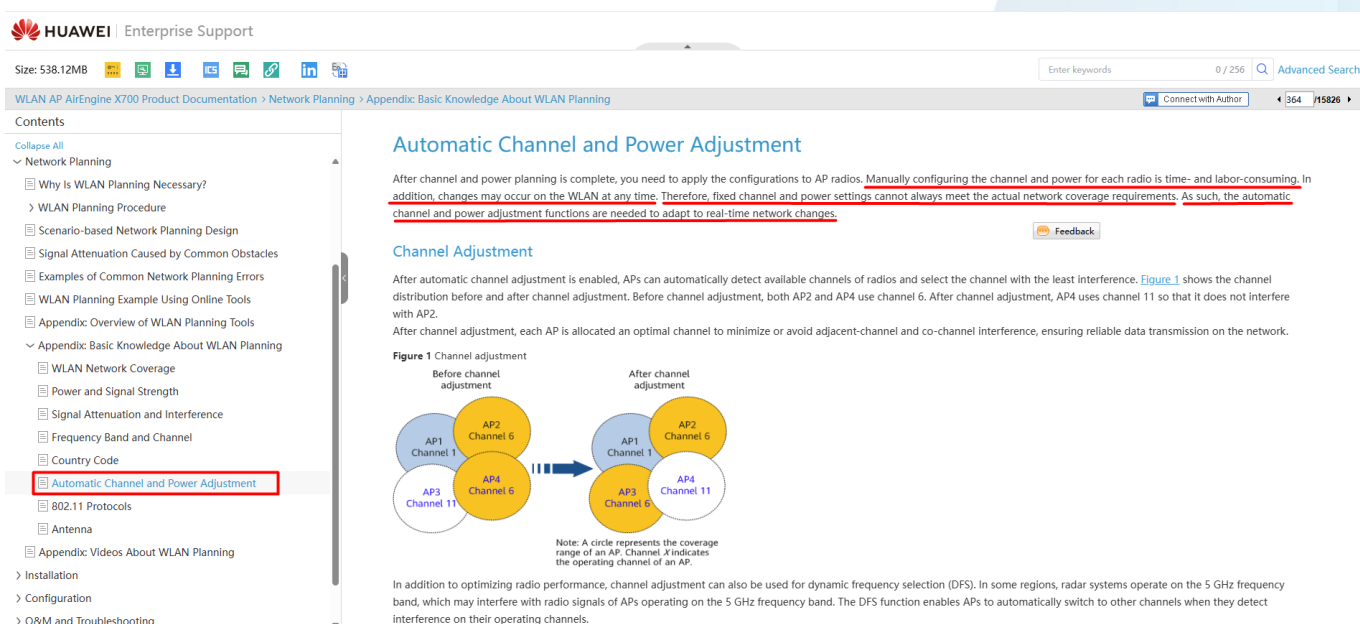
4.3) Do suposto não atendimento ao subitem 1.3.10. do Anexo I – Especificação Técnica

Aduz a Recorrente **TELESUL** que o link apresentado como comprovação demonstra o processo de configuração automática do nível de potência e do canal, não apresentando a comprovação do subitem abaixo.

1.3.10. Permitir o ajuste manual do nível de potência de transmissão;

No entanto, esclarecemos que, a indicação de documentação comprova que é permitido realizar o ajuste manual do nível de potência de transmissão, incluindo uma explicação de que o ajuste automático se demonstra ser a melhor forma de configuração para um ambiente de produção, pois manualmente, há demanda de tempo, mão de obra e possíveis alterações no ambiente, abaixo imagem extraída do link abaixo:

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100510642&id=EN-US_TOPIC_0000001484591886



The screenshot shows the Huawei Enterprise Support page for 'Automatic Channel and Power Adjustment'. The page includes a sidebar with a table of contents, a main content area with text and a diagram, and a footer with additional information.

Contents:

- WLAN AP AirEngine X700 Product Documentation > Network Planning > Appendix: Basic Knowledge About WLAN Planning
- WLAN Planning Procedure
- Scenario-based Network Planning Design
- Signal Attenuation Caused by Common Obstacles
- Examples of Common Network Planning Errors
- WLAN Planning Example Using Online Tools
- Appendix: Overview of WLAN Planning Tools
- Appendix: Basic Knowledge About WLAN Planning
 - WLAN Network Coverage
 - Power and Signal Strength
 - Signal Attenuation and Interference
 - Frequency Band and Channel
 - Country Code
 - Automatic Channel and Power Adjustment**
 - 802.11 Protocols
 - Antenna
- Appendix: Videos About WLAN Planning
- Installation
- Configuration
- O&M and Troubleshooting

Automatic Channel and Power Adjustment

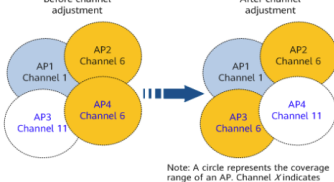
After channel and power planning is complete, you need to apply the configurations to AP radios. Manually configuring the channel and power for each radio is time- and labor-consuming. In addition, changes may occur on the WLAN at any time. Therefore, fixed channel and power settings cannot always meet the actual network coverage requirements. As such, the automatic channel and power adjustment functions are needed to adapt to real-time network changes.

Channel Adjustment

After automatic channel adjustment is enabled, APs can automatically detect available channels of radios and select the channel with the least interference. Figure 1 shows the channel distribution before and after channel adjustment. Before channel adjustment, both AP2 and AP4 use channel 6. After channel adjustment, AP4 uses channel 11 so that it does not interfere with AP2.

After channel adjustment, each AP is allocated an optimal channel to minimize or avoid adjacent-channel and co-channel interference, ensuring reliable data transmission on the network.

Figure 1 Channel adjustment



Note: A circle represents the coverage range of an AP. Channel X indicates the operating channel of an AP.

In addition to optimizing radio performance, channel adjustment can also be used for dynamic frequency selection (DFS). In some regions, radar systems operate on the 5 GHz frequency band, which may interfere with radio signals of APs operating on the 5 GHz frequency band. The DFS function enables APs to automatically switch to other channels when they detect interference on their operating channels.

Adicionalmente, demonstramos no link abaixo a opção de habilitar ou desabilitar a configuração de transmissão automática de potência, afim de realizar os ajustes de forma manual:

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100510642&id=EN-US_TOPIC_0000001894012057

Size: 538.12MB						Enter keywords		0 / 256		Advanced Search	
WLAN AP AirEngine X700 Product Documentation > ... > MD-CLI Configuration Reference > WLAN Configuration > RRM						Connect with Author		2327		15826	
Contents											
Collapse All											
		radio:radio-instance/hw-ap-radio:auto-channel-select		MDCLI> radio-instances radio-instance radio-id radio-id MDCLI> auto-channel-select { enable disable nocfg } MDCLI> commit		is not configured for a single AP radio, and the configuration of the AP group to which the AP radio belongs takes effect.		[g]root@HUAWEI MDCLI> wlan-ap ap-instances ap-instance ap-id 0 [*](g)root@HUAWEI]/wlan-ap/ap-instances/ap-instance[ap-id="0"] MDCLI> radio-instances radio-instance radio-id 1 [*](g)root@HUAWEI]/wlan-ap/ap-instances/ap-instances/ap-instance[ap-id="0"]/radio-instances/radio-instance[radio-id="1"] MDCLI> auto-channel-select disable [*](g)root@HUAWEI]/wlan-ap/ap-instances/ap-instance[ap-id="0"]/radio-instances/radio-instance[radio-id="1"] MDCLI> commit			
huawei-wlan-ap-radio.yang		/hw-wlan-ap:wlan-ap/hw-wlan-ap:ap-instances/hw-wlan-ap:ap-instance/hw-ap-radio:radio-instances/hw-ap-radio:radio-instance/hw-ap-radio:auto-tpower-select		MDCLI> edit-config MDCLI> wlan-ap ap-instances ap-instance ap-id ap-id MDCLI> radio-instances radio-instance radio-id radio-id MDCLI> auto-tpower-select { enable disable nocfg } MDCLI> commit		Enables or disables automatic transmit power selection. By default, automatic transmit power selection is not configured for a single AP radio, and the configuration of the AP group to which the AP radio belongs takes effect.		[root@HUAWEI] MDCLI> edit-config [g]root@HUAWEI MDCLI> wlan-ap ap-instances ap-instance ap-id 0 [*](g)root@HUAWEI]/wlan-ap/ap-instances/ap-instance[ap-id="0"] MDCLI> radio-instances radio-instance radio-id 1 [*](g)root@HUAWEI]/wlan-ap/ap-instances/ap-instance[ap-id="0"]/radio-instances/radio-instance[radio-id="1"] MDCLI> auto-tpower-select disable [*](g)root@HUAWEI]/wlan-ap/ap-instances/ap-instance[ap-id="0"]/radio-instances/radio-instance[radio-id="1"] MDCLI> commit			

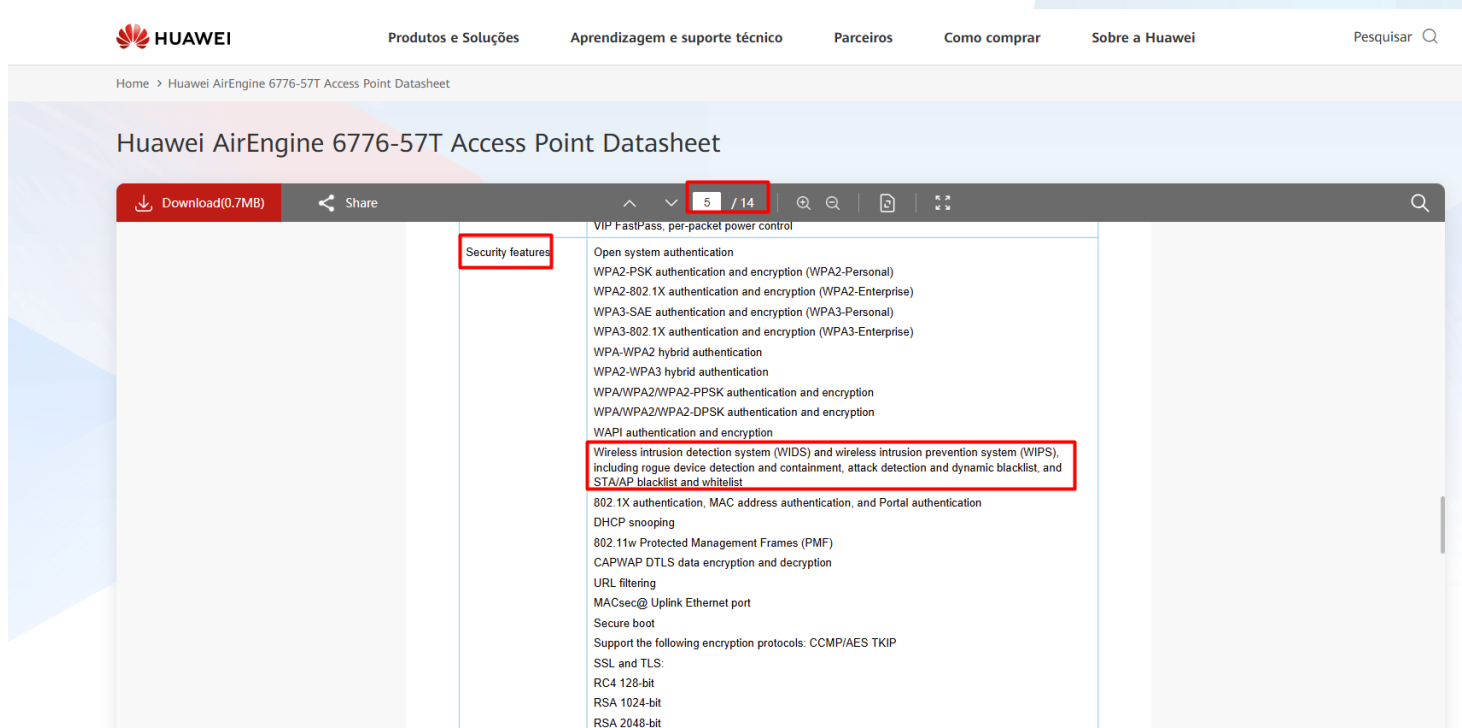
4.4) Do suposto não atendimento ao subitem 1.3.15. do Anexo I – Especificação Técnica

Aduz a Recorrente **TELESUL** que no documento apresentado, a Recorrida **3CORP** não demonstrou que o access-point possui capacidade de configurar um rádio para operar como sensor wIPS, limitando-se a dizer que oferece suporte a wIPS/wIDS apenas, não apresentando a comprovação do subitem abaixo.

- 1.3.15. Deve implementar a configuração de um rádio do Ponto de Acesso como um "Sensor wIPS" da rede sem fio, com a finalidade de monitorar ataques à rede sem fio de uma determinada região;

No entanto, esclarecemos que, foi comprovado que o modelo de Access Point ofertado (AriEngine 6776-57T) possui sistema de prevenção de intrusão (WIPS), conforme abaixo na imagem extraída do datasheet, página 5, na seção de recursos de segurança:

<https://e.huawei.com/br/documents/products/enterprise-network/f74dc124f31c4a3eb0c8b4ea77cf1efe>



The screenshot displays the Huawei website's product page for the AirEngine 6776-57T Access Point. The page title is "Huawei AirEngine 6776-57T Access Point Datasheet". The navigation bar includes links for "Produtos e Soluções", "Aprendizagem e suporte técnico", "Parceiros", "Como comprar", and "Sobre a Huawei". The main content area shows the "Security features" section, which lists various security protocols and features. A red box highlights the "Wireless intrusion detection system (WIDS) and wireless intrusion prevention system (WIPS)" feature, which includes rogue device detection and containment, attack detection and dynamic blacklist, and STA/AP blacklist and whitelist.

Download(0.7MB) Share

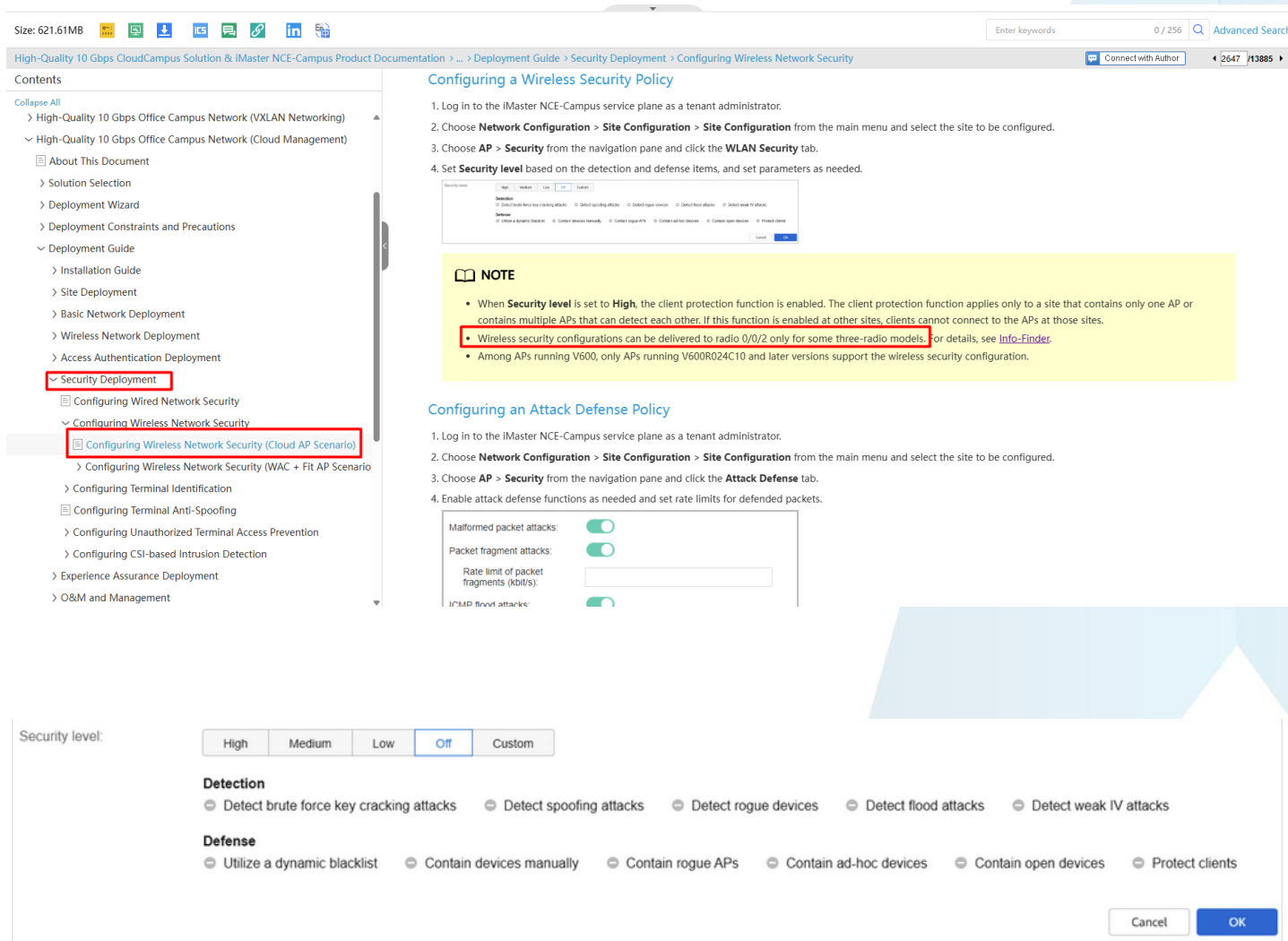
5 / 14

Security features

- VIP FastPass, per-packet power control
- Open system authentication
- WPA2-PSK authentication and encryption (WPA2-Personal)
- WPA2-802.1X authentication and encryption (WPA2-Enterprise)
- WPA3-SAE authentication and encryption (WPA3-Personal)
- WPA3-802.1X authentication and encryption (WPA3-Enterprise)
- WPA-WPA2 hybrid authentication
- WPA2-WPA3 hybrid authentication
- WPA/WPA2/WPA2-PPSK authentication and encryption
- WPA/WPA2/WPA2-DPSK authentication and encryption
- WAPI authentication and encryption
- Wireless intrusion detection system (WIDS) and wireless intrusion prevention system (WIPS), including rogue device detection and containment, attack detection and dynamic blacklist, and STA/AP blacklist and whitelist
- 802.1X authentication, MAC address authentication, and Portal authentication
- DHCP snooping
- 802.11w Protected Management Frames (PMF)
- CAPWAP DTLS data encryption and decryption
- URL filtering
- MACsec@ Uplink Ethernet port
- Secure boot
- Support the following encryption protocols: CCMP/AES TKIP
- SSL and TLS:
- RC4 128-bit
- RSA 1024-bit
- RSA 2048-bit

Adicionalmente, temos abaixo a comprovação de que o recurso está disponível para aplicação no Access Point ofertado (AirEngine 6776-57T).

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100516678&id=EN-US_TOPIC_0000001186150892



The screenshot displays the Huawei support page for configuring wireless network security. The left sidebar shows the 'Contents' menu with 'Security Deployment' and 'Configuring Wireless Network Security (Cloud AP Scenario)' highlighted. The main content area, titled 'Configuring a Wireless Security Policy', lists four steps: logging in, navigating to 'Site Configuration', selecting 'WLAN Security', and setting the security level. A 'NOTE' box specifies that when the security level is 'High', client protection is enabled, and wireless security configurations are only delivered to radio 0/0/2 on three-radio models. Below this, the 'Configuring an Attack Defense Policy' section shows a configuration window with 'Security level' set to 'Off'. The 'Detection' section includes options for brute force key cracking, spoofing, rogue devices, flood attacks, and weak IV attacks. The 'Defense' section includes options for dynamic blacklist, manual containment, rogue APs, ad-hoc devices, open devices, and client protection. The bottom of the configuration window shows 'Cancel' and 'OK' buttons.

O modelo ofertado AirEngine 6776-57T possui três rádios e atende ao item 1.3.15. do Anexo I da Especificação Técnica.

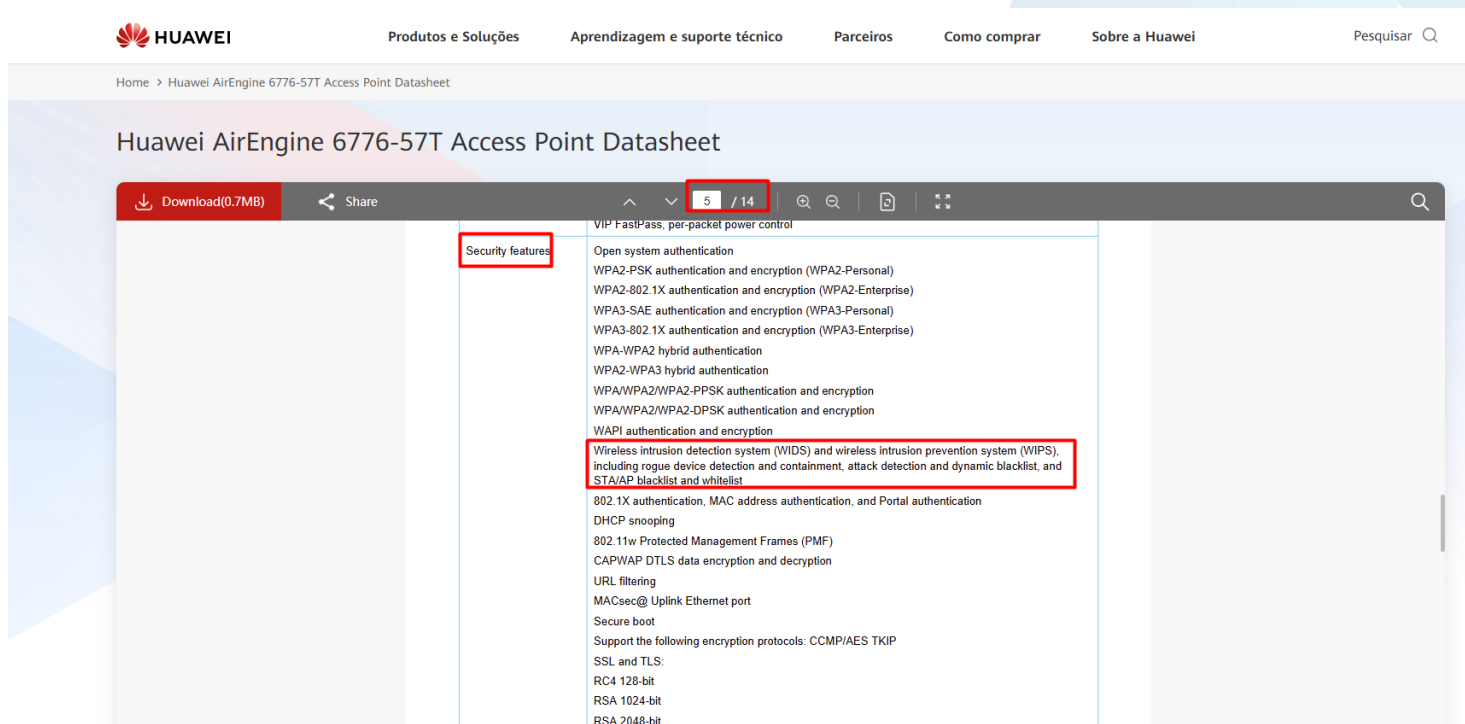
4.5) Do suposto não atendimento ao subitem 1.3.16. do Anexo I – Especificação Técnica

Aduz a Recorrente **TELESUL** que no documento apresentado, a Recorrida **3CORP** não demonstrou que o access-point pode fazer a monitoração de todos os espectros, implementando a configuração como sensor seja em tempo integral, seja em modo compartilhado, limitando-se a dizer que oferece suporte a WIPS/WIDS apenas, não apresentando a comprovação do subitem abaixo.

- 1.3.16, Deve implementar a monitoração de todos os canais nos espectros 2,4GHz, 5GHz e 6 GHz. O Ponto de Acesso deve implementar a configuração como sensor em tempo integral ou como sensor em modo compartilhado com atendimento de tráfego de cliente sem fio;

No entanto, esclarecemos que, foi comprovado que o modelo de Access Point ofertado (AriEngine 6776-57T) possui sistema de prevenção de intrusão (WIPS), conforme abaixo na imagem extraída do datasheet, página 5, na seção de recursos de segurança:

<https://e.huawei.com/br/documents/products/enterprise-network/f74dc124f31c4a3eb0c8b4ea77cf1efe>



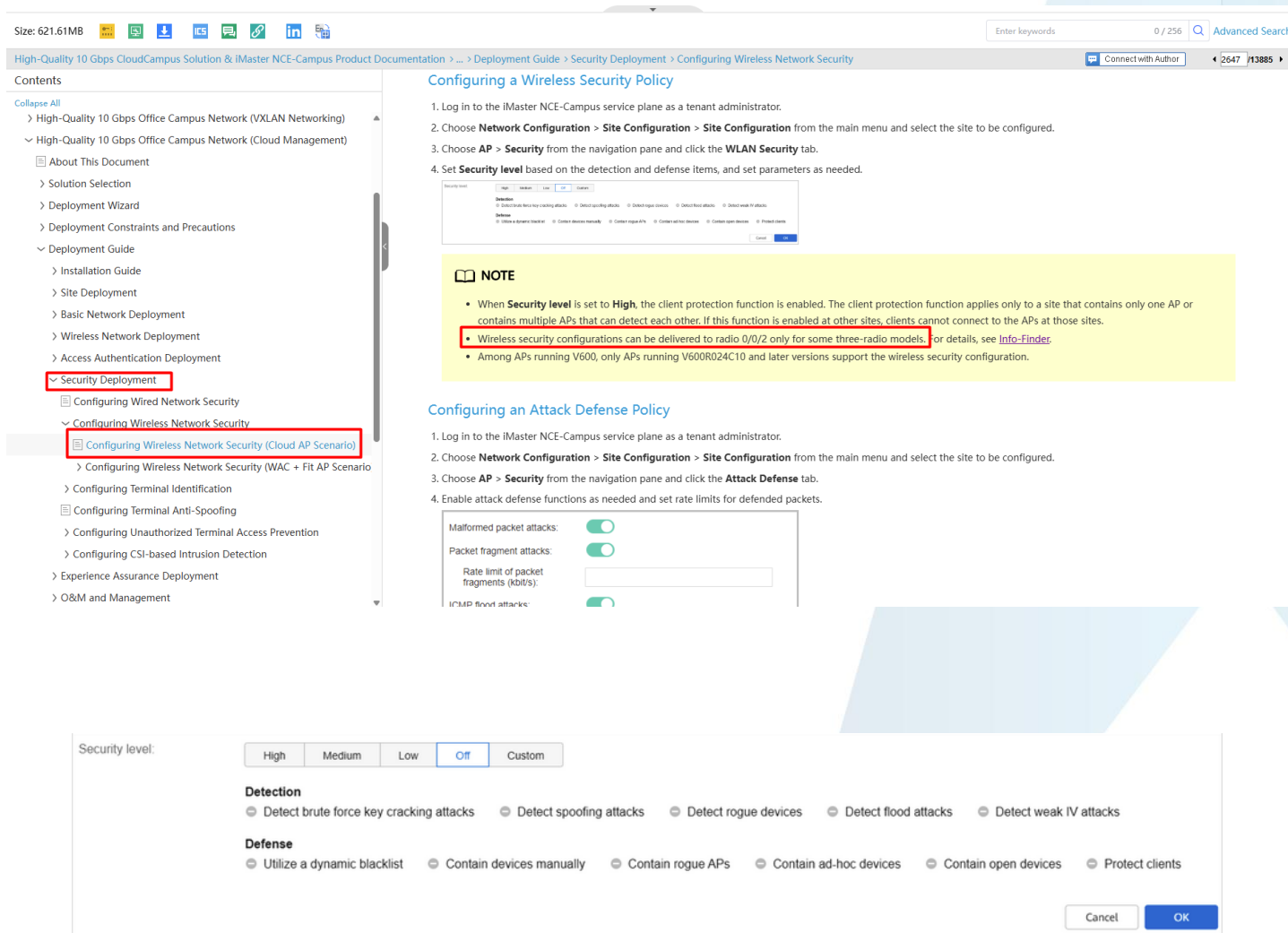
The screenshot displays the Huawei AirEngine 6776-57T Access Point Datasheet, specifically page 5, which details security features. The document is viewed in a web browser, with the page number '5 / 14' visible in the top right corner. The 'Security features' section is highlighted with a red box, and the 'Wireless intrusion detection system (WIDS) and wireless intrusion prevention system (WIPS)' feature is also highlighted with a red box. The features listed include:

- Open system authentication
- WPA2-PSK authentication and encryption (WPA2-Personal)
- WPA2-802.1X authentication and encryption (WPA2-Enterprise)
- WPA3-SAE authentication and encryption (WPA3-Personal)
- WPA3-802.1X authentication and encryption (WPA3-Enterprise)
- WPA-WPA2 hybrid authentication
- WPA2-WPA3 hybrid authentication
- WPA/WPA2/WPA2-PPSK authentication and encryption
- WPA/WPA2/WPA2-DPSK authentication and encryption
- WAPI authentication and encryption
- Wireless intrusion detection system (WIDS) and wireless intrusion prevention system (WIPS), including rogue device detection and containment, attack detection and dynamic blacklist, and STA/AP blacklist and whitelist**
- 802.1X authentication, MAC address authentication, and Portal authentication
- DHCP snooping
- 802.11w Protected Management Frames (PMF)
- CAPWAP DTLS data encryption and decryption
- URL filtering
- MACsec@ Uplink Ethernet port
- Secure boot
- Support the following encryption protocols: CCMP/AES TKIP
- SSL and TLS:
- RC4 128-bit
- RSA 1024-bit
- RSA 2048-bit

Adicionalmente, temos abaixo a comprovação de que o recurso está disponível para aplicação no Access Point ofertado (AirEngine 6776-57T).

Por se tratar de uma “policy” tal recurso pode ser configurado de forma integral ou em modo compartilhado.

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100516678&id=EN-US_TOPIC_0000001186150892



The screenshot displays the Huawei iMaster NCE-Campus documentation and configuration interface. The left sidebar shows the 'Contents' section with 'Security Deployment' highlighted. The main content area is titled 'Configuring a Wireless Security Policy' and includes a list of steps: 1. Log in to the iMaster NCE-Campus service plane as a tenant administrator. 2. Choose **Network Configuration > Site Configuration > Site Configuration** from the main menu and select the site to be configured. 3. Choose **AP > Security** from the navigation pane and click the **WLAN Security** tab. 4. Set **Security level** based on the detection and defense items, and set parameters as needed.

Below the steps, there is a 'NOTE' section with the following information:

- When **Security level** is set to **High**, the client protection function is enabled. The client protection function applies only to a site that contains only one AP or contains multiple APs that can detect each other. If this function is enabled at other sites, clients cannot connect to the APs at those sites.
- Wireless security configurations can be delivered to radio 0/0/2 only for some three-radio models. For details, see [Info-Finder](#).
- Among APs running V600, only APs running V600R024C10 and later versions support the wireless security configuration.

The bottom section of the screenshot shows the 'Configuring an Attack Defense Policy' steps: 1. Log in to the iMaster NCE-Campus service plane as a tenant administrator. 2. Choose **Network Configuration > Site Configuration > Site Configuration** from the main menu and select the site to be configured. 3. Choose **AP > Security** from the navigation pane and click the **Attack Defense** tab. 4. Enable attack defense functions as needed and set rate limits for defended packets.

The configuration interface shows the following settings:

- Security level:** High, Medium, Low, **Off**, Custom
- Detection:** Detect brute force key cracking attacks, Detect spoofing attacks, Detect rogue devices, Detect flood attacks, Detect weak IV attacks
- Defense:** Utilize a dynamic blacklist, Contain devices manually, Contain rogue APs, Contain ad-hoc devices, Contain open devices, Protect clients

The interface includes 'Cancel' and 'OK' buttons at the bottom right.

O modelo ofertado AirEngine 6776-57T possui três rádios e atende ao item 1.3.15. do Anexo I da Especificação Técnica.

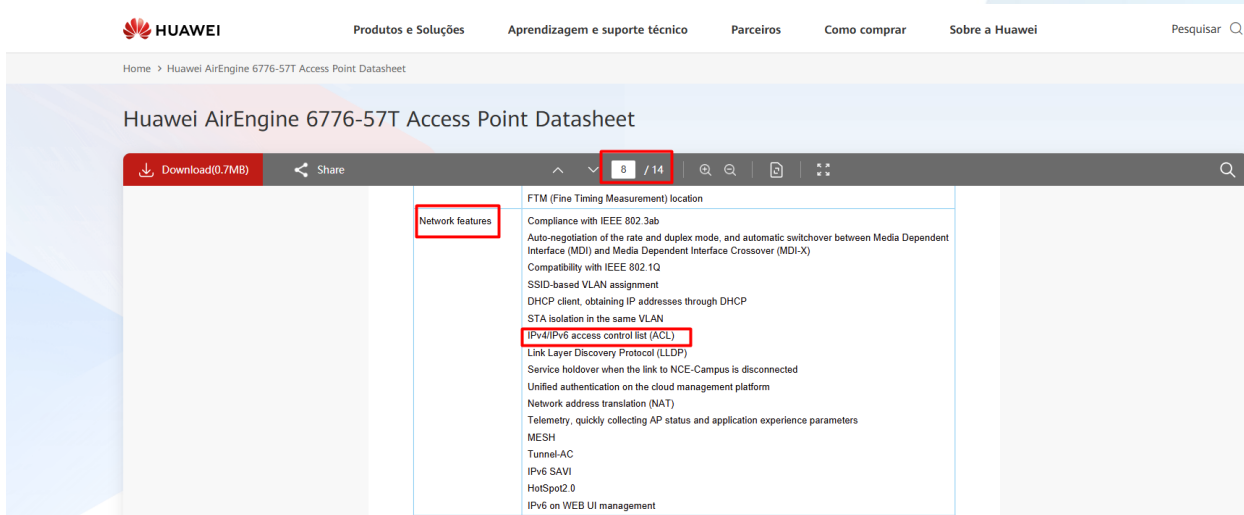
4.6) Do suposto não atendimento ao subitem 1.4.1. do Anexo I – Especificação Técnica

Aduz a Recorrente **TELESUL** que a comprovação de dual-stack não foi atendida, e que portanto, não comprovou o subitem abaixo.

1.4.1. Permitir a associação de clientes IPv4 e IPv6 em pilha dupla (dual stack);

No entanto, esclarecemos que, foi comprovado que o modelo de Access Point ofertado (AriEngine 6776-57T) com a demonstração de um recurso (IPv4/IPv6 access control list (ACL) que pode ser configurado para funcionar de forma simultânea, conforme página 8 do datasheet:

<https://e.huawei.com/br/documents/products/enterprise-network/f74dc124f31c4a3eb0c8b4ea77cf1efe>



Adicionalmente, apresentamos comprovação de que o dual-stack pode ser implementado no ambiente, com exemplo de instalação documentado em plataforma oficial do Fabricante Huawei:

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100460176&id=EN-US_TOPIC_000002089082329

Abaixo imagem extraída do link acima confirmando o atendimento ao item 1.4.1. do Anexo I – Especificação Técnica.

Size: 592.11MB

High-Quality 10 Gbps CloudCampus Solution & iMaster NCE-Campus Product Documentation > ... > High-Quality 10 Gbps Office Campus Network (Cloud Management) > Deployment Wizard > Egress Gateway + LSW + Cloud AP Networking Solution

Contents

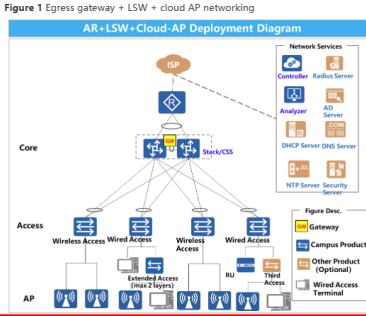
- > Deployment Wizard: External Gateway + Layer 2 VXLAN Deployed Across Core and Access Layers (Stacking)
- > Deployment Constraints and Precautions
- > Deployment Guide
- > High-Quality 10 Gbps Office Campus Network (Cloud Management)
 - > About This Document
 - > Solution Selection
 - > Deployment Wizard
 - > Deployment Process
 - > Single-AP Networking Solution
 - > Single-AR Networking Solution
 - > AR + AP Networking Solution
 - > Egress Gateway + LSW + Cloud AP Networking Solution
 - [Recommended] [Multi-GE + Wi-Fi 7] [Premium] 2000 Clients (AR6710-H + S6700-H + S5755-H + Wi-Fi 7 AP)
 - [Recommended] [Multi-GE + Wi-Fi 7] [Standard] 1000 Clients (AR6710-L + S5735-L-V2 + Wi-Fi 7 AP)
 - [V200] 2000 Clients (AR651 + S67 + S57 + AP)
 - [V600] 2000 Clients (AR6710-H + S67 + S57 + AP)
 - [V600] 1000 Clients (AR6710-L + S57 + AP)
 - [V200] 1000 Clients (AR651 + S57 + AP)
 - > Egress Gateway + LSW + WAC + Fit AP Networking Solution
- > Deployment Constraints and Precautions

Networking Overview

The baseline is the egress gateway + LSW + cloud AP networking using V600 devices. An AR functions as the egress gateway, and core switches function as user gateways.

The egress gateway AR provides egress features such as WAN access and NAT. Core switches function as user gateways and provide gateway features such as DHCP. Layer 2 switches provide extended PoE access and wired client access functions. APs provide access for wireless clients at the site.

Figure 1 Egress gateway + LSW + cloud AP networking



Number of users: < 2000 (IPv4/IPv6 dual-stack users); < 4000 (IPv4 single-stack users)

Deployment design:
I. Deployment of network management services

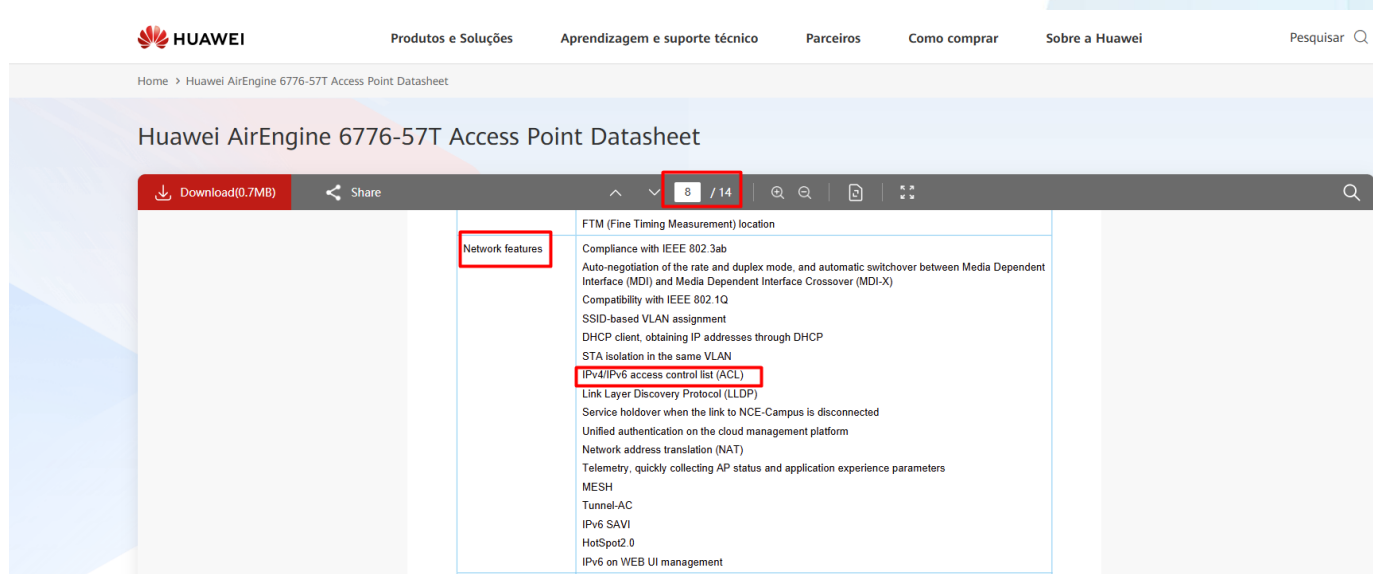
4.7) Do suposto não atendimento ao subitem 1.5.6. do Anexo I – Especificação Técnica

Aduz a Recorrente **TELESUL** que no documento apresentado, a Recorrida **3CORP** não comprovou a possibilidade de criação de filtros por MAC ou protocolos, não atendendo assim o subitem abaixo.

1.5.6. Implementar filtros baseados em protocolos e em endereços MAC;

No entanto, esclarecemos que, foi comprovado que o modelo de Access Point ofertado (AriEngine 6776-57T) com a demonstração de suporte à ACL (IPv4/IPv6 access control list (ACL), conforme página 8 do datasheet:

<https://e.huawei.com/br/documents/products/enterprise-network/f74dc124f31c4a3eb0c8b4ea77cf1efe>



The screenshot displays the Huawei website's product page for the AirEngine 6776-57T Access Point. The page title is "Huawei AirEngine 6776-57T Access Point Datasheet". The navigation bar includes links for "Produtos e Soluções", "Aprendizagem e suporte técnico", "Parceiros", "Como comprar", and "Sobre a Huawei". The main content area shows a list of network features, with "IPv4/IPv6 access control list (ACL)" highlighted in a red box. Other features listed include FTM (Fine Timing Measurement) location, Compliance with IEEE 802.3ab, Auto-negotiation of the rate and duplex mode, and various protocols like DHCP, LLDP, and NAT.

Adicionalmente, apresentamos comprovação de Classificação suportada pelo Access Point ofertado, conforme link e imagens abaixo:

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100510642&id=EN-US_CONCEPT_0000001264831289

Size: 538.12MB

WLAN AP AirEngine X700 Product Documentation > ... > IP Addresses and Services Configuration > ACL Configuration > Understanding ACL

Contents

- Application Identification Configuration
- ACL Configuration
 - Overview of ACL
 - Understanding ACL
 - ACL Classification**
 - ACL Matching Process
 - ACL Configuration Guidelines
 - Configuration Precautions for ACL
 - Default Settings for ACL
 - Creating a Time Range in Which an ACL is Applied
 - Configuring an ACL
 - Applying an ACL
 - Modifying an ACL
 - Deleting an ACL
- ACL6 Configuration
- ND Configuration
- IPsec Configuration

ACL Classification

Table 1 describes ACL classification by function.

Table 1 ACL classification

Category	Function	Number Range
Basic ACL	Defines packet filtering rules based on information such as source IPv4 addresses, fragment information, and time ranges.	2000 to 2999
Advanced ACL	Defines packet filtering rules based on information such as source and destination IPv4 addresses, IP protocol types, TCP source and destination port numbers, UDP source and destination port numbers, fragment information, and time ranges.	3000 to 3999
Layer 2 ACL	Defines packet filtering rules based on the information in Ethernet frame headers, such as source and destination MAC addresses, VLAN IDs, and Layer 2 protocol types.	4000 to 4999
User ACL	Defines rules based on information about IP packets to implement packet filtering. Such information includes source IP addresses or source UCL groups, destination IP addresses or destination UCL groups, IP protocol types, ICMP types, TCP source/destination port numbers, UDP source/destination port numbers, and effective time ranges.	6000 to 9999

You can create a numbered or named ACL.

- A named ACL is created using a name. This type of ACL is named in the format of name + number. The number can be manually specified or automatically assigned by the system. If a number is not manually specified for an ACL, the system assigns the largest number available for the ACL.

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100510642&id=EN-US_CONCEPT_0000002072013201

Size: 538.12MB

WLAN AP AirEngine X700 Product Documentation > ... > IP Addresses and Services Configuration > ACL6 Configuration > Understanding ACL6

Contents

- Application Identification Configuration
- ACL Configuration
 - Overview of ACL
 - Understanding ACL
 - ACL Classification
 - ACL Matching Process
 - ACL Configuration Guidelines
 - Configuration Precautions for ACL
 - Default Settings for ACL
 - Creating a Time Range in Which an ACL is Applied
 - Configuring an ACL
 - Applying an ACL
 - Modifying an ACL
 - Deleting an ACL
- ACL6 Configuration
 - Overview of ACL6
 - Understanding ACL6
 - ACL6 Classification**
 - ACL6 Matching Process
 - ACL6 Configuration Guidelines
 - Configuration Precautions for ACL6

ACL6 Classification

Table 1 describes ACL6 classification by function.

Table 1 ACL6 classification

Category	Function	ACL Number
Advanced ACL6	Defines packet filtering rules based on information such as source and destination IPv6 addresses, IP protocol types, TCP source and destination port numbers, UDP source and destination port numbers, fragment information, and time ranges.	3000 to 3999
User ACL6	Defines rules based on information about IPv6 packets to implement packet filtering. Such information includes source IPv6 addresses or source UCL groups, destination IPv6 addresses or destination UCL groups, IPv6 protocol types, ICMP types, TCP source/destination port numbers, UDP source/destination port numbers, and effective time ranges.	6000 to 9999

You can create a numbered or named ACL6.

- A named ACL6 is created using a name. This type of ACL6 is named in the format of name + number. The number can be manually specified or automatically assigned by the system. If a number is not manually specified for an ACL6, the system assigns the largest number available for the ACL6.

NOTE

Once a named ACL6 is created, its name cannot be changed. If a different name is required, the named ACL6 must be deleted and a new one created.

- A numbered ACL6 is created using a number.

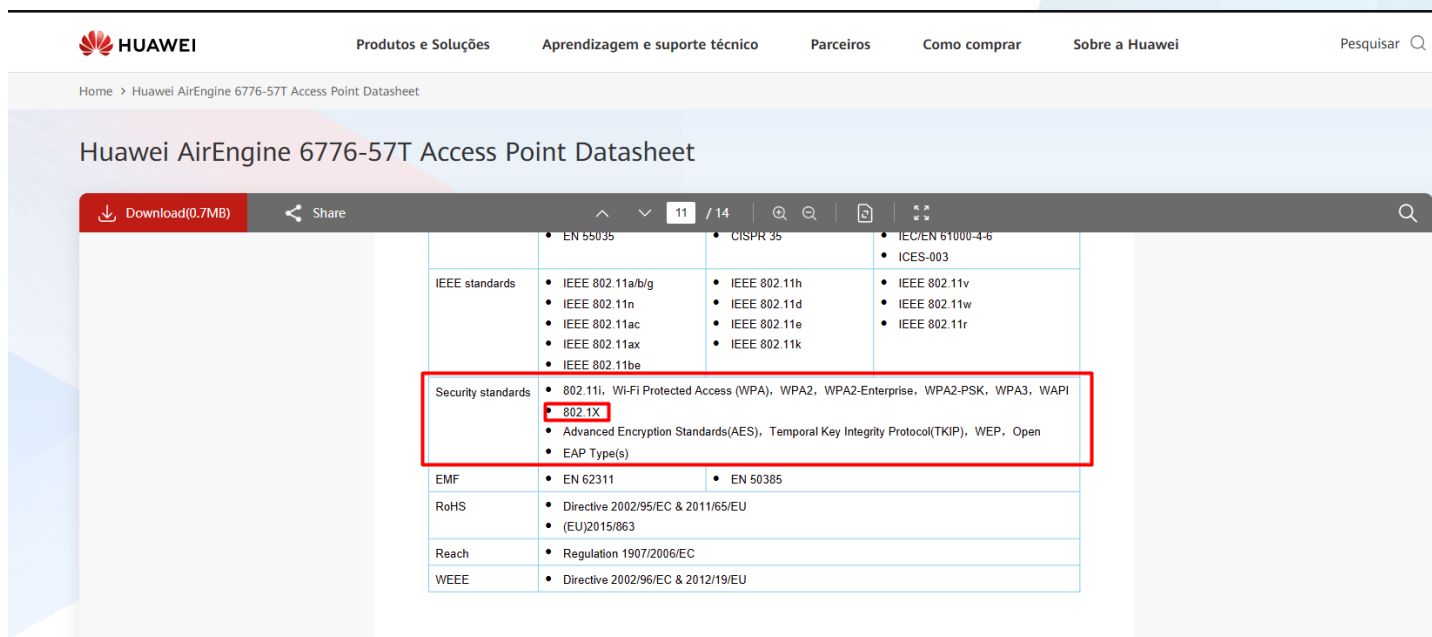
4.8) Do suposto não atendimento ao subitem 1.5.9. do Anexo I – Especificação Técnica

Aduz a Recorrente **TELESUL** que não há comprovação de que o access-point possui o suplicante carregado para ser autorizado a entrar na rede cabeada, indicando uma falha na integração e segurança do acesso, não atendendo assim o subitem abaixo.

1,5,9. Deve implementar suplicante 802.1X para identificar os Pontos de Acesso ao serem conectados na estrutura de rede cabeada;

No entanto, esclarecemos que, foi comprovado que o modelo de Access Point ofertado (AriEngine 6776-57T) atende à especificação solicitada, uma vez que possui suporte ao 802.1X, conforme indicação no datasheet, página 11, demonstrado no link e imagem abaixo:

<https://e.huawei.com/br/documents/products/enterprise-network/f74dc124f31c4a3eb0c8b4ea77cf1efe>

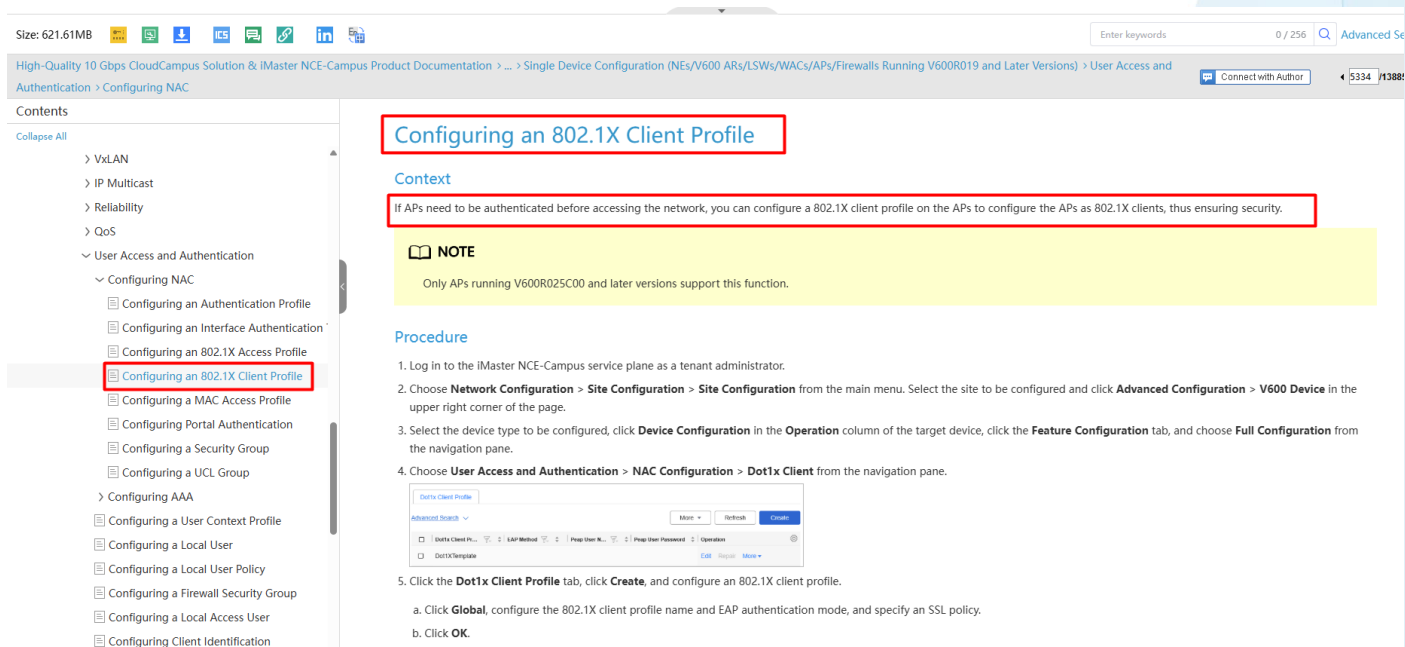


The screenshot shows the Huawei AirEngine 6776-57T Access Point Datasheet. The 'Security standards' section is highlighted with a red box, and '802.1X' is specifically marked within it.

Standard	Details
IEEE standards	<ul style="list-style-type: none"> IEEE 802.11a/b/g IEEE 802.11n IEEE 802.11ac IEEE 802.11ax IEEE 802.11be
Security standards	<ul style="list-style-type: none"> 802.11i, Wi-Fi Protected Access (WPA), WPA2, WPA2-Enterprise, WPA2-PSK, WPA3, WAPI 802.1X Advanced Encryption Standards(AES), Temporal Key Integrity Protocol(TKIP), WEP, Open EAP Type(s)
EMF	<ul style="list-style-type: none"> EN 62311 EN 50385
RoHS	<ul style="list-style-type: none"> Directive 2002/95/EC & 2011/65/EU (EU)2015/863
Reach	<ul style="list-style-type: none"> Regulation 1907/2006/EC
WEEE	<ul style="list-style-type: none"> Directive 2002/96/EC & 2012/19/EU

Adicionalmente, apresentamos comprovação de configuração via Gerência de perfil a ser aplicado no Access Point para conexão à rede cabeada:

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100516678&id=EN-US_TOPIC_0000002230971637



The screenshot displays the Huawei iMaster NCE-Campus configuration interface. The left sidebar shows the navigation tree with 'Configuring an 802.1X Client Profile' selected. The main content area is titled 'Configuring an 802.1X Client Profile' and includes a 'Context' section stating: 'If APs need to be authenticated before accessing the network, you can configure a 802.1X client profile on the APs to configure the APs as 802.1X clients, thus ensuring security.' Below this is a 'NOTE' box indicating that only APs running V600R025C00 and later versions support this function. The 'Procedure' section lists five steps: 1. Log in to the iMaster NCE-Campus service plane as a tenant administrator. 2. Choose **Network Configuration** > **Site Configuration** > **Site Configuration** from the main menu. Select the site to be configured and click **Advanced Configuration** > **V600 Device** in the upper right corner of the page. 3. Select the device type to be configured, click **Device Configuration** in the **Operation** column of the target device, click the **Feature Configuration** tab, and choose **Full Configuration** from the navigation pane. 4. Choose **User Access and Authentication** > **NAC Configuration** > **Dot1x Client** from the navigation pane. 5. Click the **Dot1x Client Profile** tab, click **Create**, and configure an 802.1X client profile. Below step 5, there are sub-steps: a. Click **Global**, configure the 802.1X client profile name and EAP authentication mode, and specify an SSL policy. b. Click **OK**.

4.9) Do suposto não atendimento ao subitem 1.5.13.1. do Anexo I – Especificação Técnica

Aduz a Recorrente **TELESUL** que o link apresentado como comprovação não comprova a aplicação da ACL dinâmica baseada nos atributos do Radius no processo de autenticação, limitando-se a explicar o processo básico de autenticação, autorização e accounting, não atendendo assim o subitem abaixo.

- 1.5.13. Deve implementar listas de controle de acesso (ACLs) baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino e endereços MAC;
1.5.13.1. Permitir a atribuição dinâmica de ACLs dependendo dos atributos RADIUS enviados durante o processo de autorização;

No entanto, esclarecemos que, foi comprovado que o modelo de Access Point ofertado (AriEngine 6776-57T) atende à especificação solicitada, uma vez que no mesmo link fornecido com a explicação do processo AAA, há a indicação de configuração dos atributos Radius que podem ser aplicados.

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100510642&id=EN-US_CONCEPT_0000002507628362


HUAWEI Enterprise Support

Size: 538.12MB

Enter keywords 0 / 256 Advanced Search

WLAN AP AirEngine X700 Product Documentation > ... > AAA Configuration > Understanding AAA > Understanding RADIUS-based AAA

Connect with Author 2380 / 1582

Contents

- Understanding AAA
 - Authentication Scheme
 - Authorization Scheme
 - Accounting Scheme
 - Understanding Local Authentication and Authorization
 - Understanding RADIUS-based AAA
 - Overview of RADIUS
 - RADIUS Packets
 - RADIUS Authentication, Authorization, and Accounting Process**
 - RADIUS Packet Retransmission Mechanism
 - RADIUS Server Selection Mechanism
 - RADIUS Server Status Detection
 - RADIUS CoA/DM
 - RADIUS Attribute Disabling and Translation**
 - RADIUS Attributes
 - RADIUS Attribute Dictionary
 - Understanding HWTACACS-based AAA
- Configuration Precautions for AAA
- AAA Configuration

RADIUS Authentication, Authorization, and Accounting Process

A device that functions as a RADIUS client collects user information (for example, user names and passwords) and sends the information to a RADIUS server. The RADIUS server then authenticates users according to the information, after which it performs authorization and accounting for the users. Figure 1 shows the information exchange process between a user, a RADIUS client, and a RADIUS server.

Figure 1 RADIUS authentication, authorization, and accounting process



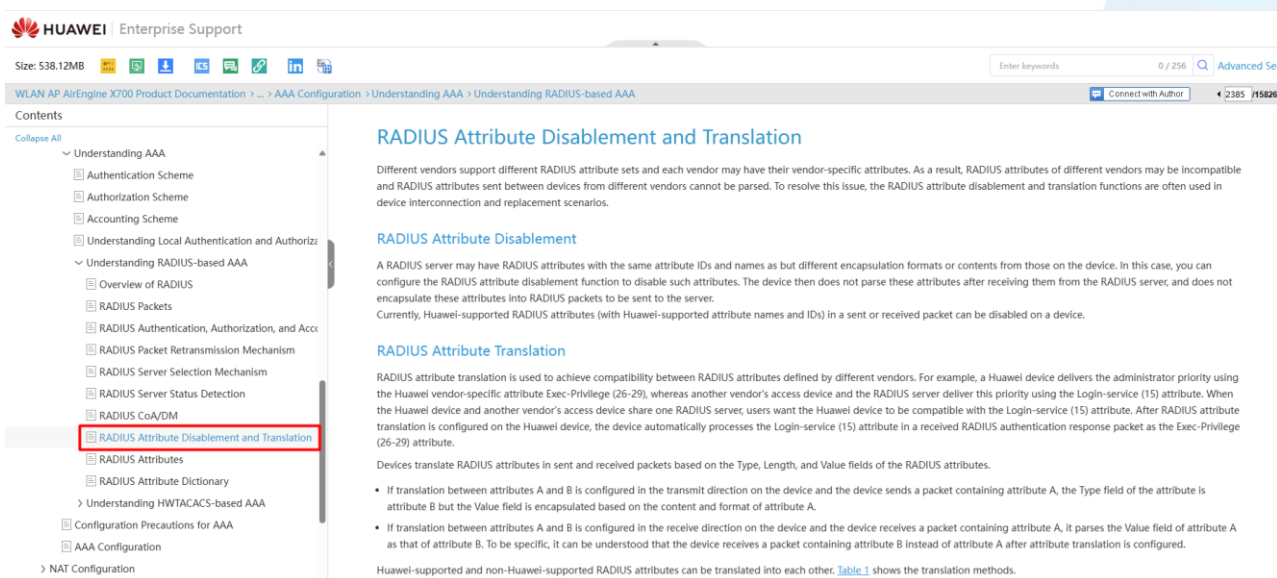
```

sequenceDiagram
    participant User
    participant Device
    participant RADIUS_server as RADIUS server

    User->>Device: 1. Enter the user name and password.
    Device->>RADIUS_server: 2. Send an Access-Request packet.
    RADIUS_server-->>Device: 3. Send an Access-Accept or Access-Reject packet.
    Device-->>User: 4. Notify the user of the authentication result.
    Device->>RADIUS_server: 5. Send an Accounting-Request(Start) packet.
    RADIUS_server-->>Device: 6. Send an Accounting-Response(Start) packet.
    Note over User, Device: 7. The user starts to access network resources.
    Device->>RADIUS_server: 8. (Optional) Send an Accounting-Request(Interim-update) packet.
    RADIUS_server-->>Device: 9. (Optional) Send an Accounting-Response(Interim-update) packet.
    Device->>RADIUS_server: 10. Request for disconnection.
    RADIUS_server-->>Device: 11. Send an Accounting-Request(Stop) packet.
    RADIUS_server-->>Device: 12. Send an Accounting-Response(Stop) packet.
    Device-->>User: 13. Notify the user that access ends.
    
```

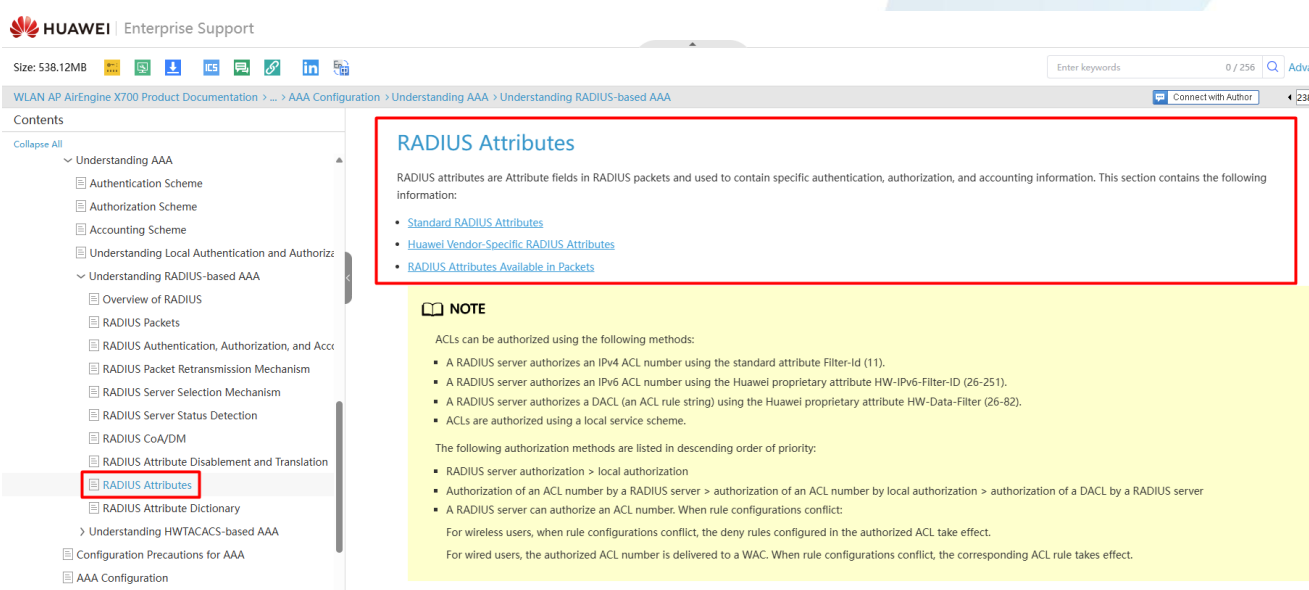

Sendo assim, adicionalmente apresentamos os atributos que podem ser aplicados aos dispositivos de forma dinâmica, atendendo assim ao item 1.5.13.1. do Anexo I – Especificação Técnica:

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100510642&id=EN-US_CONCEPT_0000002539388085



The screenshot shows the Huawei Enterprise Support portal. The left sidebar contains a 'Contents' menu with a tree structure. Under 'Understanding RADIUS-based AAA', the item 'RADIUS Attribute Disablement and Translation' is highlighted with a red box. The main content area displays the title 'RADIUS Attribute Disablement and Translation' and a detailed explanation of how RADIUS attributes are handled by different vendors and how Huawei devices manage them. It includes sections for 'RADIUS Attribute Disablement' and 'RADIUS Attribute Translation'.

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100510642&id=EN-US_CONCEPT_0000002478991358



The screenshot shows the Huawei Enterprise Support portal. The left sidebar contains a 'Contents' menu with a tree structure. Under 'Understanding RADIUS-based AAA', the item 'RADIUS Attributes' is highlighted with a red box. The main content area displays the title 'RADIUS Attributes' and a detailed explanation of what RADIUS attributes are and how they are used. It includes a 'NOTE' section that lists various authorization methods and their priorities.

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100510642&id=EN-US_CONCEPT_0000002507788204

Size: 538.12MB

Enter keywords 0 / 256 [Advanced Search](#)

WLAN AP AirEngine X700 Product Documentation > ... > AAA Configuration > Understanding AAA > Understanding RADIUS-based AAA

Connect with Author 2387 / 15826

Contents

Collapse All

Understanding AAA

- Authentication Scheme
- Authorization Scheme
- Accounting Scheme
- Understanding Local Authentication and Authoriz...
- Understanding RADIUS-based AAA
 - Overview of RADIUS
 - RADIUS Packets
 - RADIUS Authentication, Authorization, and Acc...
 - RADIUS Packet Retransmission Mechanism
 - RADIUS Server Selection Mechanism
 - RADIUS Server Status Detection
 - RADIUS CoA/DM
 - RADIUS Attribute Disablement and Translation
 - RADIUS Attributes
 - RADIUS Attribute Dictionary**
- Understanding HWTACACS-based AAA
- Configuration Precautions for AAA
- AAA Configuration
- NAT Configuration
- Security Configuration
- QoS Configuration

RADIUS Attribute Dictionary

After a RADIUS server has the RADIUS attribute dictionary loaded, it can identify the RADIUS attributes defined by vendors. The dictionary file contains the vendor IDs, user-defined attribute IDs, attribute names, and attribute types. When a Huawei device interconnects with a RADIUS server, to allow the RADIUS server to correctly identify and process Huawei vendor-specific RADIUS attributes, the Huawei vendor-specific RADIUS attribute dictionary file must be loaded to the RADIUS server. The same RADIUS attribute ID on different products of the same vendor may represent different attribute values. Therefore, you are advised not to configure information about multiple products of the same vendor in the same RADIUS attribute dictionary file. The following table lists the steps of installing the FreeRADIUS server of Linux SUSE 12.

Configuration	Procedure	Description
Configure a local server.	Obtain the root permission.	Obtain the root permission on the Linux server where the RADIUS server is installed.
Replace the RADIUS attribute dictionary.	Open the directory where the RADIUS attribute dictionary is saved.	Open the directory <code>/usr/share/freeradius</code> on the RADIUS server.
	Replace dictionary attributes.	Replace the <code>dictionary.huawei</code> file in the original directory with the RADIUS attribute dictionary. You are advised to back up the original file and name it, for example, <code>dictionary.huawei.bak</code> .
-	Verifying the Configuration	After the replacement, restart the RADIUS server and verify that the vendor-specific RADIUS attributes take effect and the replacement is successful based on the onsite services.

NOTE

- The RADIUS attribute dictionary contains the attributes supported on all products of this series. For details about the RADIUS attributes supported by each type of product, see the RADIUS attribute list of the corresponding product.
- The attachment is the RADIUS attribute dictionary in FreeRADIUS format.

RADIUS Attribute Dictionary

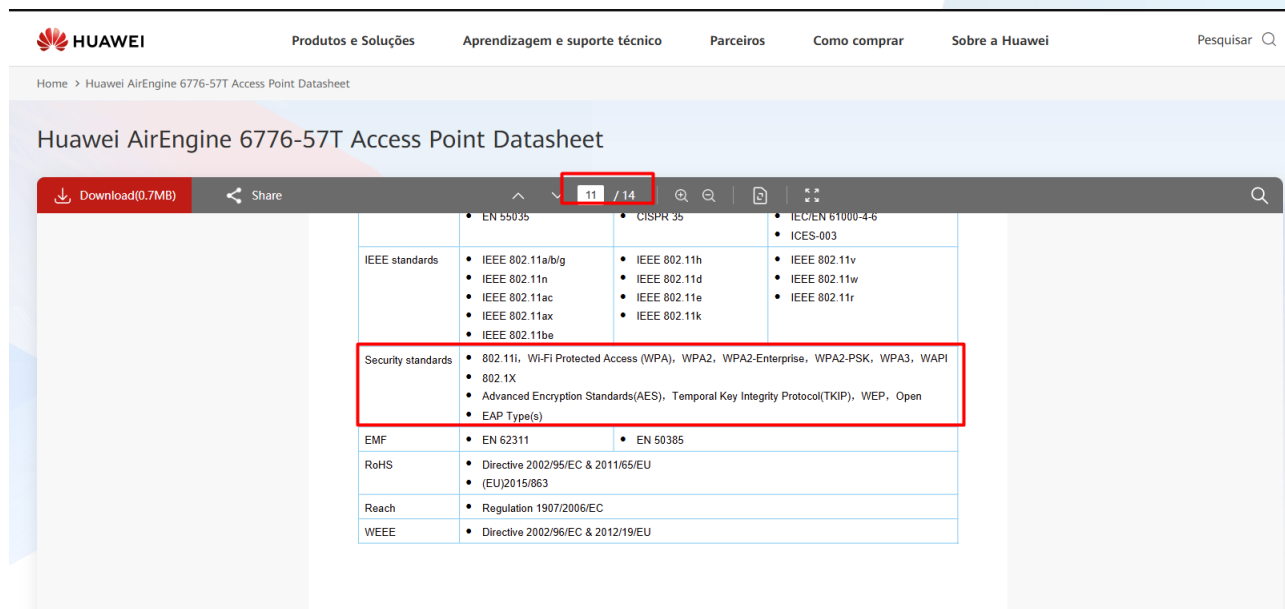
4.10) Do suposto não atendimento ao subitem 1.5.15. do Anexo I – Especificação Técnica

Aduz a Recorrente **TELESUL** que no documento apresentado como comprovação, a licitante **3CORP** se limitou a mostrar os padrões de segurança que atende no access-point, deixando de comprovar a existência da autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário, não comprovando o subitem abaixo.

1.5.15. Suportar a autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário;

No entanto, esclarecemos que, foi comprovado que o modelo de Access Point ofertado (AriEngine 6776-57T) atende à especificação solicitada, uma vez que os protocolos listados no Datasheet (WPA2/WPA3-Enterprise (802.1X)), página 11, são utilizados ao requisito descrito na Especificação Técnica:

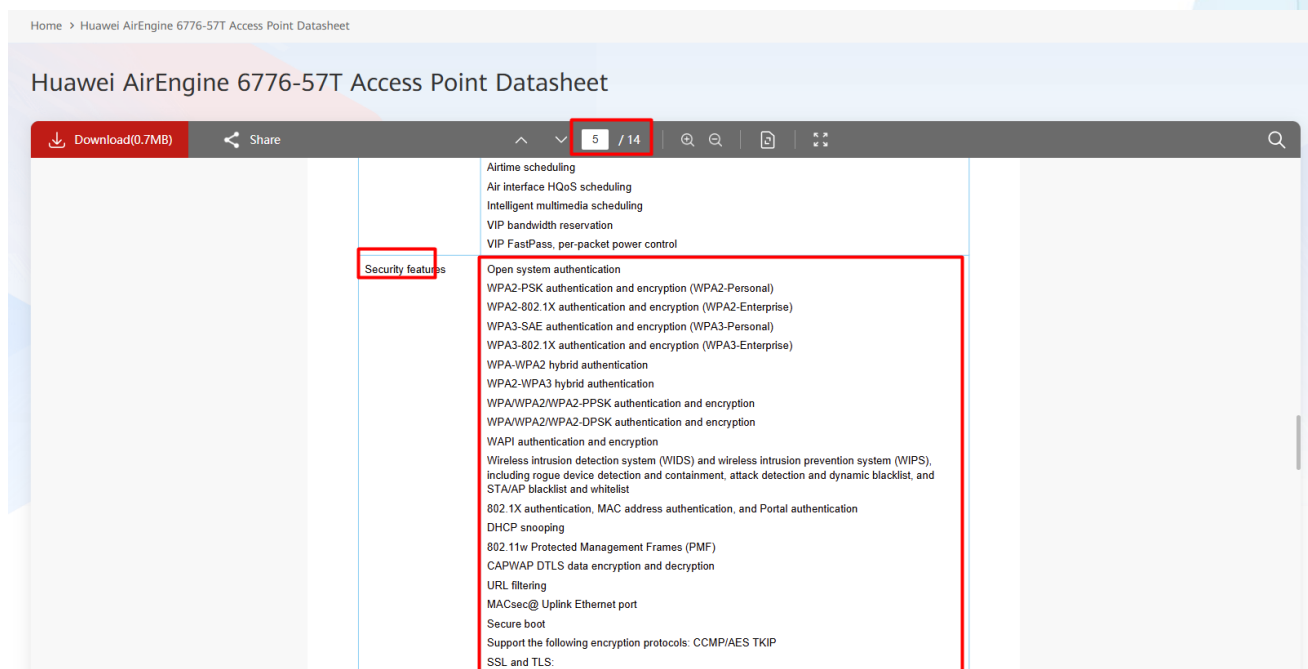
<https://e.huawei.com/br/documents/products/enterprise-network/f74dc124f31c4a3eb0c8b4ea77cf1efe>



The screenshot shows the Huawei website's product datasheet for the AirEngine 6776-57T Access Point. The page is titled "Huawei AirEngine 6776-57T Access Point Datasheet" and is page 11 of 14. A red box highlights the "Security standards" section, which lists the following protocols: 802.11i, Wi-Fi Protected Access (WPA), WPA2, WPA2-Enterprise, WPA2-PSK, WPA3, WAPI, 802.1X, Advanced Encryption Standards (AES), Temporal Key Integrity Protocol (TKIP), WEP, Open, and EAP Type(s).

Category	Standards
IEEE standards	<ul style="list-style-type: none">• EN 55035• IEEE 802.11a/b/g• IEEE 802.11n• IEEE 802.11ac• IEEE 802.11ax• IEEE 802.11be
Security standards	<ul style="list-style-type: none">• IEEE 802.11h• IEEE 802.11d• IEEE 802.11e• IEEE 802.11k• IEEE 802.11v• IEEE 802.11w• IEEE 802.11r
EMF	<ul style="list-style-type: none">• EN 55035• CISPR 35• EN 50385
RoHS	<ul style="list-style-type: none">• Directive 2002/95/EC & 2011/65/EU• (EU)2015/863
Reach	<ul style="list-style-type: none">• Regulation 1907/2006/EC
WEEE	<ul style="list-style-type: none">• Directive 2002/96/EC & 2012/19/EU

Assim como a presença dos métodos na página 5:



Cabe salientar que:

Em ambientes corporativos, os protocolos **WPA2 (Wi-Fi Protected Access 2)** e **WPA3 (Wi-Fi Protected Access 3)** são amplamente utilizados para prover segurança em redes sem fio, especialmente quando integrados a mecanismos de autenticação centralizada como **802.1X**. Ambos suportam geração dinâmica de chaves criptográficas por sessão e por usuário.

WPA2-Enterprise (802.1X / EAP)

No modo corporativo, o WPA2 opera como **WPA2-Enterprise**, utilizando o padrão **IEEE 802.1X** para controle de acesso baseado em porta, em conjunto com métodos **EAP (Extensible Authentication Protocol)**, como:

- EAP-TLS (certificados digitais)
- PEAP (Protected EAP)
- EAP-TTLS

Processo de autenticação e geração de chaves

1. O cliente (suplicante) solicita acesso ao AP (autenticador).
2. O AP encaminha a requisição para um servidor de autenticação (ex: RADIUS).
3. Após validação das credenciais do usuário (login/senha ou certificado), é estabelecida uma chave mestra:

- **PMK (Pairwise Master Key)**

4. A partir da PMK, ocorre o **4-Way Handshake**, que gera dinamicamente:
- **PTK (Pairwise Transient Key)** → exclusiva por sessão e por cliente
 - **GTK (Group Temporal Key)** → usada para tráfego broadcast/multicast

Características de segurança

- Chaves únicas por usuário e por sessão
- Renovação automática de chaves (rekeying)
- Criptografia baseada em AES-CCMP
- Dependência de servidor RADIUS

WPA3-Enterprise (802.1X aprimorado)

O WPA3 mantém o modelo 802.1X, porém introduz melhorias significativas em segurança criptográfica e proteção contra-ataques modernos.

Evoluções no processo de autenticação

- Continua utilizando EAP (ex: EAP-TLS), porém com requisitos mais fortes
- Suporte a **PMF (Protected Management Frames)** obrigatório
- Possibilidade de operação em modo **192-bit security suite** (nível governamental)

Geração dinâmica de chaves

Assim como no WPA2-Enterprise:

- Cada usuário autenticado gera uma **PMK exclusiva**
- O handshak gera **PTK única por sessão**
- Chaves são derivadas com algoritmos mais robustos (ex: SHA-384 no modo 192-bit)

Melhorias de segurança

- Proteção contra-ataques de dicionário offline
- Forward secrecy (dependendo do método EAP)
- Criptografia mais forte (GCMP-256, CNSA suite)
- Integridade reforçada dos frames de gerenciamento

Dessa forma demonstramos o atendimento ao item 1.5.15. do Anexo I – Especificação Técnica.

4.11) Do suposto não atendimento ao subitem 1.6.4. do Anexo I – Especificação Técnica

Aduz a Recorrente **TELESUL** que no documento apresentado, o texto usado como comprovação não faz menção a conectividade entre access-point e controladora, não faz menção a qual o tipo da comunicação, deixando de comprovar o subitem abaixo.

1.6.4. O Ponto de Acesso poderá estar diretamente ou remotamente conectado à Controladora WLAN, inclusive via roteamento nível 3 da camada OSI;

No entanto, esclarecemos que, ponto de acesso Huawei AirEngine 6776-57T opera de forma integrada à plataforma de gerenciamento centralizado Huawei iMaster NCE-CloudCampus na modalidade em nuvem, o que caracteriza uma arquitetura de controle desacoplada do plano de dados. Nesse modelo, a inteligência de controle WLAN é concentrada na controladora lógica hospedada na nuvem, enquanto o AP atua como elemento de acesso, estabelecendo comunicação segura com o controlador por meio da rede IP.

A topologia adotada demonstra que o gerenciamento do AP ocorre de forma remota, não sendo necessária conectividade direta em camada 2 com a controladora WLAN. O tráfego de controle entre o AP e a plataforma NCE-CloudCampus é encapsulado e transportado sobre infraestrutura IP, permitindo que o dispositivo esteja conectado à controladora inclusive por meio de roteamento em camada 3 do modelo OSI. Esse comportamento é típico de arquiteturas baseadas em CAPWAP (Control and Provisioning of Wireless Access Points), nas quais o AP estabelece túneis seguros até o controlador independentemente da localização física na rede.

Dessa forma, o Huawei AirEngine 6776-57T atende plenamente ao requisito especificado, uma vez que pode ser implantado em cenários distribuídos, conectando-se à controladora WLAN na nuvem por redes locais ou WAN, com suporte a comunicação via camada 3. Isso garante flexibilidade de implantação, escalabilidade e gerenciamento centralizado, mesmo em ambientes onde os pontos de acesso estejam geograficamente dispersos ou segmentados por domínios de roteamento distintos.

Abaixo comprovação da arquitetura proposta, demonstrando atendimento ao item 1.6.4. do Anexo I – Especificação Técnica:

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100516678&id=EN-US_TOPIC_0000002089082329

Size: 621.61MB

Configuring an AP as an 802.11n 37 / 256 Advanced Search

High-Quality 10 Gbps CloudCampus Solution & iMaster NCE-Campus Product Documentation > ... > High-Quality 10 Gbps Office Campus Network (Cloud Management) > Deployment Wizard > Egress Gateway + LSW + Cloud AP

Networking Solution

Contents

Collapse All

Deployment Wizard

Deployment Process

Single-AP Networking Solution

Single-AR Networking Solution

AR + AP Networking Solution

Egress Gateway + LSW + Cloud AP Networking Solution

[Recommended] [Multi-GE + Wi-Fi 7] [Premium] 2000 Clients (AR6710-H + S6700-H + S5755-H + Wi-Fi 7 AP)

[Recommended] [Multi-GE + Wi-Fi 7] [Standard] 1000 Clients (AR6710-

[V200] 2000 Clients (AR651 + S67 + S57 + AP)

[V600] 2000 Clients (AR6710-H + S67 + S57 + AP)

[V600] 1000 Clients (AR6710-L + S57 + AP)

[V200] 1000 Clients (AR651 + S57 + AP)

Egress Gateway + LSW + WAC + Fit AP Networking Solution

Deployment Constraints and Precautions

Deployment Guide

High-Quality 10 Gbps Office Campus Network (Campus Interconnection)

High-Quality Fully-Wireless Production Campus Network

High-Quality High-Reliability Production Campus Network

High-Quality Simplified Network

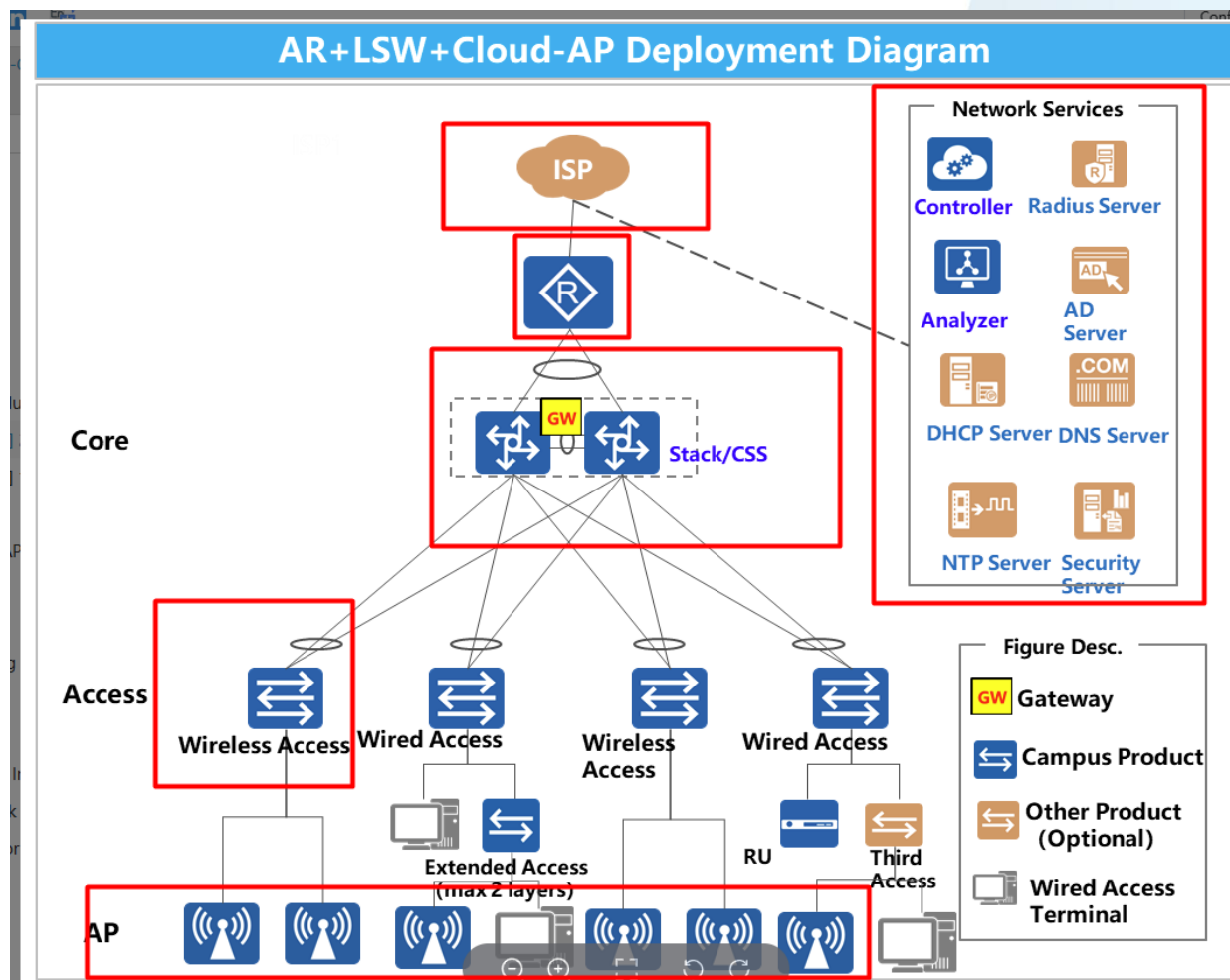
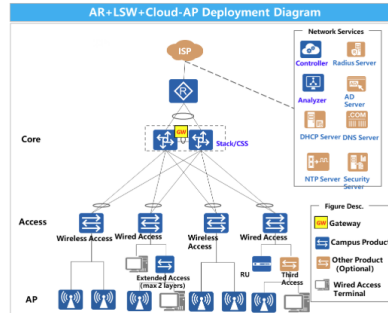
High-Quality Zero-Roaming Distributed Wi-Fi

[Recommended] [Multi-GE + Wi-Fi 7] [Premium] 2000 Clients (AR6710-H + S6700-H + S5755-H + Wi-Fi 7 AP)

Networking Overview

The baseline is the egress gateway + LSW + cloud AP networking using V600 devices. An AR functions as the egress gateway, and core switches function as user gateways. The egress gateway AR provides egress features such as WAN access and NAT. Core switches function as user gateways and provide gateway features such as DHCP. Layer 2 switches provide extended PoE access and wired client access functions. APs provide access for wireless clients at the site.

Figure 1 Egress gateway + LSW + cloud AP networking



4.12) Do suposto não atendimento ao subitem 1.6.6. do Anexo I – Especificação Técnica

Aduz a Recorrente **TELESUL** que o link apresentado, não comprovou a conectividade com controllers redundantes, nem o processo em caso de falha de uma controller, utilizando o texto de outra funcionalidade, não comprovando assim o subitem abaixo.

1.6.6. Deve possuir suporte a controladoras WLAN redundantes, no caso de falha da controladora primária, o ponto de acesso deverá se conectar automaticamente a uma controladora secundária;

No entanto, esclarecemos que, a plataforma Huawei NCE-CloudCampus, quando utilizada na modalidade em nuvem, é projetada com arquitetura distribuída e resiliente, garantindo mecanismos robustos de **redundância e alta disponibilidade (HA – High Availability)**.

Nesse modelo, os serviços de gerenciamento são hospedados em infraestrutura de data centers geograficamente distribuídos, com **replicação de dados em múltiplas zonas de disponibilidade (AZs)**. Isso assegura que, em caso de falha de um nó, instância ou até mesmo de um data center completo, as demais instâncias assumam automaticamente a operação, sem interrupção perceptível dos serviços.

A solução utiliza conceitos como:

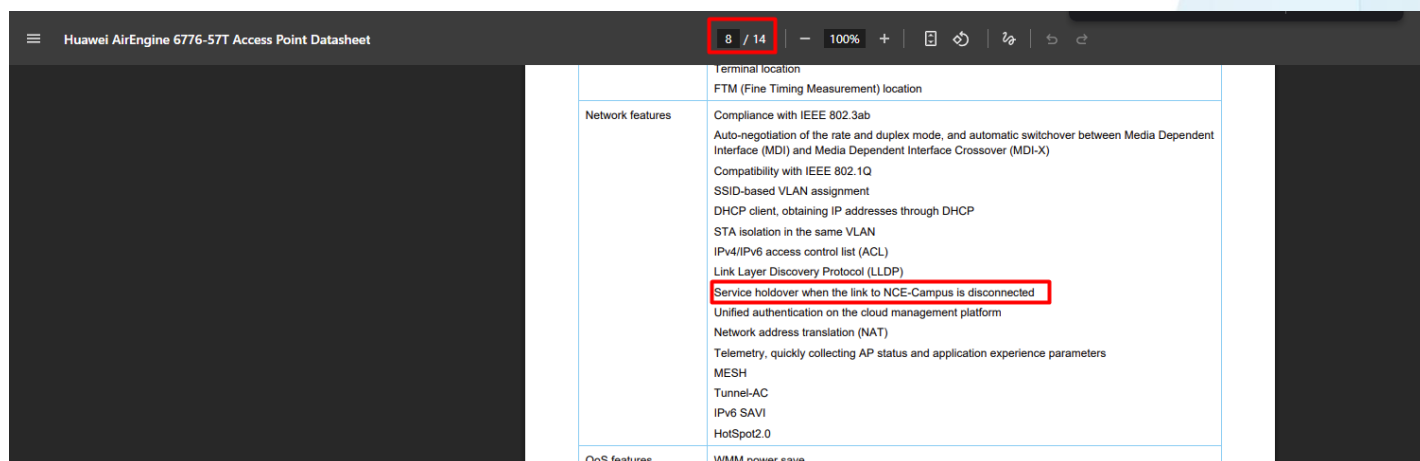
- **Clusterização de serviços:** múltiplas instâncias ativas do sistema operando em paralelo (active-active), eliminando pontos únicos de falha;
- **Balanceamento de carga dinâmico:** distribuição automática das requisições entre os nós disponíveis, garantindo desempenho e continuidade;
- **Failover automático:** comutação transparente em caso de falhas, mantendo a operação da rede gerenciada;
- **Sincronização contínua de banco de dados:** replicação em tempo real das informações de configuração, autenticação e telemetria.

Adicionalmente, os dispositivos de rede, como pontos de acesso e switches gerenciados, mantêm suas configurações operacionais localmente, permitindo que continuem funcionando normalmente mesmo em cenários de perda temporária de conectividade com a nuvem, reforçando a **resiliência da solução como um todo**.

Dessa forma, a arquitetura em nuvem da plataforma atende plenamente aos requisitos de **alta disponibilidade, continuidade operacional e tolerância a falhas**, sendo adequada para ambientes corporativos críticos que demandam elevada confiabilidade.

No datasheet, página 8, há a descrição do recurso Service holdover, conforme indicação abaixo:

<https://e.huawei.com/marketingcloud/pep/asset/20000001/Material/f74dc124f31c4a3eb0c8b4ea77cf1efe/M3T1A590N1186039378695843981/Huawei%20AirEngine%206776-57T%20Access%20Point%20Datasheet.pdf>



Huawei AirEngine 6776-57T Access Point Datasheet	
8 / 14 100%	
Network features	Terminal location
	FTM (Fine Timing Measurement) location
	Compliance with IEEE 802.3ab
	Auto-negotiation of the rate and duplex mode, and automatic switchover between Media Dependent Interface (MDI) and Media Dependent Interface Crossover (MDI-X)
	Compatibility with IEEE 802.1Q
	SSID-based VLAN assignment
	DHCP client, obtaining IP addresses through DHCP
	STA isolation in the same VLAN
	IPv4/IPv6 access control list (ACL)
	Link Layer Discovery Protocol (LLDP)
	Service holdover when the link to NCE-Campus is disconnected
	Unified authentication on the cloud management platform
	Network address translation (NAT)
	Telemetry, quickly collecting AP status and application experience parameters
QoS features	MESH
	Tunnel-AC
	IPv6 SAVI
	HotSpot2.0
QoS features	WMM power save

Vale ressaltar que a plataforma proposta está hospedada na Huawei Cloud, plataforma de computação em nuvem pública da Huawei, projetada para fornecer recursos de TI sob demanda por meio da internet, seguindo os princípios de **cloud computing** como elasticidade, escalabilidade e pagamento conforme o uso (*pay-as-you-go*).

Do ponto de vista técnico, o Huawei Cloud oferece um conjunto abrangente de serviços estruturados em camadas, incluindo:

1. Infraestrutura como Serviço (IaaS)

Disponibiliza recursos básicos de computação, como máquinas virtuais (ECS – Elastic Cloud Server), redes virtuais (VPC – Virtual Private Cloud) e armazenamento (OBS – Object Storage Service). Esses recursos são provisionados dinamicamente, permitindo rápida alocação e ajuste conforme a demanda da aplicação.

2. Plataforma como Serviço (PaaS)

Fornece ambientes gerenciados para desenvolvimento, teste e execução de aplicações, incluindo bancos de dados (RDS), containers (CCE – Cloud Container Engine) e serviços de middleware. Essa camada abstrai a complexidade da infraestrutura subjacente, permitindo maior foco no desenvolvimento de software.

3. Software como Serviço (SaaS)

Oferece aplicações prontas hospedadas na nuvem, acessíveis via navegador ou APIs, eliminando a necessidade de instalação local.

Arquitetura e características técnicas relevantes:

- **Alta disponibilidade e redundância:**
A plataforma é baseada em múltiplas zonas de disponibilidade (*Availability Zones – AZs*), com replicação de dados e balanceamento de carga, garantindo continuidade dos serviços mesmo em caso de falhas.
- **Escalabilidade elástica:**
Recursos computacionais podem ser automaticamente expandidos ou reduzidos conforme a carga, suportando variações dinâmicas de tráfego.
- **Segurança integrada:**
Inclui mecanismos como controle de identidade e acesso (IAM), criptografia de dados em repouso e em trânsito, além de conformidade com padrões internacionais de segurança.
- **Virtualização e isolamento:**
Utiliza tecnologias avançadas de virtualização para garantir isolamento entre tenants, permitindo ambientes multiusuário com segurança e desempenho.
- **Automação e orquestração:**
APIs e ferramentas de automação permitem provisionamento rápido de infraestrutura (Infraestrutura como Código – IaC), integração com pipelines DevOps e gerenciamento centralizado.
- **Integração com soluções corporativas Huawei:**
O Huawei Cloud integra-se a soluções como o Huawei CloudCampus, possibilitando gerenciamento centralizado de redes, dispositivos e políticas, especialmente em cenários de campus corporativo e redes definidas por software (SDN).

Atualmente Huawei Cloud Brasil está distribuído em 03 (três) locais distintos, conforme link e imagem abaixo:

https://support.huaweicloud.com/intl/pt-br/productdesc-dc/dc_01_0004.html#:~:text=A%20Direct%20Connect%20fornece%20uma%20s%C3%A9rie%20de,acesso%20%C3%A0%20Huawei%20Cloud%20em%20uma%20regi%C3%A3o.

			Johannesburg-Ieraco	Ieraco
América latina	México	LA-Mexico City1	Mexico City1-COM Ixtlahuaca	COM Ixtlahuaca
			Mexico-KIO MEX 5	KIO MEX 5
		LA-Mexico City2	Mexico-Tultitlan	Data center neutro para operadora
	Brasil (São Paulo)	LA-Sao Paulo1	Sao Paulo-Telefonica	Telefonica
			Sao Paulo-Equinix	Equinix
			Sao Paulo-ODATA	OData
	Santiago	LA-Santiago	Santiago-Paine	Paine
			Santiago-Claro	Claro

Diante do exposto, comprova-se o atendimento ao item 1.6.6. do Anexo I – Especificação Técnica.

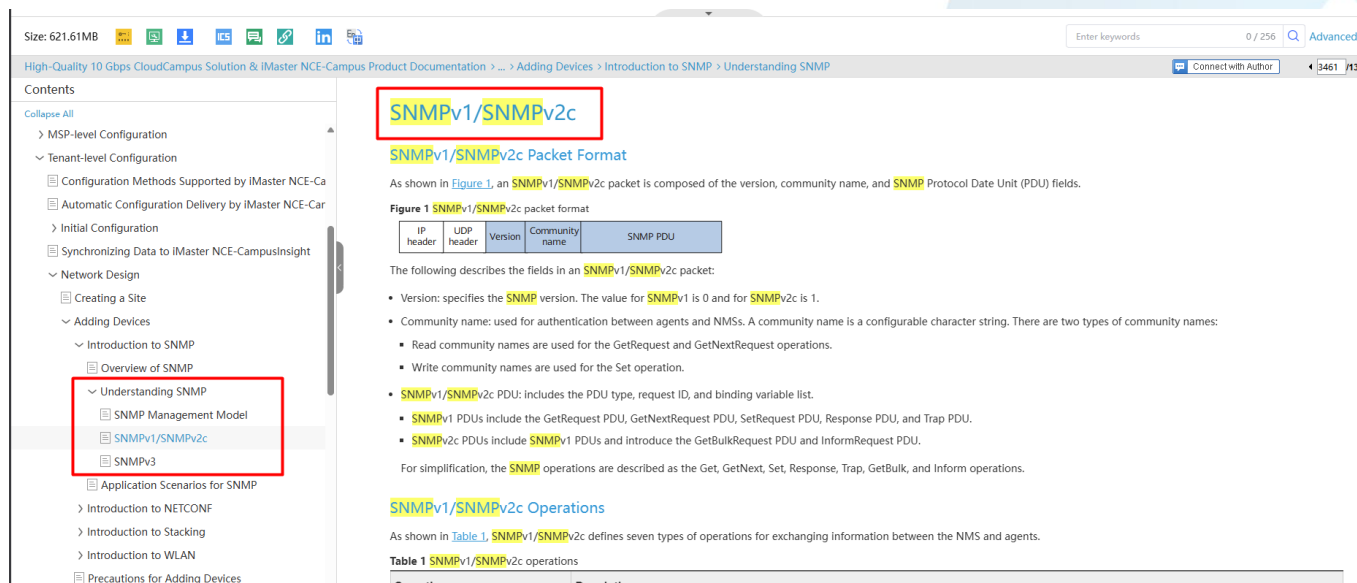
4.13) Do suposto não atendimento ao subitem 1.6.7.1. do Anexo I – Especificação Técnica

Aduz a Recorrente **TELESUL** que o documento utilizado para comprovação não fornece informação de suporte a SNMP, não fornece informação de como obter informações de CPU e demais itens solicitados no subitem abaixo.

- 1.6.7, Deve oferecer monitoramento via SNMP nas versões 2 ou 2c e 3 incluindo a geração de traps;
1.6.7.1, Deve ser possível a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e antenas;

No entanto, esclarecemos que, a Plataforma de Gerência NCE-CloudCampus inclui o monitoramento via SNMP nas versões V2C e V3, conforme links e imagens abaixo:

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100516678&id=EN-US_CONCEPT_0000001126200958



The screenshot displays the Huawei NCE-CloudCampus documentation interface. The left sidebar shows the navigation menu with 'SNMPv1/SNMPv2c' highlighted. The main content area is titled 'SNMPv1/SNMPv2c Packet Format' and includes a table describing the packet structure. The table has columns for IP header, UDP header, Version, Community name, and SNMP PDU. Below the table, there is a list of operations and their descriptions.

IP header	UDP header	Version	Community name	SNMP PDU
The following describes the fields in an SNMPv1/SNMPv2c packet:				
<ul style="list-style-type: none"> Version: specifies the SNMP version. The value for SNMPv1 is 0 and for SNMPv2c is 1. Community name: used for authentication between agents and NMSs. A community name is a configurable character string. There are two types of community names: <ul style="list-style-type: none"> Read community names are used for the GetRequest and GetNextRequest operations. Write community names are used for the Set operation. SNMPv1/SNMPv2c PDU: Includes the PDU type, request ID, and binding variable list. SNMPv1 PDUs include the GetRequest PDU, GetNextRequest PDU, SetRequest PDU, Response PDU, and Trap PDU. SNMPv2c PDUs include SNMPv1 PDUs and introduce the GetBulkRequest PDU and InformRequest PDU. 				

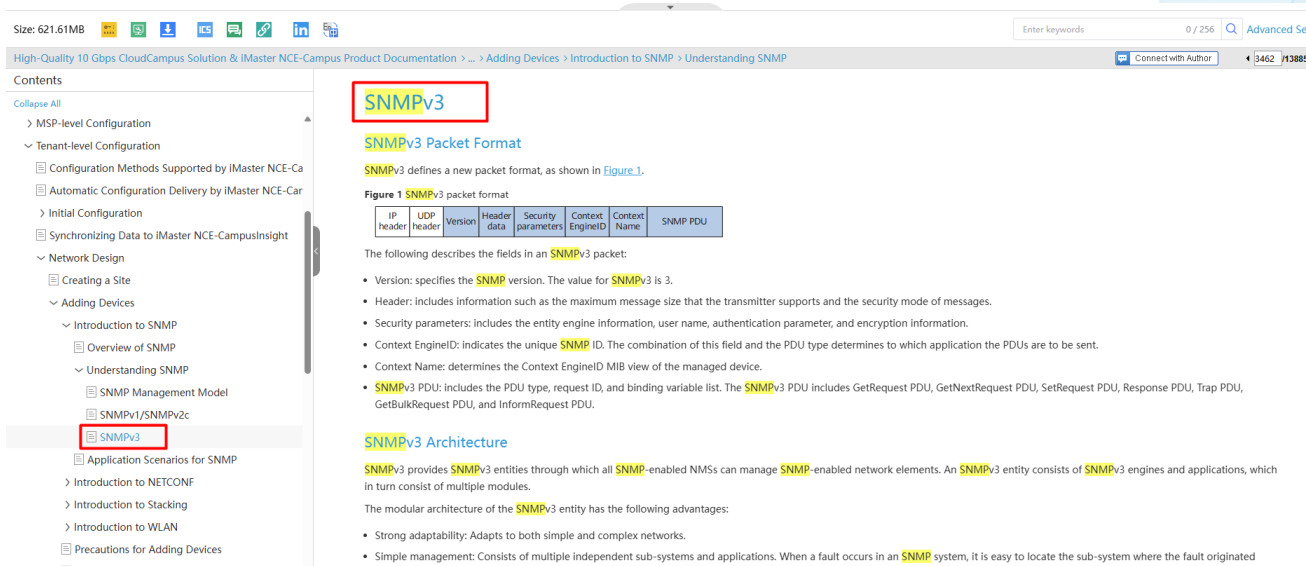
For simplification, the SNMP operations are described as the Get, GetNext, Set, Response, Trap, GetBulk, and Inform operations.

SNMPv1/SNMPv2c Operations

As shown in Table 1, SNMPv1/SNMPv2c defines seven types of operations for exchanging information between the NMS and agents.

Operation	Description
Get	Used to retrieve the value of one or more variables.
GetNext	Used to retrieve the value of the next variable in the sequence.
Set	Used to set the value of one or more variables.
Response	Used to return the result of a request.
Trap	Used to send a message to the NMS.
GetBulk	Used to retrieve a large number of variables.
Inform	Used to send a message to the NMS.

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100516678&id=EN-US_CONCEPT_0000001172280643



Size: 621.61MB

High-Quality 10 Gbps CloudCampus Solution & iMaster NCE-Campus Product Documentation > ... > Adding Devices > Introduction to SNMP > Understanding SNMP

Contents

- MSP-level Configuration
- Tenant-level Configuration
 - Configuration Methods Supported by iMaster NCE-Ca
 - Automatic Configuration Delivery by iMaster NCE-Car
 - Initial Configuration
 - Synchronizing Data to iMaster NCE-Campus Insight
 - Network Design
 - Creating a Site
 - Adding Devices
 - Introduction to SNMP
 - Overview of SNMP
 - Understanding SNMP
 - SNMP Management Model
 - SNMPv1/SNMPv2c
 - SNMPv3**
 - Application Scenarios for SNMP

Introduction to SNMP

Overview of SNMP

Understanding SNMP

SNMP Management Model

SNMPv1/SNMPv2c

SNMPv3

Application Scenarios for SNMP

Introduction to NETCONF

Introduction to Stacking

Introduction to WLAN

Precautions for Adding Devices

SNMPv3

SNMPv3 Packet Format

SNMPv3 defines a new packet format, as shown in Figure 1.

Figure 1 SNMPv3 packet format

IP header	UDP header	Version	Header data	Security parameters	Context EngineID	Context Name	SNMP PDU
-----------	------------	---------	-------------	---------------------	------------------	--------------	----------

The following describes the fields in an SNMPv3 packet:

- Version: specifies the **SNMP** version. The value for **SNMPv3** is 3.
- Header: includes information such as the maximum message size that the transmitter supports and the security mode of messages.
- Security parameters: includes the entity engine information, user name, authentication parameter, and encryption information.
- Context EngineID: indicates the unique **SNMP** ID. The combination of this field and the PDU type determines to which application the PDUs are to be sent.
- Context Name: determines the Context EngineID MIB view of the managed device.
- SNMPv3** PDU: includes the PDU type, request ID, and binding variable list. The **SNMPv3** PDU includes GetRequest PDU, GetNextRequest PDU, SetRequest PDU, Response PDU, Trap PDU, GetBulkRequest PDU, and InformRequest PDU.

SNMPv3 Architecture

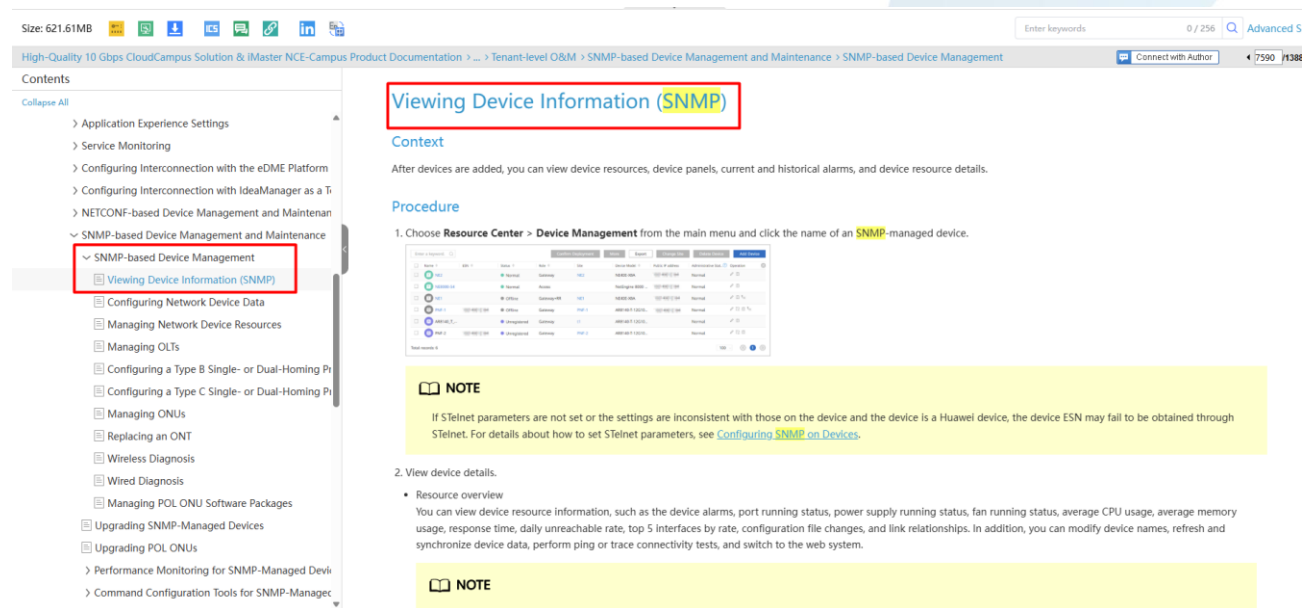
SNMPv3 provides **SNMPv3** entities through which all **SNMP**-enabled NMs can manage **SNMP**-enabled network elements. An **SNMPv3** entity consists of **SNMPv3** engines and applications, which in turn consist of multiple modules.

The modular architecture of the **SNMPv3** entity has the following advantages:

- Strong adaptability: Adapts to both simple and complex networks.
- Simple management: Consists of multiple independent sub-systems and applications. When a fault occurs in an **SNMP** system, it is easy to locate the sub-system where the fault originated.

Comprova-se ainda, por meio de link e imagens abaixo, o atendimento quanto à informações de CPU, memória e antenas:

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100516678&id=EN-US_TOPIC_0317327746



Size: 621.61MB

High-Quality 10 Gbps CloudCampus Solution & iMaster NCE-Campus Product Documentation > ... > Tenant-level O&M > SNMP-based Device Management and Maintenance > SNMP-based Device Management

Contents

- Application Experience Settings
- Service Monitoring
- Configuring Interconnection with the eDME Platform
- Configuring Interconnection with IdeaManager as a Tr
- NETCONF-based Device Management and Maintenan
- SNMP-based Device Management and Maintenance
 - SNMP-based Device Management
 - Viewing Device Information (SNMP)**
 - Configuring Network Device Data
 - Managing Network Device Resources
 - Managing OLTs
 - Configuring a Type B Single- or Dual-Homing Pi
 - Configuring a Type C Single- or Dual-Homing Pi
 - Managing ONUs
 - Replacing an ONT
 - Wireless Diagnosis
 - Wired Diagnosis
 - Managing POL ONU Software Packages
 - Upgrading SNMP-Managed Devices
 - Upgrading POL ONUs
 - Performance Monitoring for SNMP-Managed Devi
 - Command Configuration Tools for SNMP-Managec

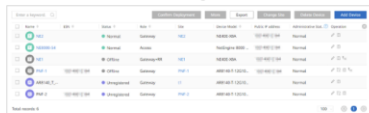
Viewing Device Information (SNMP)

Context

After devices are added, you can view device resources, device panels, current and historical alarms, and device resource details.

Procedure

- Choose **Resource Center > Device Management** from the main menu and click the name of an **SNMP**-managed device.



NOTE

If Stelnet parameters are not set or the settings are inconsistent with those on the device and the device is a Huawei device, the device ESN may fail to be obtained through Stelnet. For details about how to set Stelnet parameters, see [Configuring SNMP on Devices](#).

- View device details.
 - Resource overview

You can view device resource information, such as the device alarms, port running status, power supply running status, fan running status, average CPU usage, average memory usage, response time, daily unreachable rate, top 5 interfaces by rate, configuration file changes, and link relationships. In addition, you can modify device names, refresh and synchronize device data, perform ping or trace connectivity tests, and switch to the web system.

NOTE

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100516678&id=EN-US_TOPIC_000002287379350

Size: 621.61MB

High-Quality 10 Gbps CloudCampus Solution & iMaster NCE-Campus Product Documentation > ... > Tenant-level O&M > SNMP-based Device Management and Maintenance > SNMP-based Device Management

Contents

- > Configuring Interconnection with IdeaManager as a T...
- > NETCONF-based Device Management and Maintenan...
- > SNMP-based Device Management and Maintenance
 - > SNMP-based Device Management
 - Viewing Device Information (SNMP)
 - Configuring Network Device Data
 - Managing Network Device Resources
 - Managing OLTs
 - Configuring a Type B Single- or Dual-Homing P...
 - Configuring a Type C Single- or Dual-Homing P...
 - Managing ONUs
 - Replacing an ONT
 - Wireless Diagnosis**
 - Wired Diagnosis
 - Managing POL ONU Software Packages
 - Upgrading SNMP-Managed Devices
 - Upgrading POL ONUs
 - > Performance Monitoring for SNMP-Managed Devi...

Wireless Diagnosis

This function can be used to quickly locate network exceptions for a wireless STA and improve user satisfaction.

Prerequisites

- iMaster NCE-Campus is operating normally.
- ONUs have been added to iMaster NCE-Campus.

Restrictions and Limitations

- The OLT and ONU versions must be R025C00 or later.
- ONUs work in fit AP mode.
- W series ONUs are used.

Procedure

- Choose **Network Monitoring** > **LAN Monitoring** > **Device 360** from the main menu.
- In the navigation pane, choose **ONU**.
- Click an ONU name.
- Click **...** and choose **Wireless Diagnosis** to view the Wi-Fi signal interference, Wi-Fi signal coverage, device detection result, load detection result, and rectification suggestions.

The wireless network diagnosis function detects network issues from four dimensions: Wi-Fi interference, Wi-Fi coverage, device, and load. For details, see [Table 1](#).

Size: 621.61MB

High-Quality 10 Gbps CloudCampus Solution & iMaster NCE-Campus Product Documentation > ... > Tenant-level O&M > SNMP-based Device Management and Maintenance > SNMP-based Device Management

Contents

- > Configuring Interconnection with IdeaManager as a T...
- > NETCONF-based Device Management and Maintenan...
- > SNMP-based Device Management and Maintenance
 - > SNMP-based Device Management
 - Viewing Device Information (SNMP)
 - Configuring Network Device Data
 - Managing Network Device Resources
 - Managing OLTs
 - Configuring a Type B Single- or Dual-Homing P...
 - Configuring a Type C Single- or Dual-Homing P...
 - Managing ONUs
 - Replacing an ONT
 - Wireless Diagnosis**
 - Wired Diagnosis
 - Managing POL ONU Software Packages
 - Upgrading SNMP-Managed Devices
 - Upgrading POL ONUs
 - > Performance Monitoring for SNMP-Managed Devi...
 - > Command Configuration Tools for SNMP-Managec...
 - > Customizing Device Management
 - > SLA Management
 - > Certificate Management

Interference	Interference traffic	The interference traffic is heavy.	Manually trigger channel reselection.	Yes
Noise	Noise	The noise is high.	Channel reselection may cause the Wi-Fi function to be temporarily unavailable. Exercise caution when performing this operation.	Yes
Wi-Fi SSID conflict	Wi-Fi SSID conflict	Wi-Fi SSID conflict, which may cause Wi-Fi failure.	Change the Wi-Fi name.	Yes
Wi-Fi Coverage	Wi-Fi strength of connected wireless devices	The signal strength of the connected wireless devices is weak.	Relocate the connected wireless device, gateway, or AP	No
Device Detection	CPU usage	The CPU usage of the device is xx (higher than or equal to the threshold).	-	No
	Memory usage	The memory usage of the device is xx (higher than or equal to the threshold).	-	No
	Memory temperature	The memory temperature of the device is xx°C (higher than or equal to the threshold).	-	No
	AP status	The AP is offline.	Check whether the power supply of the AP is normal or whether fit AP configurations are correct.	No
Load Detection	Idle duty cycle	The idle duty cycle of the 2.4 GHz or 5 GHz band is xx (lower than or equal to the threshold).	-	No

Com isso, comprova-se o atendimento ao item 1.6.7.1. do Anexo I – Especificação Técnica.

4.14) Do suposto não atendimento ao subitem 3.1.9. do Anexo I – Especificação Técnica

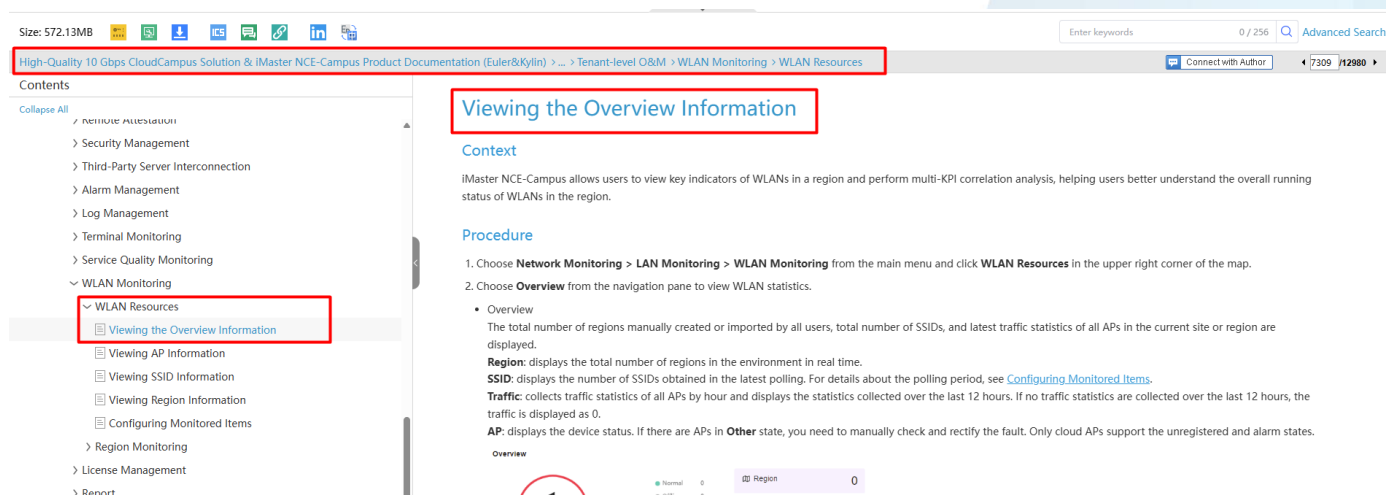
Aduz a Recorrente **TELESUL** que a Recorrida **3CORP**, não comprovou o requisito deste item, apresentando uma descrição equivocada da exigência abaixo.

3.1.9. Não será aceita solução em padrão controller-less. Rejeita-se, portanto, qualquer arquitetura na qual as funcionalidades de controladora da rede sem fio sejam desempenhadas pelos próprios Pontos de Acesso, incluindo tanto modelos onde essa responsabilidade é entre múltiplos Pontos de Acesso, quanto configurações onde um

ou mais Pontos de Acesso são designados ou eleitos para exercer o papel de controladora para outros dispositivos de acesso.

No entanto, esclarecemos que, foi comprovado o atendimento ao item 3.1.9. da Especificação descrevendo que o iMaster NCE-CloudCampus monitora o ambiente Wlan:

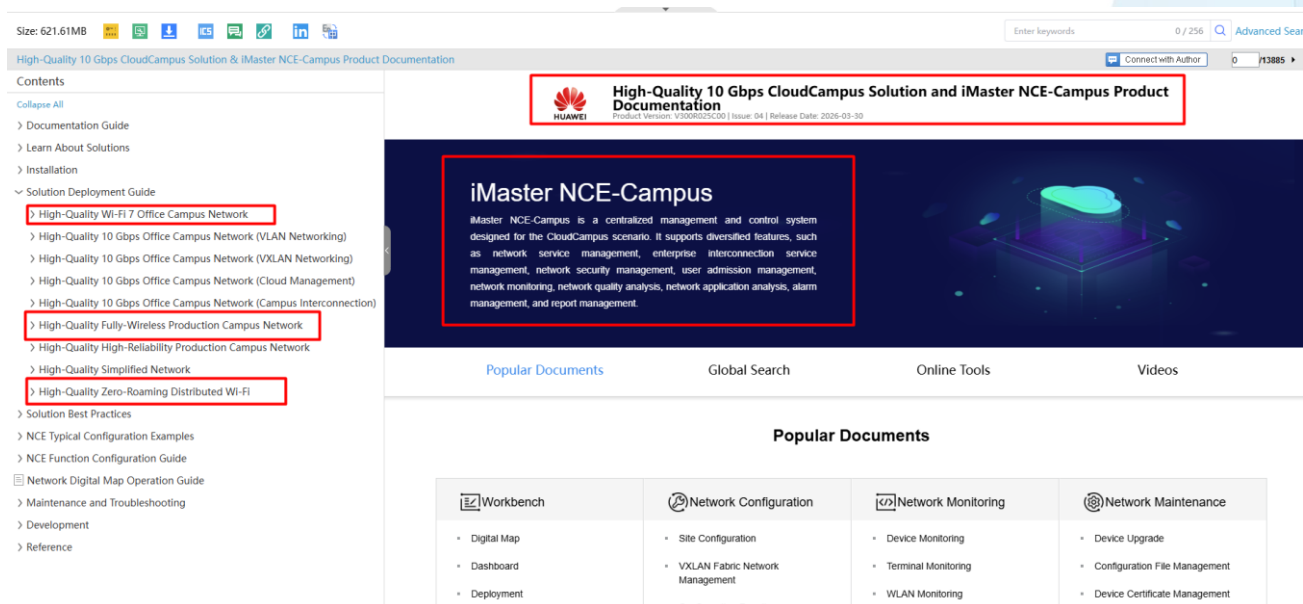
https://support.huawei.com/hedex/hdx.do?docid=EDOC1100413634&id=EN-US_TOPIC_0226027482



Adicionalmente, informamos que a Plataforma de Gerência ofertada baseia-se na modalidade Nuvem e a demonstração de seu acesso para gerência do ambiente Wlan comprova de que não se trata de oferta Controller-less.

Abaixo link e imagem demonstrando de que se trata de uma plataforma de Gerência Centralizada para ambiente de rede, seja ele cabeado ou sem fio.

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100516678&tocURL=resources%2Findex_campus_v25c00_en.html



Size: 621.61MB

High-Quality 10 Gbps CloudCampus Solution & iMaster NCE-Campus Product Documentation

Contents

- > Documentation Guide
- > Learn About Solutions
- > Installation
- > Solution Deployment Guide
 - > High-Quality Wi-Fi 7 Office Campus Network
 - > High-Quality 10 Gbps Office Campus Network (VLAN Networking)
 - > High-Quality 10 Gbps Office Campus Network (VXLAN Networking)
 - > High-Quality 10 Gbps Office Campus Network (Cloud Management)
 - > High-Quality 10 Gbps Office Campus Network (Campus Interconnection)
 - > High-Quality Fully-Wireless Production Campus Network
 - > High-Quality High-Reliability Production Campus Network
 - > High-Quality Simplified Network
 - > High-Quality Zero-Roaming Distributed Wi-Fi
- > Solution Best Practices
- > NCE Typical Configuration Examples
- > NCE Function Configuration Guide
- > Network Digital Map Operation Guide
- > Maintenance and Troubleshooting
- > Development
- > Reference

High-Quality 10 Gbps CloudCampus Solution and iMaster NCE-Campus Product Documentation

iMaster NCE-Campus

iMaster NCE-Campus is a centralized management and control system designed for the CloudCampus scenario. It supports diversified features, such as network service management, enterprise interconnection service management, network security management, user admission management, network monitoring, network quality analysis, network application analysis, alarm management, and report management.

Popular Documents

Global Search

Online Tools

Videos

Popular Documents

Workbench	Network Configuration	Network Monitoring	Network Maintenance
<ul style="list-style-type: none"> Digital Map Dashboard Deployment 	<ul style="list-style-type: none"> Site Configuration VXLAN Fabric Network Management Configuration Decimals 	<ul style="list-style-type: none"> Device Monitoring Terminal Monitoring WLAN Monitoring 	<ul style="list-style-type: none"> Device Upgrade Configuration File Management Device Certificate Management

Conclui-se, assim, que o item 3.1.9. do Anexo I – Especificação Técnica foi atendido conforme sua descrição.

4.15) Do suposto não atendimento ao subitem 3.1.14. do Anexo I – Especificação Técnica

Aduz a Recorrente **TELESUL** que o link apresentado não foi comprovado que a solução permite o uso de APs em sites remotos, limitando a escalabilidade e abrangência da rede, consoante a exigência abaixo.

3.1.14. Deve possuir funcionalidade que permita a utilização dos APs em sites remotos;

No entanto, esclarecemos que, a utilização da plataforma Huawei iMaster NCE-CloudCampus para gerenciamento de pontos de acesso (APs) implica, por definição arquitetural, a operação desses dispositivos em cenários distribuídos, tipicamente caracterizados como sites remotos.

O Huawei iMaster NCE-CloudCampus é uma solução de gerenciamento baseada em nuvem, na qual o plano de controle e gerenciamento é centralizado em uma infraestrutura cloud, enquanto os dispositivos de rede — como access points — permanecem fisicamente distribuídos em diferentes localidades. Essa separação entre plano de gerenciamento e plano de dados elimina a necessidade de controladoras WLAN locais, permitindo que os APs sejam implantados em redes geograficamente dispersas e conectados à nuvem por meio de redes IP (tipicamente via WAN/Internet).

Nesse contexto, ao adotar o modelo de gerenciamento cloud, os access points estabelecem túneis seguros (como CAPWAP sobre DTLS) diretamente com a plataforma na nuvem, independentemente de sua localização física. Essa característica operacional é inerente ao conceito de “cloud-managed network”, no qual os dispositivos são projetados para funcionar fora de um site centralizado, sendo instalados em filiais, unidades remotas, escritórios distribuídos ou ambientes externos ao datacenter principal.

Portanto, a simples utilização do Huawei iMaster NCE-CloudCampus já pressupõe que os access points estejam aptos a operar em sites remotos, uma vez que:

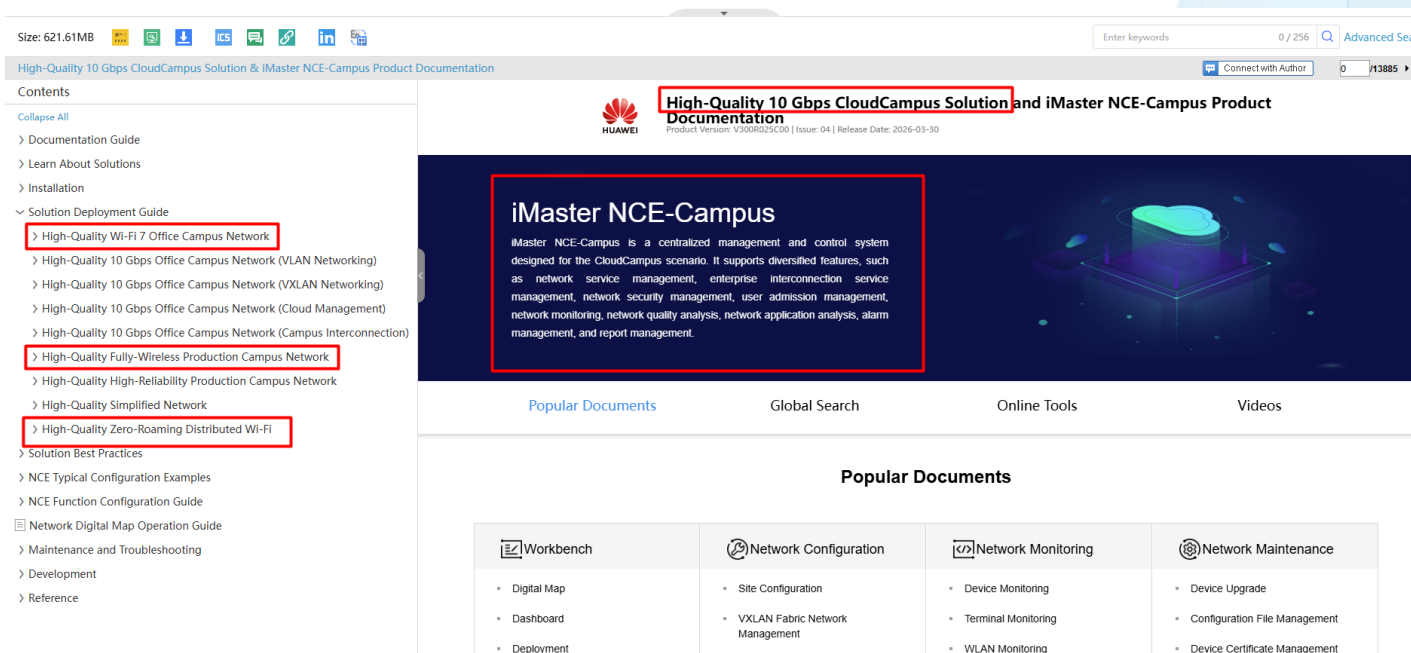
- Não há dependência de controladora local;
- O gerenciamento é realizado de forma centralizada via nuvem;
- A comunicação ocorre sobre infraestrutura IP, sem restrição de topologia Layer 2;
- Os dispositivos podem ser provisionados e operados remotamente (zero-touch provisioning).

Dessa forma, conclui-se tecnicamente que a adoção da gerência via nuvem, por meio do Huawei iMaster NCE-CloudCampus, caracteriza intrinsecamente a utilização dos access

points em ambientes remotos e distribuídos, sendo este um comportamento nativo da solução.

Abaixo link e imagem para comprovação:

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100516678&tocURL=resources%2Findex_campus_v25c00_en.html



Workbench	Network Configuration	Network Monitoring	Network Maintenance
<ul style="list-style-type: none">Digital MapDashboardDeployment	<ul style="list-style-type: none">Site ConfigurationVXLAN Fabric Network Management	<ul style="list-style-type: none">Device MonitoringTerminal MonitoringWLAN Monitoring	<ul style="list-style-type: none">Device UpgradeConfiguration File ManagementDevice Certificate Management

Desta forma, fica comprovado o atendimento ao item 3.1.14. do Anexo I – Especificação Técnica.

4.16) Do suposto não atendimento ao subitem 3.2.2.1. do Anexo I – Especificação Técnica

Aduz a Recorrente **TELESUL** que o documento apresentado, não comprovou a persistência de sessão, impactando a experiência do usuário em ambientes com mobilidade, portanto, não atendendo o subitem abaixo.

3.2.2.1. Neste tipo de topologia, para redução no tempo de indisponibilidade dos serviços, deve ser implementada persistência de sessão entre Pontos de Acesso e as controladoras ativa e redundante, resultando na comutação entre controladoras sem interrupção do serviço;

No entanto, esclarecemos que, a plataforma Huawei NCE-CloudCampus, quando utilizada na modalidade em nuvem, é projetada com arquitetura distribuída e resiliente, garantindo mecanismos robustos de **redundância e alta disponibilidade (HA – High Availability)**.

Nesse modelo, os serviços de gerenciamento são hospedados em infraestrutura de data centers geograficamente distribuídos, com **replicação de dados em múltiplas zonas de disponibilidade (AZs)**. Isso assegura que, em caso de falha de um nó, instância ou até mesmo de um data center completo, as demais instâncias assumam automaticamente a operação, sem interrupção perceptível dos serviços.

A solução utiliza conceitos como:

- **Clusterização de serviços:** múltiplas instâncias ativas do sistema operando em paralelo (active-active), eliminando pontos únicos de falha;
- **Balanceamento de carga dinâmico:** distribuição automática das requisições entre os nós disponíveis, garantindo desempenho e continuidade;
- **Failover automático:** comutação transparente em caso de falhas, mantendo a operação da rede gerenciada;
- **Sincronização contínua de banco de dados:** replicação em tempo real das informações de configuração, autenticação e telemetria.

Adicionalmente, os dispositivos de rede, como pontos de acesso e switches gerenciados, mantêm suas configurações operacionais localmente, permitindo que continuem funcionando normalmente mesmo em cenários de perda temporária de conectividade com a nuvem, reforçando a **resiliência da solução como um todo**.

Dessa forma, a arquitetura em nuvem da plataforma atende plenamente aos requisitos de **alta disponibilidade, continuidade operacional e tolerância a falhas**, sendo adequada para ambientes corporativos críticos que demandam elevada confiabilidade.

No datasheet, página 8, há a descrição do recurso Service holdover, conforme indicação abaixo:

<https://e.huawei.com/marketingcloud/pep/asset/20000001/Material/f74dc124f31c4a3eb0c8b4ea77cf1efe/M3T1A590N1186039378695843981/Huawei%20AirEngine%206776-57T%20Access%20Point%20Datasheet.pdf>

Huawei AirEngine 6776-57T Access Point Datasheet

8 / 14

100%

+

-

	Terminal location
	FTM (Fine Timing Measurement) location
Network features	Compliance with IEEE 802.3ab
	Auto-negotiation of the rate and duplex mode, and automatic switchover between Media Dependent Interface (MDI) and Media Dependent Interface Crossover (MDI-X)
	Compatibility with IEEE 802.1Q
	SSID-based VLAN assignment
	DHCP client, obtaining IP addresses through DHCP
	STA isolation in the same VLAN
	IPv4/IPv6 access control list (ACL)
	Link Layer Discovery Protocol (LLDP)
	Service holdover when the link to NCE-Campus is disconnected
	Unified authentication on the cloud management platform
	Network address translation (NAT)
	Telemetry, quickly collecting AP status and application experience parameters
	MESH
Tunnel-AC	
IPv6 SAVI	
HotSpot2.0	
QoS features	WMM power save

Vale ressaltar que a plataforma proposta está hospedada na Huawei Cloud, plataforma de computação em nuvem pública da Huawei, projetada para fornecer recursos de TI sob demanda por meio da internet, seguindo os princípios de **cloud computing** como elasticidade, escalabilidade e pagamento conforme o uso (*pay-as-you-go*).

Do ponto de vista técnico, o Huawei Cloud oferece um conjunto abrangente de serviços estruturados em camadas, incluindo:

1. Infraestrutura como Serviço (IaaS)

Disponibiliza recursos básicos de computação, como máquinas virtuais (ECS – Elastic Cloud Server), redes virtuais (VPC – Virtual Private Cloud) e armazenamento (OBS – Object Storage Service). Esses recursos são provisionados dinamicamente, permitindo rápida alocação e ajuste conforme a demanda da aplicação.

2. Plataforma como Serviço (PaaS)

Fornece ambientes gerenciados para desenvolvimento, teste e execução de aplicações, incluindo bancos de dados (RDS), containers (CCE – Cloud Container Engine) e serviços de middleware. Essa camada abstrai a complexidade da infraestrutura subjacente, permitindo maior foco no desenvolvimento de software.

3. Software como Serviço (SaaS)

Oferece aplicações prontas hospedadas na nuvem, acessíveis via navegador ou APIs, eliminando a necessidade de instalação local.

Arquitetura e características técnicas relevantes:

- **Alta disponibilidade e redundância:**
A plataforma é baseada em múltiplas zonas de disponibilidade (*Availability Zones – AZs*), com replicação de dados e balanceamento de carga, garantindo continuidade dos serviços mesmo em caso de falhas.
- **Escalabilidade elástica:**
Recursos computacionais podem ser automaticamente expandidos ou reduzidos conforme a carga, suportando variações dinâmicas de tráfego.
- **Segurança integrada:**
Inclui mecanismos como controle de identidade e acesso (IAM), criptografia de dados em repouso e em trânsito, além de conformidade com padrões internacionais de segurança.
- **Virtualização e isolamento:**
Utiliza tecnologias avançadas de virtualização para garantir isolamento entre tenants, permitindo ambientes multiusuário com segurança e desempenho.
- **Automação e orquestração:**
APIs e ferramentas de automação permitem provisionamento rápido de infraestrutura (Infraestrutura como Código – IaC), integração com pipelines DevOps e gerenciamento centralizado.
- **Integração com soluções corporativas Huawei:**
O Huawei Cloud integra-se a soluções como o Huawei CloudCampus, possibilitando gerenciamento centralizado de redes, dispositivos e políticas, especialmente em cenários de campus corporativo e redes definidas por software (SDN).

Atualmente Huawei Cloud Brasil está distribuído em 03 (três) locais distintos, conforme link e imagem abaixo:

https://support.huaweicloud.com/intl/pt-br/productdesc-dc/dc_01_0004.html#:~:text=A%20Direct%20Connect%20fornece%20uma%20s%C3%A9rie%20de,acesso%20%C3%A0%20Huawei%20Cloud%20em%20uma%20regi%C3%A3o.

			Johannesburg-Ieraco	Ieraco
América latina	México	LA-Mexico City1	Mexico City1-COM Ixtlahuaca	COM Ixtlahuaca
			Mexico-KIO MEX 5	KIO MEX 5
		LA-Mexico City2	Mexico-Tultitlan	Data center neutro para operadora
	Brasil (São Paulo)	LA-Sao Paulo1	Sao Paulo-Telefonica	Telefonica
			Sao Paulo-Equinix	Equinix
			Sao Paulo-ODATA	OData
	Santiago	LA-Santiago	Santiago-Paine	Paine
Santiago-Claro			Claro	

Diante do exposto, comprova-se o atendimento ao item 3.2.2.1. do Anexo I – Especificação Técnica.

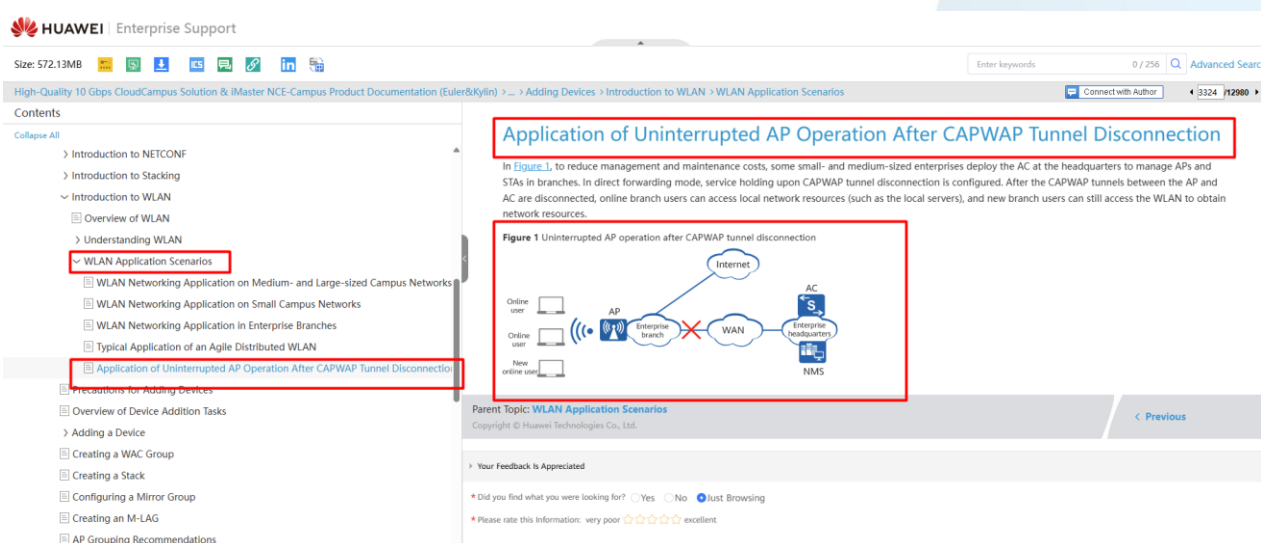
4.17) Do suposto não atendimento ao subitem 3.2.4. do Anexo I – Especificação Técnica

Aduz a Recorrente **TELESUL** que o link apresentado como comprovação, não comprovada a sincronização entre as controllers, e não comprova que as sessões dos usuários serão sincronizadas entre as controladoras em alta disponibilidade, não atendendo o subitem abaixo.

3.2.4. Quando operando em uma topologia do tipo (1+1), para que não exista interrupção no serviço prestado aos clientes, as sessões dos usuários devem ser também sincronizadas entre as controladoras em alta disponibilidade;

No entanto, esclarecemos que, a evidência enviada anteriormente de atendimento quanto à não existência de interrupção no serviço prestado aos clientes demonstra o atendimento ao item, com um dos cenários propostos:

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100413634&id=EN-US_CONCEPT_0000001172291507



The screenshot displays the Huawei Enterprise Support portal. The left sidebar shows a navigation tree with 'WLAN Application Scenarios' and 'Application of Uninterrupted AP Operation After CAPWAP Tunnel Disconnection' highlighted. The main content area features the document title 'Application of Uninterrupted AP Operation After CAPWAP Tunnel Disconnection' and a diagram labeled 'Figure 1 Uninterrupted AP operation after CAPWAP tunnel disconnection'. The diagram illustrates a network topology where an AP (Access Point) is connected to an AC (Access Controller) via a WAN (Wide Area Network). The AC is connected to the Internet and an NMS (Network Management System). The diagram shows that even after a CAPWAP tunnel disconnection, the AP can still provide service to online users.

Reforçamos que a plataforma Huawei NCE-CloudCampus, quando utilizada na modalidade em nuvem, é projetada com arquitetura distribuída e resiliente, garantindo mecanismos robustos de **redundância e alta disponibilidade (HA – High Availability)**.

Nesse modelo, os serviços de gerenciamento são hospedados em infraestrutura de data centers geograficamente distribuídos, com **replicação de dados em múltiplas zonas de disponibilidade (AZs)**. Isso assegura que, em caso de falha de um nó, instância ou até mesmo de um data center completo, as demais instâncias assumam automaticamente a operação, sem interrupção perceptível dos serviços.

A solução utiliza conceitos como:

- **Clusterização de serviços:** múltiplas instâncias ativas do sistema operando em paralelo (active-active), eliminando pontos únicos de falha;
- **Balanceamento de carga dinâmico:** distribuição automática das requisições entre os nós disponíveis, garantindo desempenho e continuidade;
- **Failover automático:** comutação transparente em caso de falhas, mantendo a operação da rede gerenciada;
- **Sincronização contínua de banco de dados:** replicação em tempo real das informações de configuração, autenticação e telemetria.

Adicionalmente, os dispositivos de rede, como pontos de acesso e switches gerenciados, mantêm suas configurações operacionais localmente, permitindo que continuem funcionando normalmente mesmo em cenários de perda temporária de conectividade com a nuvem, reforçando a **resiliência da solução como um todo**.

Dessa forma, a arquitetura em nuvem da plataforma atende plenamente aos requisitos de **alta disponibilidade, continuidade operacional e tolerância a falhas**, sendo adequada para ambientes corporativos críticos que demandam elevada confiabilidade.

No datasheet, página 8, há a descrição do recurso Service holdover, conforme indicação abaixo:

<https://e.huawei.com/marketingcloud/pep/asset/20000001/Material/f74dc124f31c4a3eb0c8b4ea77cf1efe/M3T1A590N1186039378695843981/Huawei%20AirEngine%206776-57T%20Access%20Point%20Datasheet.pdf>

Huawei AirEngine 6776-57T Access Point Datasheet		8 / 14	100%						
Network features	Terminal location								
	FTM (Fine Timing Measurement) location								
Network features	Compliance with IEEE 802.3ab								
	Auto-negotiation of the rate and duplex mode, and automatic switchover between Media Dependent Interface (MDI) and Media Dependent Interface Crossover (MDI-X)								
	Compatibility with IEEE 802.1Q								
	SSID-based VLAN assignment								
	DHCP client, obtaining IP addresses through DHCP								
	STA isolation in the same VLAN								
	IPv4/IPv6 access control list (ACL)								
	Link Layer Discovery Protocol (LLDP)								
	Service holdover when the link to NCE-Campus is disconnected								
	Unified authentication on the cloud management platform								
	Network address translation (NAT)								
	Telemetry, quickly collecting AP status and application experience parameters								
	MESH								
	Tunnel-AC								
	IPv6 SAVI								
	HotSpot2.0								
QoS features	WMM power save								

Vale ressaltar que a plataforma proposta está hospedada na Huawei Cloud, plataforma de computação em nuvem pública da Huawei, projetada para fornecer recursos de TI sob demanda por meio da internet, seguindo os princípios de **cloud computing** como elasticidade, escalabilidade e pagamento conforme o uso (*pay-as-you-go*).

Do ponto de vista técnico, o Huawei Cloud oferece um conjunto abrangente de serviços estruturados em camadas, incluindo:

1. Infraestrutura como Serviço (IaaS)

Disponibiliza recursos básicos de computação, como máquinas virtuais (ECS – Elastic Cloud Server), redes virtuais (VPC – Virtual Private Cloud) e armazenamento (OBS – Object Storage Service). Esses recursos são provisionados dinamicamente, permitindo rápida alocação e ajuste conforme a demanda da aplicação.

2. Plataforma como Serviço (PaaS)

Fornece ambientes gerenciados para desenvolvimento, teste e execução de aplicações, incluindo bancos de dados (RDS), containers (CCE – Cloud Container Engine) e serviços de middleware. Essa camada abstrai a complexidade da infraestrutura subjacente, permitindo maior foco no desenvolvimento de software.

3. Software como Serviço (SaaS)

Oferece aplicações prontas hospedadas na nuvem, acessíveis via navegador ou APIs, eliminando a necessidade de instalação local.

Arquitetura e características técnicas relevantes:

- **Alta disponibilidade e redundância:**
A plataforma é baseada em múltiplas zonas de disponibilidade (*Availability Zones – AZs*), com replicação de dados e balanceamento de carga, garantindo continuidade dos serviços mesmo em caso de falhas.

- **Escalabilidade elástica:**
Recursos computacionais podem ser automaticamente expandidos ou reduzidos conforme a carga, suportando variações dinâmicas de tráfego.
- **Segurança integrada:**
Inclui mecanismos como controle de identidade e acesso (IAM), criptografia de dados em repouso e em trânsito, além de conformidade com padrões internacionais de segurança.
- **Virtualização e isolamento:**
Utiliza tecnologias avançadas de virtualização para garantir isolamento entre tenants, permitindo ambientes multiusuário com segurança e desempenho.
- **Automação e orquestração:**
APIs e ferramentas de automação permitem provisionamento rápido de infraestrutura (Infraestrutura como Código – IaC), integração com pipelines DevOps e gerenciamento centralizado.
- **Integração com soluções corporativas Huawei:**
O Huawei Cloud integra-se a soluções como o Huawei CloudCampus, possibilitando gerenciamento centralizado de redes, dispositivos e políticas, especialmente em cenários de campus corporativo e redes definidas por software (SDN).

Atualmente Huawei Cloud Brasil está distribuído em 03 (três) locais distintos, conforme link e imagem abaixo:

https://support.huaweicloud.com/intl/pt-br/productdesc-dc/dc_01_0004.html#:~:text=A%20Direct%20Connect%20fornece%20uma%20s%C3%A9rie%20de,acesso%20%C3%A0%20Huawei%20Cloud%20em%20uma%20regi%C3%A3o.

América latina	México	LA-Mexico City1	Johannesburg-Ieraco	Ieraco
			Mexico City1-COM Ixtlahuaca	COM Ixtlahuaca
		LA-Mexico City2	Mexico-KIO MEX 5	KIO MEX 5
			Mexico-Tultitlan	Data center neutro para operadora
	Brasil (São Paulo)	LA-Sao Paulo1	Sao Paulo-Telefonica	Telefonica
			Sao Paulo-Equinix	Equinix
			Sao Paulo-ODATA	OData
	Santiago	LA-Santiago	Santiago-Paine	Paine
			Santiago-Claro	Claro

Diante do exposto, comprova-se o atendimento ao item 3.2.4. do Anexo I – Especificação Técnica.

4.18) Do suposto não atendimento ao subitem 3.3.4. do Anexo I – Especificação Técnica

Aduz a Recorrente **TELESUL** que no documento, a licitante **3CORP** não comprovou visibilidade na camada 7 nem a capacidade de fazer bloqueios por aplicação, funcionalidades importantes para controle de tráfego e segurança, não atendendo o subitem abaixo.

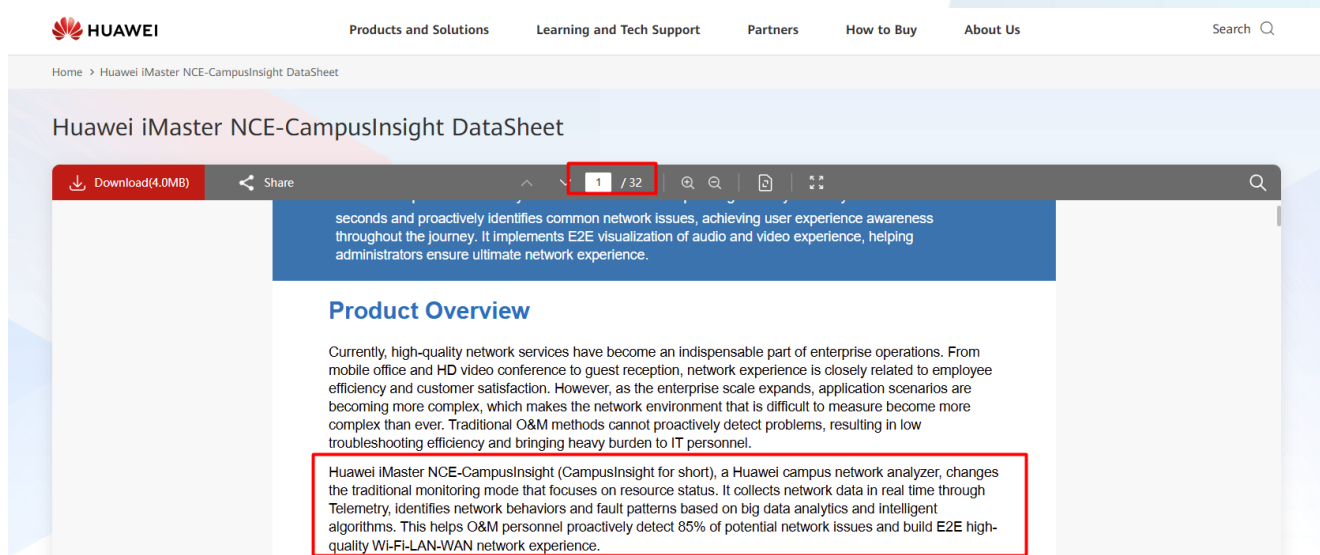
- 3.3.4. Deve permitir visibilidade e controle das aplicações em camada 7, permitindo a priorização de aplicações críticas, redução na prioridade de aplicações menos críticas e o bloqueio de aplicações não permitidas já na camada de acesso.

No entanto, esclarecemos que, a evidência enviada comprova a função de visibilidade e controle pelo módulo NCE-CampusInsight incluso na oferta da 3Corp Technology.

Tal recurso fornece todas as informações referentes às aplicações em camada 7.

Na página 01 do datasheet, temos a evidência quanto à sua função:

<https://e.huawei.com/en/documents/products/enterprise-network/2f55644fbe3f4628a061ed26cf8bf541>



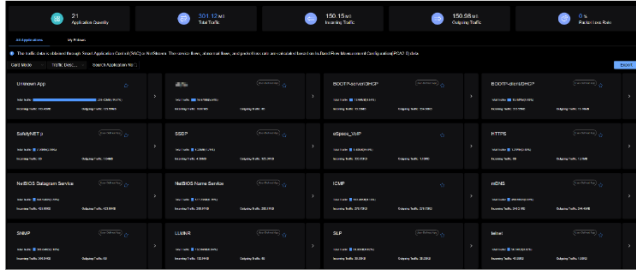
No mesmo documento, página 18, há a descrição das funções referentes a aplicações e demais itens a serem visualizados/analísados:

Huawei iMaster NCE-CampusInsight DataSheet

Download(4.0MB) Share 18 / 32

Real-Time Application Identification, Traffic Analysis, Quality Awareness, and Fault Locating, Ensuring E2E Application Experience from Wi-Fi, LAN, to WAN

The application identification technology is used to accurately identify 1,000+ mainstream applications on the entire network and their traffic usage, including Teams, DingTalk, WebEX, XYLink, and Skype.



For each application, you can view the traffic usage and specific users of the application. In addition, the application usage of the user can be played back throughout the user journey.

Ainda no mesmo documento, página 20, temos um mapa para visualização de utilização das aplicações:

HUAWEI Products and Solutions Learning and Tech Support Partners How to Buy About Us Search

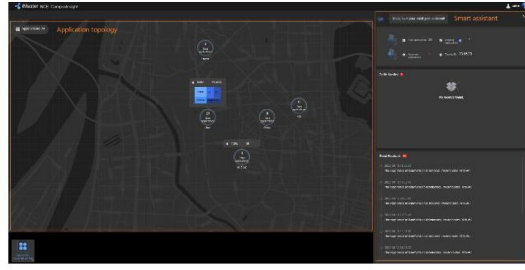
Home > Huawei iMaster NCE-CampusInsight DataSheet

Huawei iMaster NCE-CampusInsight DataSheet

Download(4.0MB) Share 20 / 32

Application Experience Map

The homepage of the application experience map displays the site topology, including the total number of applications, total traffic, and top N applications with the largest traffic. The smart assistant pane on the right displays the number of applications, traffic, to-dos, and event broadcast.



The **Application Statistics** page displays the total number of applications and numbers of normal and abnormal applications. The application list displays the application name, traffic, and total number of abnormal/service flows.

Com isso, comprovamos o atendimento ao item 3.3.4. do Anexo I – Especificação Técnica.

4.19) Do suposto não atendimento ao subitem 3.4.1. do Anexo I – Especificação Técnica

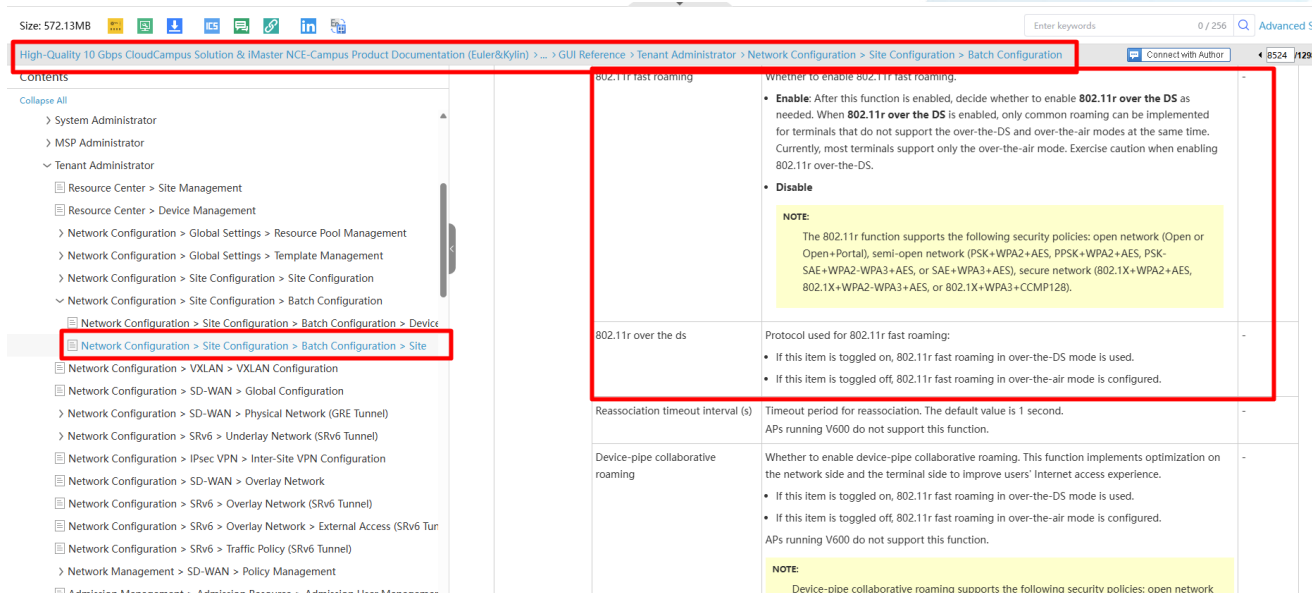
Aduz a Recorrente **TELESUL** que no documento, a licitante **3CORP** apresentou o fast roaming, o qual não comprova o roaming do IPv6 nem a manutenção da integridade da sessão para aplicações (VoIP, VoWLAN, VideoConf), essencial para ambientes modernos e de alta demanda, não atendendo o subitem abaixo.

3.4.1. Possibilitar roaming com integridade de sessão L2 e L3 IPV4/IPV6, dando suporte a aplicações em tempo real, tais como, VoIP, VoWLAN (Voz sem fio), videoconferência, dentre outras;

No entanto, esclarecemos que, a evidência apresentada atende integralmente ao descrito no item.

Foi realizado apontamento ao padrão técnico 802.11r:

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100413634&id=EN-US_TOPIC_0159770948



The screenshot shows a Huawei support page for '802.11r fast roaming'. The left sidebar contains a navigation tree with the following structure:

- System Administrator
- MSP Administrator
- Tenant Administrator
 - Resource Center > Site Management
 - Resource Center > Device Management
 - Network Configuration > Global Settings > Resource Pool Management
 - Network Configuration > Global Settings > Template Management
 - Network Configuration > Site Configuration > Site Configuration
 - Network Configuration > Site Configuration > Batch Configuration
 - Network Configuration > Site Configuration > Batch Configuration > Device
 - Network Configuration > Site Configuration > Batch Configuration > Site
 - Network Configuration > VXLAN > VXLAN Configuration
 - Network Configuration > SD-WAN > Global Configuration
 - Network Configuration > SD-WAN > Physical Network (GRE Tunnel)
 - Network Configuration > SRv6 > Underlay Network (SRv6 Tunnel)
 - Network Configuration > IPsec VPN > Inter-Site VPN Configuration
 - Network Configuration > SD-WAN > Overlay Network
 - Network Configuration > SRv6 > Overlay Network (SRv6 Tunnel)
 - Network Configuration > SRv6 > Overlay Network > External Access (SRv6 Tunnel)
 - Network Configuration > SRv6 > Traffic Policy (SRv6 Tunnel)
 - Network Management > SD-WAN > Policy Management
 - Admission Management > Admission Resource > Admission User Management

The main content area displays the configuration details for '802.11r fast roaming'. The 'Enable' section states: 'After this function is enabled, decide whether to enable 802.11r over the DS as needed. When 802.11r over the DS is enabled, only common roaming can be implemented for terminals that do not support the over-the-DS and over-the-air modes at the same time. Currently, most terminals support only the over-the-air mode. Exercise caution when enabling 802.11r over-the-DS.' The 'Disable' section is empty. The 'NOTE' section states: 'The 802.11r function supports the following security policies: open network (Open or Open+Portal), semi-open network (PSK+WPA2+AES, PPSK+WPA2+AES, PSK+SAE+WPA2-WPA3+AES, or SAE+WPA3+AES), secure network (802.1X+WPA2+AES, 802.1X+WPA2-WPA3+AES, or 802.1X+WPA3+CCMP128).' The '802.11r over the ds' section states: 'Protocol used for 802.11r fast roaming: If this item is toggled on, 802.11r fast roaming in over-the-DS mode is used. If this item is toggled off, 802.11r fast roaming in over-the-air mode is configured.' The 'Reassociation timeout interval (s)' section states: 'Timeout period for reassociation. The default value is 1 second. APs running V600 do not support this function.' The 'Device-pipe collaborative roaming' section states: 'Whether to enable device-pipe collaborative roaming. This function implements optimization on the network side and the terminal side to improve users' Internet access experience. If this item is toggled on, 802.11r fast roaming in over-the-DS mode is used. If this item is toggled off, 802.11r fast roaming in over-the-air mode is configured. APs running V600 do not support this function.' The 'NOTE' section states: 'Device-pipe collaborative roaming supports the following security policies: open network'.

Salientamos que o padrão 802.11r se aplica a IPV4 e IPV6, conforme sua descrição IEEE 802.11.

O mecanismo definido pelo 802.11r (*Fast BSS Transition – FT*) tem como objetivo otimizar o processo de mobilidade em redes WLAN, reduzindo o tempo de transição (*roaming*) entre pontos de acesso por meio da antecipação de processos de autenticação e estabelecimento de chaves criptográficas.

Ressalta-se que o referido padrão atua exclusivamente na **camada 2 (enlace de dados)** do modelo OSI, sendo responsável por procedimentos relacionados à mobilidade e segurança no domínio da rede sem fio (IEEE 802.11), não havendo qualquer interação direta com protocolos de camada 3.

Dessa forma, os protocolos IP, tais como IPv4 e IPv6, operam em camada superior e são **completamente transparentes** aos mecanismos implementados pelo 802.11r. Não existe, portanto:

- dependência funcional entre o 802.11r e o protocolo IP utilizado;
- limitação técnica quanto ao uso de IPv4 ou IPv6;
- necessidade de configuração específica do 802.11r em função da versão do protocolo IP.

Adicionalmente, destaca-se que o funcionamento do 802.11r está intrinsecamente associado aos mecanismos de segurança definidos pelo padrão IEEE 802.11i (WPA2) e suas evoluções, sendo a troca e derivação de chaves criptográficas (PMK-R0 e PMK-R1) realizada no contexto da autenticação da rede sem fio, igualmente independente da pilha IP utilizada.

Diante do exposto, resta tecnicamente comprovado que o padrão 802.11r:

- é agnóstico ao protocolo IP;
- é plenamente aplicável em redes IPv4, IPv6 ou em ambiente dual stack;
- não impõe qualquer restrição ou condicionante relacionada à camada 3 da rede.

Portanto, qualquer interpretação que condicione a aplicação do 802.11r ao uso específico de IPv4 ou IPv6 não encontra respaldo técnico nos padrões IEEE, devendo ser desconsiderada.

O 802.11r é um **padrão (emenda normativa)** da família IEEE 802.11, e não apenas uma recomendação ou regulamentação. Ele é amplamente utilizado em ambientes corporativos para garantir **mobilidade contínua com baixa latência**, sendo especialmente relevante em redes com alta densidade de APs e aplicações críticas.

Adicionalmente, no datasheet, página 11, temos a informação de que o access point ofertado possui o padrão informado:

<https://e.huawei.com/marketingcloud/pep/asset/20000001/Material/f74dc124f31c4a3eb0c8b4ea77cf1efe/M3T1A590N1186039378695843981/Huawei%20AirEngine%206776-57T%20Access%20Point%20Datasheet.pdf>

Huawei AirEngine 6776-57T Access Point Datasheet

11 / 14

Standards Compliance

Item	Description
Safety standards	<ul style="list-style-type: none"> EN 62368-1 IEC 62368-1
Radio standards	<ul style="list-style-type: none"> ETSI EN 300 328 ETSI EN 303 687 ETSI EN 301 893 AN/NZS 4268
EMC standards	<ul style="list-style-type: none"> EN 301 489-1 EN 301 489-17 EN 60601-1-2 EN 55032 EN 55035 GB 9254 GB 17625.2 AS/NZS CISPR32 CISPR 32 CISPR 35 IEC/EN61000-4-2 IEC/EN 61000-4-3 IEC/EN 61000-4-4 IEC/EN 61000-4-5 IEC/EN 61000-4-6 ICES-003
IEEE standards	<ul style="list-style-type: none"> IEEE 802.11a/b/g IEEE 802.11n IEEE 802.11ac IEEE 802.11ax IEEE 802.11be IEEE 802.11h IEEE 802.11d IEEE 802.11e IEEE 802.11k IEEE 802.11v IEEE 802.11w IEEE 802.11r
Security standards	<ul style="list-style-type: none"> 802.11i, Wi-Fi Protected Access (WPA), WPA2, WPA2-Enterprise, WPA2-PSK, WPA3, WPA3-Enterprise 802.1X Advanced Encryption Standards(AES), Temporal Key Integrity Protocol(TKIP), WEP, Open EAP Type(s)
EMF	<ul style="list-style-type: none"> EN 62311 EN 50385
RoHS	<ul style="list-style-type: none"> Directive 2002/95/EC & 2011/65/EU (EU)2015/863
Reach	<ul style="list-style-type: none"> Regulation 1907/2006/EC
WEEE	<ul style="list-style-type: none"> Directive 2002/96/EC & 2012/19/EU

No mesmo documento, página 8, temos a mesma informação:

Huawei AirEngine 6776-57T Access Point Datasheet

8 / 14

Item	Description
	<ul style="list-style-type: none"> Advanced cellular coexistence (ACC), minimizing the impact of interference from cellular networks 802.11k and 802.11v smart roaming 802.11r fast roaming (≤ 50 ms) Spectrum analysis Terminal location FTM (Fine Timing Measurement) location
Network features	<ul style="list-style-type: none"> Compliance with IEEE 802.3ab Auto-negotiation of the rate and duplex mode, and automatic switchover between Media Dependent Interface (MDI) and Media Dependent Interface Crossover (MDI-X) Compatibility with IEEE 802.1Q SSID-based VLAN assignment DHCP client, obtaining IP addresses through DHCP STA isolation in the same VLAN IPv4/IPv6 access control list (ACL) Link Layer Discovery Protocol (LLDP) Service holdover when the link to NCE-Campus is disconnected Unified authentication on the cloud management platform Network address translation (NAT) Telemetry, quickly collecting AP status and application experience parameters MESH Tunnel-AC IPv6 SAVI HotSpot2.0

Diante do exposto, fica comprovado o atendimento ao item 3.4.1. do Anexo I – Especificação Técnica.

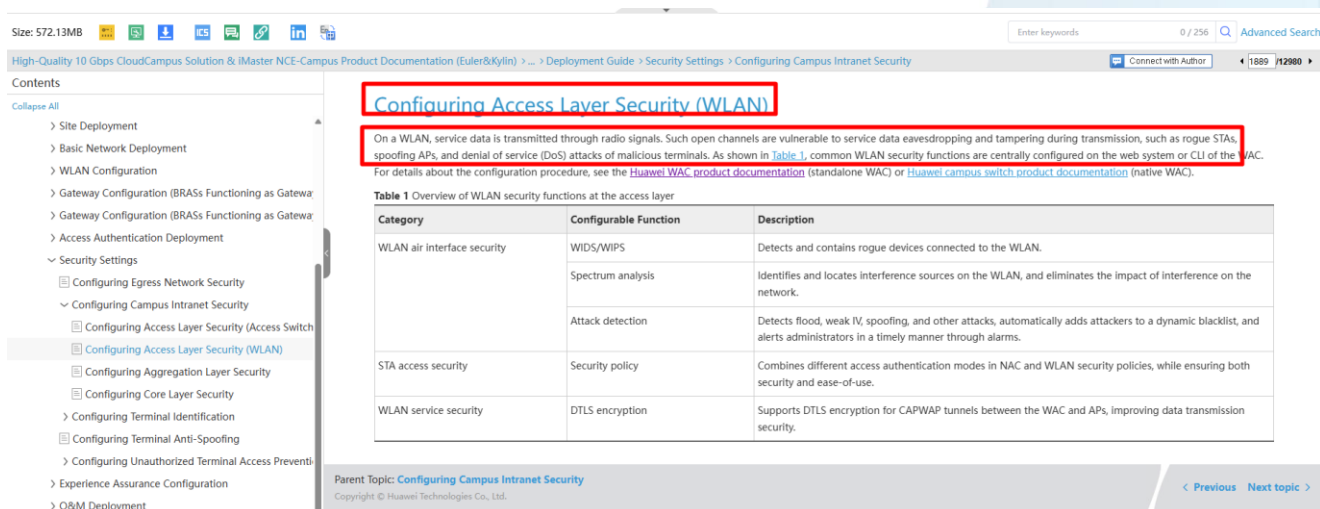
4.20) Do suposto não atendimento ao subitem 3.4.8. do Anexo I – Especificação Técnica

Aduz a Recorrente **TELESUL** que o link apresentado, não houve a comprovação que a solução possui assinaturas para detecção de ameaças, um componente crítico de segurança., não atendendo o subitem abaixo.

3.4.8. Possuir assinaturas de ataques de RF e prevenção de intrusão para rapidamente detectar ataques de RF mais comuns tais como denial of service (DoS).

No entanto, esclarecemos que, a evidência enviada comprova a solicitação descrita no item, inclusive com apontamento de tipos de ataques, incluído DOS.

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100413634&id=EN-US_TOPIC_000001167428289



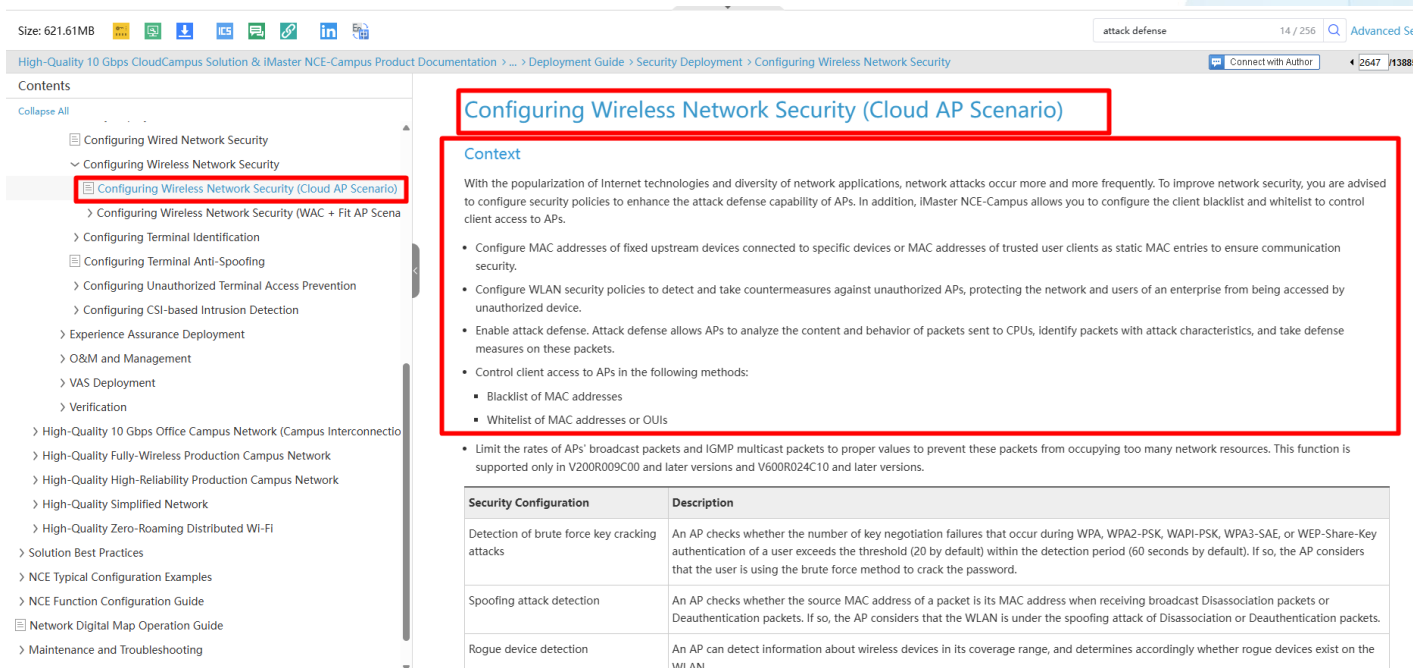
The screenshot shows a Huawei support page for 'Configuring Access Layer Security (WLAN)'. The page includes a table titled 'Table 1 Overview of WLAN security functions at the access layer'.

Category	Configurable Function	Description
WLAN air interface security	WIDS/WIPS	Detects and contains rogue devices connected to the WLAN.
	Spectrum analysis	Identifies and locates interference sources on the WLAN, and eliminates the impact of interference on the network.
	Attack detection	Detects flood, weak IV, spoofing, and other attacks, automatically adds attackers to a dynamic blacklist, and alerts administrators in a timely manner through alarms.
STA access security	Security policy	Combines different access authentication modes in NAC and WLAN security policies, while ensuring both security and ease-of-use.
WLAN service security	DTLS encryption	Supports DTLS encryption for CAPWAP tunnels between the WAC and APs, improving data transmission security.

A solução baseada na plataforma Huawei iMaster NCE-CloudCampus implementa mecanismos avançados de segurança WLAN por meio das funcionalidades WIDS/WIPS (Wireless Intrusion Detection and Prevention System). Esses recursos permitem a detecção e mitigação de ameaças no espectro de radiofrequência, incluindo ataques de negação de serviço (DoS), spoofing e flood. A solução utiliza análise de assinaturas e comportamento de tráfego para identificar atividades maliciosas, aplicando automaticamente contramedidas como blacklist dinâmica e geração de alarmes, garantindo a proteção proativa da rede sem fio.

Adicionalmente, abaixo link e imagem comprovando os recursos de segurança em ambiente Wlan.

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100516678&id=EN-US_TOPIC_0000001186150892



Size: 621.61MB

attack defense 14 / 256 Q Advanced Se

High-Quality 10 Gbps CloudCampus Solution & iMaster NCE-Campus Product Documentation > ... > Deployment Guide > Security Deployment > Configuring Wireless Network Security

Contents

Collapse All

- Configuring Wired Network Security
- Configuring Wireless Network Security
 - Configuring Wireless Network Security (Cloud AP Scenario)**
 - Configuring Wireless Network Security (WAC + Fit AP Scenario)
 - Configuring Terminal Identification
 - Configuring Terminal Anti-Spoofing
 - Configuring Unauthorized Terminal Access Prevention
 - Configuring CSI-based Intrusion Detection
 - Experience Assurance Deployment
 - O&M and Management
 - VAS Deployment
 - Verification
 - High-Quality 10 Gbps Office Campus Network (Campus Interconnection)
 - High-Quality Fully-Wireless Production Campus Network
 - High-Quality High-Reliability Production Campus Network
 - High-Quality Simplified Network
 - High-Quality Zero-Roaming Distributed Wi-Fi
- Solution Best Practices
- NCE Typical Configuration Examples
- NCE Function Configuration Guide
- Network Digital Map Operation Guide
- Maintenance and Troubleshooting

Configuring Wireless Network Security (Cloud AP Scenario)

Context

With the popularization of Internet technologies and diversity of network applications, network attacks occur more and more frequently. To improve network security, you are advised to configure security policies to enhance the attack defense capability of APs. In addition, iMaster NCE-Campus allows you to configure the client blacklist and whitelist to control client access to APs.

- Configure MAC addresses of fixed upstream devices connected to specific devices or MAC addresses of trusted user clients as static MAC entries to ensure communication security.
- Configure WLAN security policies to detect and take countermeasures against unauthorized APs, protecting the network and users of an enterprise from being accessed by unauthorized device.
- Enable attack defense. Attack defense allows APs to analyze the content and behavior of packets sent to CPUs, identify packets with attack characteristics, and take defense measures on these packets.
- Control client access to APs in the following methods:
 - Blacklist of MAC addresses
 - Whitelist of MAC addresses or OUIs
- Limit the rates of APs' broadcast packets and IGMP multicast packets to proper values to prevent these packets from occupying too many network resources. This function is supported only in V200R009C00 and later versions and V600R024C10 and later versions.

Security Configuration	Description
Detection of brute force key cracking attacks	An AP checks whether the number of key negotiation failures that occur during WPA, WPA2-PSK, WAPI-PSK, WPA3-SAE, or WEP-Share-Key authentication of a user exceeds the threshold (20 by default) within the detection period (60 seconds by default). If so, the AP considers that the user is using the brute force method to crack the password.
Spoofing attack detection	An AP checks whether the source MAC address of a packet is its MAC address when receiving broadcast Disassociation packets or Deauthentication packets. If so, the AP considers that the WLAN is under the spoofing attack of Disassociation or Deauthentication packets.
Rogue device detection	An AP can detect information about wireless devices in its coverage range, and determines accordingly whether rogue devices exist on the WLAN.

Diante do exposto, fica comprovado o atendimento ao item 3.4.8. do Anexo I – Especificação Técnica.

4.21) Do suposto não atendimento ao subitem 3.4.9. do Anexo I – Especificação Técnica

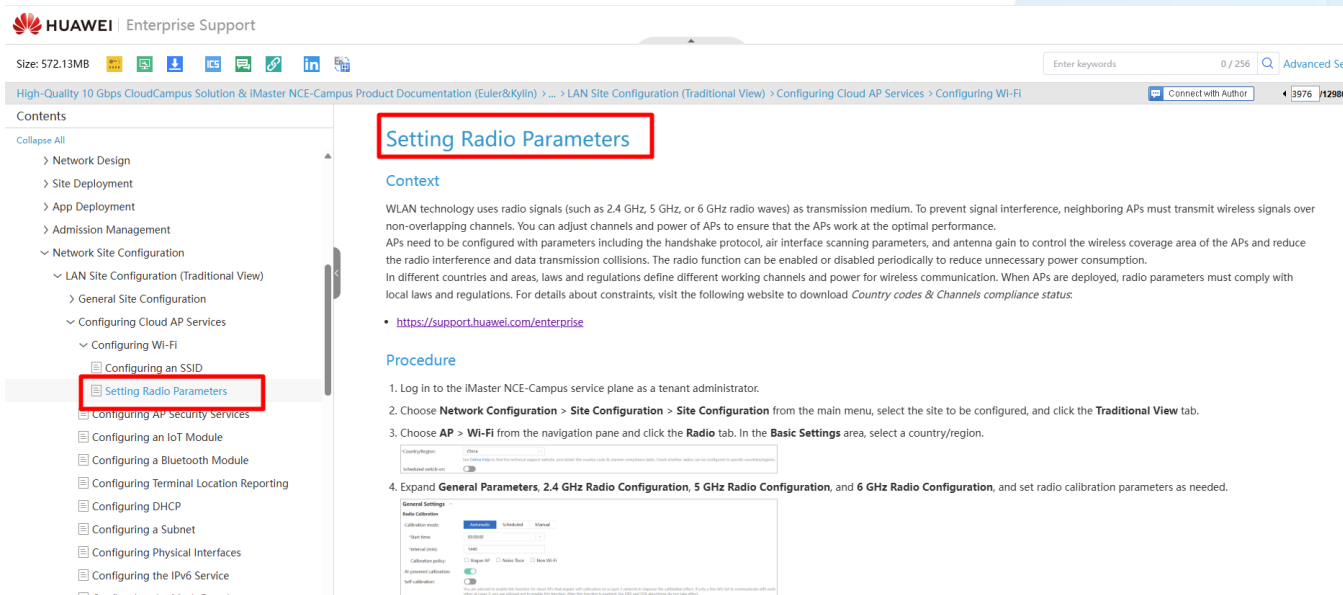
Aduz a Recorrente **TELESUL** que o link apresentado não se encontra nenhuma comprovação da varredura contínua de RF, e portanto, não atende o subitem abaixo.

3.4.9. Implementar varredura de RF contínua, programada ou sob demanda;

No entanto, esclarecemos que, a evidência enviada comprova o atendimento ao item.

No link abaixo há a informação de configuração dos parâmetros de rádio, dentre eles a função “Air interface scanning”.

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100413634&id=EN-US_TOPIC_0159898740



Setting Radio Parameters

Context

WLAN technology uses radio signals (such as 2.4 GHz, 5 GHz, or 6 GHz radio waves) as transmission medium. To prevent signal interference, neighboring APs must transmit wireless signals over non-overlapping channels. You can adjust channels and power of APs to ensure that the APs work at the optimal performance.

APs need to be configured with parameters including the handshake protocol, air interface scanning parameters, and antenna gain to control the wireless coverage area of the APs and reduce the radio interference and data transmission collisions. The radio function can be enabled or disabled periodically to reduce unnecessary power consumption.

In different countries and areas, laws and regulations define different working channels and power for wireless communication. When APs are deployed, radio parameters must comply with local laws and regulations. For details about constraints, visit the following website to download *Country codes & Channels compliance status*.

- <https://support.huawei.com/enterprise>

Procedure

1. Log in to the iMaster NCE-Campus service plane as a tenant administrator.
2. Choose **Network Configuration > Site Configuration > Site Configuration** from the main menu, select the site to be configured, and click the **Traditional View** tab.
3. Choose **AP > Wi-Fi** from the navigation pane and click the **Radio** tab. In the **Basic Settings** area, select a country/region.
4. Expand **General Parameters**, **2.4 GHz Radio Configuration**, **5 GHz Radio Configuration**, and **6 GHz Radio Configuration**, and set radio calibration parameters as needed.

A plataforma **iMaster NCE-CloudCampus**, em conjunto com os APs, permite:

1. Varredura contínua de RF

- APs em modo sensor realizam **monitoramento permanente do espectro RF**
- Identificação de:
 - APs rogue
 - Interferências

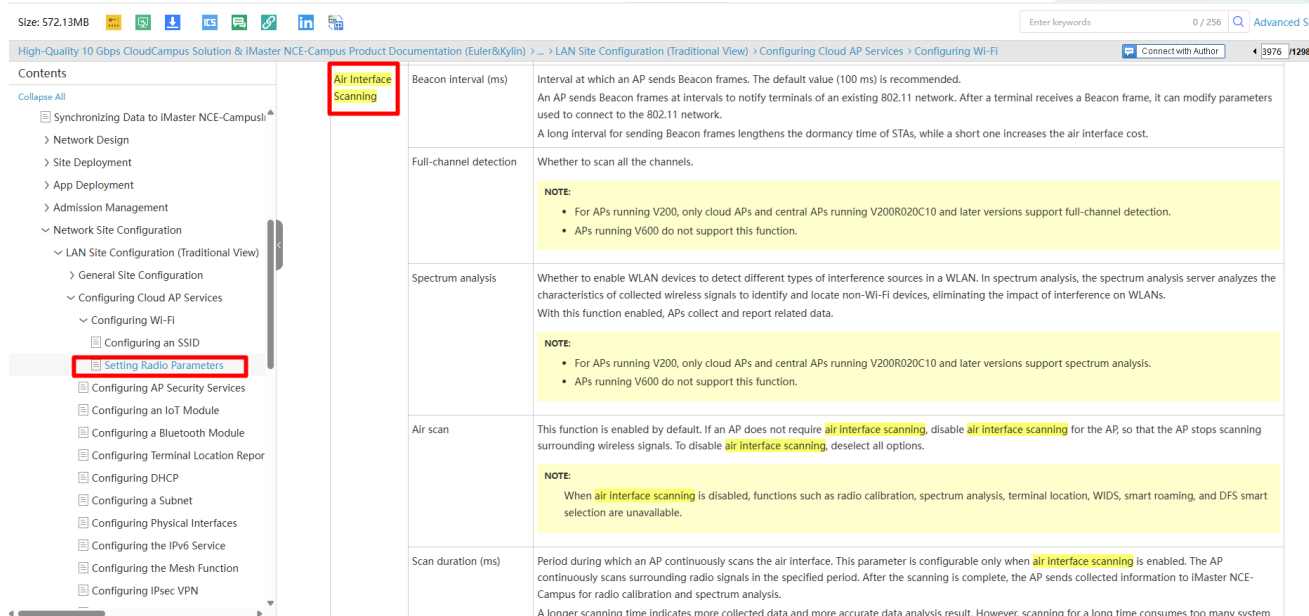
- Ataques wireless (DoS, spoofing, etc.)

2. Varredura programada

- Possibilidade de configurar **políticas e janelas de varredura**
- Ajuste de horários e frequência via controladora CloudCampus

3. Varredura sob demanda

- Execução manual de:
 - **Air Scan**
 - **Spectrum Analysis**
- Acionada diretamente pela interface do CloudCampus para troubleshooting



Size: 572.13MB

High-Quality 10 Gbps CloudCampus Solution & iMaster NCE-Campus Product Documentation (Euler&Kylin) > LAN Site Configuration (Traditional View) > Configuring Cloud AP Services > Configuring Wi-Fi

Contents

- Synchronizing Data to iMaster NCE-Campus
 - Network Design
 - Site Deployment
 - App Deployment
 - Admission Management
 - Network Site Configuration
 - LAN Site Configuration (Traditional View)
 - General Site Configuration
 - Configuring Cloud AP Services
 - Configuring Wi-Fi
 - Setting Radio Parameters**
 - Configuring AP Security Services
 - Configuring an IoT Module
 - Configuring a Bluetooth Module
 - Configuring Terminal Location Report
 - Configuring DHCP
 - Configuring a Subnet
 - Configuring Physical Interfaces
 - Configuring the IPv6 Service
 - Configuring the Mesh Function
 - Configuring IPsec VPN

Air Interface Scanning

Beacon interval (ms)	Interval at which an AP sends Beacon frames. The default value (100 ms) is recommended. An AP sends Beacon frames at intervals to notify terminals of an existing 802.11 network. After a terminal receives a Beacon frame, it can modify parameters used to connect to the 802.11 network. A long interval for sending Beacon frames lengthens the dormancy time of STAs, while a short one increases the air interface cost.
Full-channel detection	Whether to scan all the channels. NOTE: <ul style="list-style-type: none"> For APs running V200, only cloud APs and central APs running V200R020C10 and later versions support full-channel detection. APs running V600 do not support this function.
Spectrum analysis	Whether to enable WLAN devices to detect different types of interference sources in a WLAN. In spectrum analysis, the spectrum analysis server analyzes the characteristics of collected wireless signals to identify and locate non-Wi-Fi devices, eliminating the impact of interference on WLANs. With this function enabled, APs collect and report related data. NOTE: <ul style="list-style-type: none"> For APs running V200, only cloud APs and central APs running V200R020C10 and later versions support spectrum analysis. APs running V600 do not support this function.
Air scan	This function is enabled by default. If an AP does not require air interface scanning , disable air interface scanning for the AP, so that the AP stops scanning surrounding wireless signals. To disable air interface scanning , deselect all options. NOTE: <ul style="list-style-type: none"> When air interface scanning is disabled, functions such as radio calibration, spectrum analysis, terminal location, WIDS, smart roaming, and DFS smart selection are unavailable.
Scan duration (ms)	Period during which an AP continuously scans the air interface. This parameter is configurable only when air interface scanning is enabled. The AP continuously scans surrounding radio signals in the specified period. After the scanning is complete, the AP sends collected information to iMaster NCE-Campus for radio calibration and spectrum analysis. A longer scanning time indicates more collected data and more accurate data analysis result. However, scanning for a long time consumes too many system resources.

Adicionalmente, a documentação do access point demonstra o recurso “Air Scan Config” disponível:

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100510642&id=EN-US_TASK_0000002086465048

Size: 538.12MB

WLAN AP AirEngine X700 Product Documentation > ... > Web Configuration Guide > Web System Configuration (Fat AP) > Wireless Management

Contents

- Logging in to the web system
- Web System Configuration (Fat AP)
 - Configuring the Web Client
 - Monitoring
 - Configuration Wizard
 - Internet Access Configuration
 - Wireless Management
 - Wireless Service
 - Wi-Fi Optimization**
 - AP List
 - AP Configuration
 - Terminal Location
 - LAN
 - IoT
 - Diagnosis and O&M
 - Template Management
 - Security Policy
 - System Management
- Web System Configuration (Cloud AP)
- Web System Configuration (Fit AP)

Probe report interval (s)	Interval for reporting Probe frames. After an AP receives information about neighboring APs of STAs, it reports the information to the AC for determining the target APs to which the STAs will roam. You are advised to retain the default value. If the device has high performance pressure, you can set a longer interval. The value range is 30 to 300. The default value is 120.
Air Scan Config	-
Scanning	Whether to enable the scanning function.
Probe channel set	Air scan channel set. <ul style="list-style-type: none"> Country code channels: specifies an air scan channel set that contains all channels supported by the country code of an AP. Calibration channels: specifies a calibration channel set as the air scan channel set. Working channels: specifies an air scan channel set that contains working channels of an AP.
Channel scanning interval (ms)	Air scan interval. The value range is 300 to 600000. The default value is 10000. If the customer has high requirements on real-time data analysis, configure a small air scan interval to improve the scan frequency; however, higher scan frequency indicates a greater impact on services. In vehicle-ground communication scenarios, the air scan interval ranges from 300 ms to 1000 ms.
Channel scanning duration (ms)	Air scan period. The value range is 60 to 100. The default value is 60. A longer air scan period indicates more collected data and a more accurate data analysis result. However, if the air scan period is too large, WLAN services are affected. Therefore, the default value is recommended.

Diante do exposto, fica comprovado o atendimento ao item 3.4.9. do Anexo I – Especificação Técnica.

4.22) Do suposto não atendimento ao subitem 3.4.14. do Anexo I – Especificação Técnica

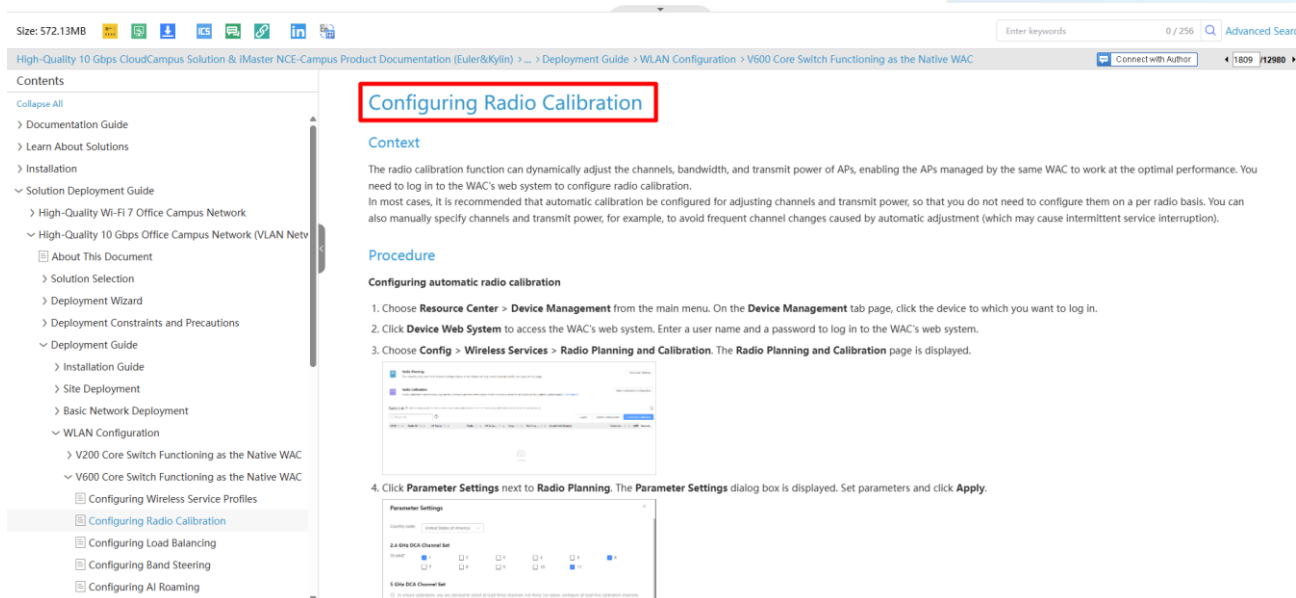
Aduz a Recorrente **TELESUL** que os quatro links apresentados não foi possível demonstrar que o produto ofertado consegue realizar o ajuste automático da potência dos access-points adjacentes para cobrir a rede em caso de falha de um access-point, com impacto na resiliência e disponibilidade do serviço, não atende o subitem abaixo.

3.4.14. Deve possuir recursos instalados para implementar mecanismo que no evento de falha de um Ponto de Acesso, a controladora ajuste automaticamente a potência dos Pontos de Acesso adjacentes para dar cobertura à área onde o Ponto de Acesso que falhou estava provendo o sinal;

No entanto, esclarecemos que, as comprovações para atendimento a este item foram enviadas, este é realizado pelo recurso RRM (Radio Resource Management), configurado de forma combinada em alguns recursos, conforme links e imagens abaixo:

Radio Calibration

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100413634&id=EN-US_TOPIC_0000001986319217



Configuring Band Steering

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100413634&id=EN-US_TOPIC_000001952799796

Size: 572.13MB

High-Quality 10 Gbps CloudCampus Solution & iMaster NCE-Campus Product Documentation (Euler&Kylin) > ... > Deployment Guide > WLAN Configuration > V600 Core Switch Functioning as the Native WAC

Contents

- High-Quality 10 Gbps Office Campus Network (VXLAN)
- High-Quality 10 Gbps Office Campus Network (Cloud)
- High-Quality 10 Gbps Office Campus Network (Campus)
- High-Quality Fully-Wireless Production Campus Network
- High-Quality High-Reliability Production Campus Network
- High-Quality Simplified Network

Configuring Band Steering

Context

On live networks, most STAs support both 2.4 GHz and 5 GHz frequency bands but usually associate with the 2.4 GHz radio by default when connecting to the WLAN. As a result, the 2.4 GHz frequency band with fewer channels is congested, heavily-loaded, and has severe interference. The 5 GHz frequency band with more channels and less interference is not well used. When the 2.4 GHz frequency band is overloaded or has severe interference, the 5 GHz frequency band can provide better access service for wireless users. However, users must manually select the 5 GHz radio to connect to it.

The band steering function enables an AP to steer STAs to the 5 GHz radio preferentially. This reduces the traffic load and interference on the 2.4 GHz frequency band and improves user experience. It is recommended that the band steering function be enabled by default. This function, together with the load balancing function, can evenly distribute STAs on one and multiple APs and improve user experience across the entire network.

NOTE

- The two frequency bands of an AP enabled with the band steering function must use the same SSID and security policy. The band steering function cannot be deployed on a single-radio AP.
- To allow STAs to preferentially associate with the 5 GHz radio and achieve better access effect, configure larger power for the 5 GHz radio than the 2.4 GHz radio.
- A Wi-Fi 7 AP supports the 6 GHz frequency band, but does not support band steering between 2.4 GHz/5 GHz and 6 GHz frequency bands.

Procedure

- Create an AP group and bind a VAP profile to the AP group.


```
[HUAWEI] system-view
[HUAWEI] sysname WAC
[WAC] wlan
[WAC-wlan] ap-group name ap-group1
[WAC-wlan-ap-group-ap-group1] quit
```

Size: 572.13MB

High-Quality 10 Gbps CloudCampus Solution & iMaster NCE-Campus Product Documentation (Euler&Kylin) > ... > Deployment Guide > WLAN Configuration > V600 Core Switch Functioning as the Native WAC

Contents

- High-Quality 10 Gbps Office Campus Network (VXLAN)
- High-Quality 10 Gbps Office Campus Network (Cloud)
- High-Quality 10 Gbps Office Campus Network (Campus)
- High-Quality Fully-Wireless Production Campus Network
- High-Quality High-Reliability Production Campus Network
- High-Quality Simplified Network

Configuring Band Steering

NOTE

When band steering is enabled on any radio of an AP, the function takes effect on the SSID of the AP. If different VAP profiles are applied to two radios of the AP, you only need to enable the band steering function in the VAP profile of one radio.

```
[WAC-wlan] vap-profile name wlan-net
[WAC-wlan-vap-prof-wlan-vap] undo band-steer disable
[WAC-wlan-vap-prof-wlan-vap] quit
```

Create the RRM profile wlan-rrm and configure load balancing between radios in the profile to prevent a heavy load on a single radio. The start threshold for load balancing between radios is 15, and the load difference threshold is 25%.

```
[WAC-wlan] rrm-profile name wlan-rrm
[WAC-wlan-rrm-prof-wlan-rrm] band-steer balance start-threshold 15
[WAC-wlan-rrm-prof-wlan-rrm] band-steer balance gap-threshold 25
[WAC-wlan-rrm-prof-wlan-rrm] quit
```

Create the 2.4 GHz radio profile radio2g and bind the RRM profile wlan-rrm to the 2.4 GHz radio profile.

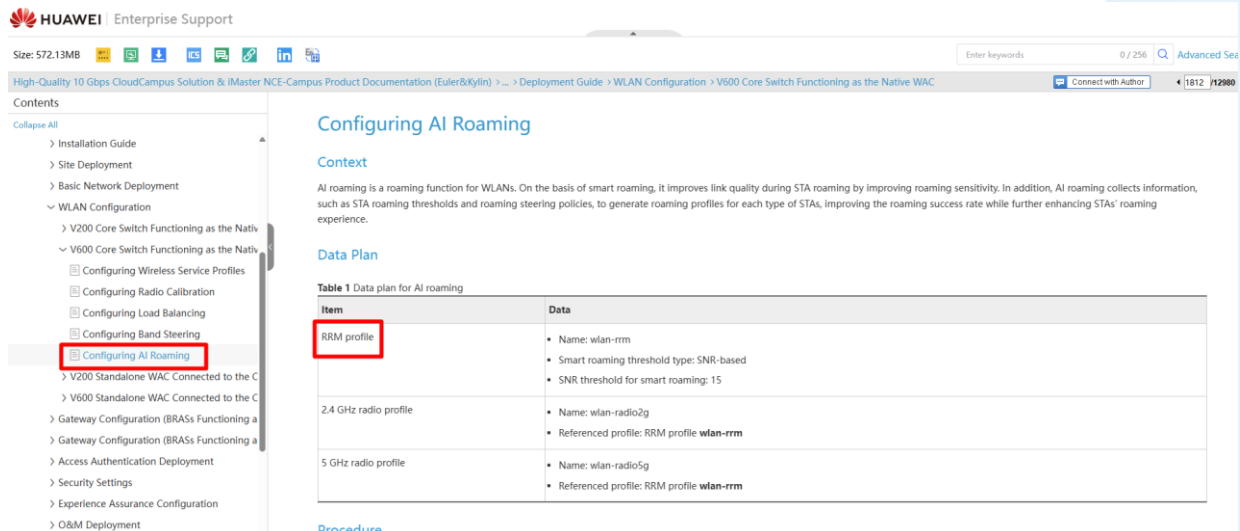
NOTE

If different RRM profiles are bound to the 2.4 GHz and 5 GHz radio profiles and configured with different band steering parameters, parameter settings in the 2.4 GHz radio profile preferentially take effect.

```
[WAC-wlan] radio-2g-profile name radio2g
[WAC-wlan-radio-2g-prof-radio2g] rrm-profile wlan-rrm
Warning: This action may cause service interruption. Continue? [Y/N] y
[WAC-wlan-radio-2g-prof-radio2g] quit
```

Configuring AI Roaming

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100413634&id=EN-US_TOPIC_000001839375729



HUAWEI Enterprise Support

Size: 572.13MB

High-Quality 10 Gbps CloudCampus Solution & iMaster NCE-Campus Product Documentation (Euler&Kylin) > ... > Deployment Guide > WLAN Configuration > V600 Core Switch Functioning as the Native WAC

Contents

- Installation Guide
- Site Deployment
- Basic Network Deployment
- WLAN Configuration
 - V200 Core Switch Functioning as the Native WAC
 - V600 Core Switch Functioning as the Native WAC
 - Configuring Wireless Service Profiles
 - Configuring Radio Calibration
 - Configuring Load Balancing
 - Configuring Band Steering
 - Configuring AI Roaming**
 - V200 Standalone WAC Connected to the Core Network
 - V600 Standalone WAC Connected to the Core Network
 - Gateway Configuration (BRASs Functioning as the Native WAC)
 - Access Authentication Deployment
 - Security Settings
 - Experience Assurance Configuration
 - O&M Deployment

Configuring AI Roaming

Context

AI roaming is a roaming function for WLANs. On the basis of smart roaming, it improves link quality during STA roaming by improving roaming sensitivity. In addition, AI roaming collects information, such as STA roaming thresholds and roaming steering policies, to generate roaming profiles for each type of STAs, improving the roaming success rate while further enhancing STAs' roaming experience.

Data Plan

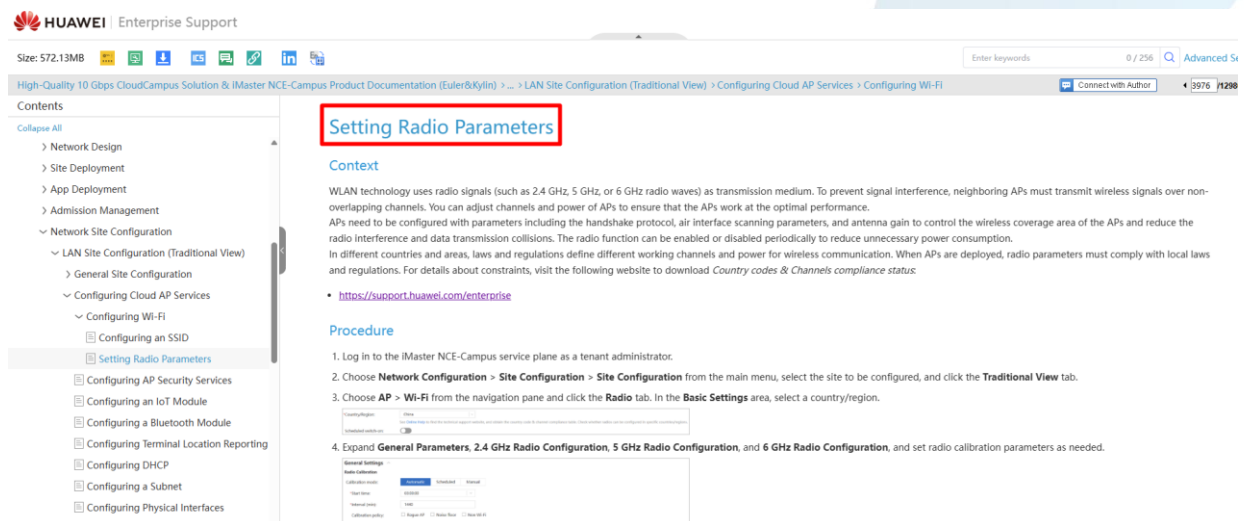
Table 1 Data plan for AI roaming

Item	Data
RRM profile	<ul style="list-style-type: none"> Name: wlan-rrm Smart roaming threshold type: SNR-based SNR threshold for smart roaming: 15
2.4 GHz radio profile	<ul style="list-style-type: none"> Name: wlan-radio2g Referenced profile: RRM profile wlan-rrm
5 GHz radio profile	<ul style="list-style-type: none"> Name: wlan-radio5g Referenced profile: RRM profile wlan-rrm

Procedure

Setting Radio Parameters

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100413634&id=EN-US_TOPIC_0159898740



HUAWEI Enterprise Support

Size: 572.13MB

High-Quality 10 Gbps CloudCampus Solution & iMaster NCE-Campus Product Documentation (Euler&Kylin) > ... > LAN Site Configuration (Traditional View) > Configuring Cloud AP Services > Configuring Wi-Fi

Contents

- Network Design
- Site Deployment
- App Deployment
- Admission Management
- Network Site Configuration
 - LAN Site Configuration (Traditional View)
 - General Site Configuration
 - Configuring Cloud AP Services
 - Configuring Wi-Fi
 - Configuring an SSID
 - Setting Radio Parameters**
 - Configuring AP Security Services
 - Configuring an IoT Module
 - Configuring a Bluetooth Module
 - Configuring Terminal Location Reporting
 - Configuring DHCP
 - Configuring a Subnet
 - Configuring Physical Interfaces

Setting Radio Parameters

Context

WLAN technology uses radio signals (such as 2.4 GHz, 5 GHz, or 6 GHz radio waves) as transmission medium. To prevent signal interference, neighboring APs must transmit wireless signals over non-overlapping channels. You can adjust channels and power of APs to ensure that the APs work at the optimal performance. APs need to be configured with parameters including the handshake protocol, air interface scanning parameters, and antenna gain to control the wireless coverage area of the APs and reduce the radio interference and data transmission collisions. The radio function can be enabled or disabled periodically to reduce unnecessary power consumption. In different countries and areas, laws and regulations define different working channels and power for wireless communication. When APs are deployed, radio parameters must comply with local laws and regulations. For details about constraints, visit the following website to download *Country codes & Channels compliance status*:

- <https://support.huawei.com/enterprise>

Procedure

- Log in to the iMaster NCE-Campus service plane as a tenant administrator.
- Choose **Network Configuration** > **Site Configuration** > **Site Configuration** from the main menu, select the site to be configured, and click the **Traditional View** tab.
- Choose **AP** > **Wi-Fi** from the navigation pane and click the **Radio** tab. In the **Basic Settings** area, select a country/region.
- Expand **General Parameters**, **2.4 GHz Radio Configuration**, **5 GHz Radio Configuration**, and **6 GHz Radio Configuration**, and set radio calibration parameters as needed.

A solução baseada no Huawei iMaster NCE-CloudCampus suporta **Radio Resource Management (RRM)** com **Radio Calibration e Transmit Power Control (TPC)**, permitindo o ajuste automático da potência dos Pontos de Acesso vizinhos em caso de falha de um AP, garantindo a compensação de cobertura (coverage hole compensation) e continuidade do serviço sem intervenção manual.

Abaixo evidência do Transmit Power Control (TPC):

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100510642&id=EN-US_TASK_0000002086465048

Size: 538.12MB

WLAN AP AirEngine X700 Product Documentation > ... > Web Configuration Guide > Web System Configuration (Fat AP) > Wireless Management

Contents

- Web Configuration Guide
 - Overview
 - Precautions for Web System Login
 - Logging In to the Web System
 - Web System Configuration (Fat AP)
 - Configuring the Web Client
 - Monitoring
 - Configuration Wizard
 - Internet Access Configuration
 - Wireless Management
 - Wireless Service
 - Wi-Fi Optimization**
 - AP List
 - AP Configuration
 - Terminal Location
 - LAN
 - IoT
 - Diagnosis and O&M
 - Template Management
 - Security Policy

Wi-Fi Optimization

Context

The radio planning and calibration function can dynamically adjust the channels, bandwidth, and transmit power of APs, enabling APs to work at the optimal performance.

Procedure

- Planning radios
 - Choose **Wireless Management > Wi-Fi Optimization**. The **Wi-Fi Optimization** page is displayed, as shown in [Figure 1](#).

Figure 1 Wi-Fi Optimization page

- Click **Settings** next to **Radio Planning**. The **Settings** dialog box is displayed, as shown in [Figure 2](#).

Figure 2 Settings dialog box

2.4G lower calibration power threshold (dBm)	The value range is 1 to 127. The default value is 127.
5G upper calibration power threshold (dBm)	Minimum transmit power that can be adjusted through 2.4G radio calibration. The value range is 1 to 127. The default value is 9.
5G lower calibration power threshold (dBm)	Maximum transmit power that can be adjusted through 5 GHz radio calibration. The value range is 1 to 127. The default value is 12.
6G upper calibration power threshold (dBm)	Minimum transmit power that can be adjusted through 6 GHz radio calibration. The value range is 1 to 127. The default value is 12.
6G lower calibration power threshold (dBm)	Maximum transmit power that can be adjusted through 6 GHz radio calibration. The value range is 1 to 127. The default value is 12.
Calibration TPC threshold (dBm)	Transmit Power Control (TPC) coverage threshold. The value range is -85 to -35. The default value is -60. The default value is recommended. You can also adjust the value based on the calibration result. A larger threshold indicates a wider transmit power range that can be adjusted through TPC.
Calibration group threshold (dBm)	Threshold for a calibration group. If the RSSI of a neighbor working at the maximum power exceeds the threshold, the neighbor is added to the same calibration group. The value range is -127 to -1. The default value is -127.
User CAC	-
UAC policy	Whether to enable CAC based on the number of users. The default setting is Off .
New user count threshold	User CAC access threshold based on the number of users. The value range is 1 to 1024. The default value is 64.

Diante do exposto, fica comprovado o atendimento ao item 3.4.14. do Anexo I – Especificação Técnica.

4.23) Do suposto não atendimento ao subitem 3.5.1. do Anexo I – Especificação Técnica

Aduz a Recorrente **TELESUL** que a Recorrida **3CORP**, apresentou um texto que não faz referência a comunicação entre o access-point e a nuvem (ou controller), desta forma, não comprovou que o tráfego de controle entre o AP e a controller é criptografado, expondo a comunicação a riscos de segurança, alegando não atendimento ao subitem abaixo.

3.5.1. Implementar criptografia do tráfego de controle, na comunicação entre Pontos de Acesso e a controladora ou sistema de gerenciamento centralizado;

No entanto, esclarecemos que, a evidência enviada comprova o atendimento ao item descrito.

No link e imagem abaixo é demonstrada a configuração de DTLS para comunicação entre a Plataforma de Gerência e dispositivo.

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100413634&id=EN-US_TOPIC_0283477168

Size: 572.13MB

Enter keywords 0 / 256 Advanced

High-Quality 10 Gbps CloudCampus Solution & iMaster NCE-Campus Product Documentation (Euler&Kylin) > NCE Function Configuration Guide > MSP-level Configuration > Network Design






Connect with Author 3152 / 12

Contents	IPsec SA generation mode	Whether to configure the IPsec SA generation mode. By default, this item is toggled off.
<ul style="list-style-type: none"> High-Quality 10 Gbps CloudCampus Solution & iMaster NCE-Campus Product Documentation (Euler&Kylin) NCE Function Configuration Guide <ul style="list-style-type: none"> Getting to Know iMaster NCE-Campus Deployment Constraints and Precautions Configuration Procedure Configuration Fundamentals System-level Configuration MSP-level Configuration <ul style="list-style-type: none"> Initial Configuration Network Design <ul style="list-style-type: none"> Setting Global Parameters Adding IWGs and RRs (Optional) Configuring the Device Access C... Creating an RR Site (Optional) Creating an IWG Site Configuring Site Isolation Viewing RR Access Statistics Viewing Gateway Access Statistics (Optional) Configuring an Email Template (Optional) Configuring a WAN Link Templat Configuring a Physical Interface Configuring the Network Access Mode for F Configuration MTD 	<p>IPsec SA generation mode</p> <p>Whether to configure the IPsec SA generation mode. By default, this item is toggled off.</p>	<p>Whether to configure the IPsec SA generation mode. By default, this item is toggled off.</p>
<p>Port Configuration</p> <p>DTLS server port</p> <p>STUN server port</p> <p>Connection source port</p>	<p>DTLS server port</p> <p>STUN server port</p> <p>Connection source port</p>	<p>Diffie-Hellman (DH) public key algorithm. It is used to dynamically negotiate encryption keys between two sites to prevent traffic monitoring between tenants connected to the same RR in multi-tenant scenarios.</p> <p>After IPsec SA generation mode is toggled on, you can select a DH group. Currently, DH group can be set only to GROUP19, GROUP20, or GROUP21. The DH group security levels are as follows: GROUP21 > GROUP20 > GROUP19. AR6700V devices do not support this function.</p> <p>Port number checked by the DTLS server.</p> <p>CPEs and RRs set up control channels over DTLS connections for TNP information exchange. When an RR goes online, iMaster NCE-Campus delivers the command for configuring the port checked by the DTLS server to the RR. As such, the RR can set up control channels with CPEs. By default, the port checked by the DTLS server is 55100. You can modify this setting as needed.</p> <p>In most cases, an RR is configured as a STUN server and the CPE functioning as a branch gateway is configured as a STUN client. To detect whether a NAT device is deployed between the RRs and CPEs, you need to enable the STUN server function on the RRs and configure the IP address and UDP port number to be checked by the STUN server for STUN messages. By default, the port checked by the STUN server is 3478. You can modify this setting as needed.</p> <p>After this item is toggled on, you can specify the scanning start port, scanning times, and scanning increment for NAT detection, hole punching, and Keepalive (KA) packets.</p>
<p>Device Activation Security</p> <p>Encryption</p> <p>Email-based deployment URL encryption key</p>	<p>Encryption</p> <p>Email-based deployment URL encryption key</p>	<p>Whether to encrypt the URL for email-based deployment. You are advised to enable this function. This function must be enabled if email-based deployment needs to be used for deploying devices running V600.</p> <p>Key for encrypting the URL in a deployment email. Email-based deployment will be successful only after you click the URL in the received email on your PC and enter this key. After the encryption key is changed, the deployment URL is encrypted using the new encryption key when a deployment email is sent to any account of the tenant. After configuring the key, keep it secure to prevent email-based deployment from being affected.</p> <p>The key must contain 8 to 12 digits and letters. If Compatibility obsolete devices is selected, the key complexity requirements will decrease. (For devices running versions earlier than V300R019C10, the key can contain only 6 to 12 digits.) Exercise caution when performing this operation.</p> <p>After this function is enabled, only the password in the URL for email-based deployment is encrypted.</p>

Esta configuração se aplica a todo dispositivo conectado ao NCE-CampusCloud.

Adicionalmente, no datasheet do Access Point (AirEngine 6776-57T), página 9, há a evidência dos mecanismos de segurança utilizados para conexão à Plataforma de Gerência.

<https://e.huawei.com/en/documents/products/enterprise-network/f74dc124f31c4a3eb0c8b4ea77cf1efe>

 Products and Solutions Learning and Tech Support Partners How to Buy About Us Search 	
Huawei AirEngine 6776-57T Access Point Datasheet	
<div>Download(0.7MB) Share <div>9 / 14</div>   </div>	
Item	Description
Security features	<div>Open system authentication</div> <div>WPA2-PSK authentication and encryption (WPA2-Personal)</div> <div>WPA2-802.1X authentication and encryption (WPA2-Enterprise)</div> <div>WPA3-SAE authentication and encryption (WPA3-Personal)</div> <div>WPA3-802.1X authentication and encryption (WPA3-Enterprise)</div> <div>WPA-WPA2 hybrid authentication</div> <div>WPA2-WPA3 hybrid authentication</div> <div>WPA/WPA2/WPA3-PPSK authentication and encryption</div> <div>WPA/WPA2/WPA3-DPSK authentication and encryption</div> <div>802.1X authentication, MAC address authentication, and Portal authentication</div> <div>Wireless intrusion detection system (WIDS) and wireless intrusion prevention system (WIPS), including rogue device detection and containment, attack detection and dynamic blacklist, and STA/AP blacklist and whitelist</div> <div>DHCP snooping</div> <div>802.11w Protected Management Frames (PMF)</div> <div>CAPWAP DTLS data encryption and decryption</div> <div>URL filtering</div> <div>MACsec@ Uplink Ethernet port</div> <div>Secure boot</div> <div>Support the following encryption protocols: COMP/AES TKIP</div> <div>SSL and TLS:</div> <div>RC4 128-bit</div> <div>RSA 1024-bit</div> <div>RSA 2048-bit</div>
EAP types	EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-CHAP, EAP-SIM, EAP-AKA, EAP-GTC, EAP-FAST, EAP-PEAP, EAP-MD5, EAP-MSCHAPv2, PEAPv0, PEAPv1
Maintenance features	<div>Unified AP management and maintenance on the cloud management platform</div> <div>Automatic AP onboarding, automatic configuration loading, and PnP</div> <div>Batch upgrade</div> <div>STelnet using SSHv2</div> <div>SFTP using SSHv2</div> <div>Remote wireless O&M through the Bluetooth serial port</div> <div>Real-time user configuration monitoring and fast fault locating using the NMS</div>

Diante do exposto, fica comprovado o atendimento ao item 3.5.1. do Anexo I – Especificação Técnica.

4.24) Do suposto não atendimento ao subitem 3.5.6. do Anexo I – Especificação Técnica

Aduz a Recorrente **TELESUL** que a Recorrida **3CORP**, não comprovou que o servidor Radius ou LDAP pode ser selecionado com base no SSID, funcionalidade importante para flexibilidade de autenticação, alegando não atendimento ao subitem abaixo.

3.5.6. Permitir a seleção/uso de servidor Radius ou LDAP com base no SSID;

No entanto, esclarecemos que, a evidência enviada comprova por meio de exemplo de configuração o atendimento ao item 3.5.6., demonstrando a configuração de um SSID guest e a forma de autenticação Dot1x, conforme abaixo:

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100413634&id=EN-US_TOPIC_0298429731

Size: 572.13MB

High-Quality 10 Gbps CloudCampus Solution & iMaster NCE-Campus Product Documentation (Euler&Kylin) > NCE Typical Configuration Examples > Examples for Configuring Access Authentication (NETCONF-based Device Management, VLAN Networking)

Contents

- Configuring Portal Authentication for Wireless Users (Cloud)
- Configuring Portal Authentication for Wireless Users (Cloud)
- Configuring Wireless Portal Authentication (Standalone WA)
- Configuring Portal Authentication for Wireless Users (Stand)
- Configuring Portal Authentication for Wireless Users (Stand)
- Configuring Portal Authentication for Wired Users (Userman)
- Configuring Portal Authentication for Wired Users (Userman)
- Configuring Portal Authentication for Wired Users (Authentic)
- Configuring 802.1X Authentication for Wireless Users (Native)
- Configuring 802.1X Authentication for Wireless Users in Boarding Mode (Native WAC, Single SSID, Built-in CA Server)
- Configuring 802.1X Authentication for Wireless Users in Boarding Mode (Native WAC, Interconnected CA Server)
- Configuring 802.1X Authentication for Wireless Users (Cloud)
- Configuring 802.1X Authentication for Wireless Users (Cloud)
- Configuring 802.1X Authentication for Wired Users (Using #)
- Configuring 802.1X Authentication for Wired Users (Using #)
- Configuring 802.1X Certificate-based EAP-TLS Authentication
- Configuring Certificate-based 802.1X Authentication Using
- Configuring Host Name-based Certificate Authentication ar
- Configuring Automatic MAC Address Authentication for Wi

Configuring 802.1X Authentication for Wireless Users in Boarding Mode (Native WAC, Single SSID, Built-in CA Server)

Networking Requirements

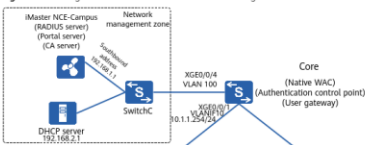
An enterprise has deployed a campus network as shown in [Figure 1](#).

- iMaster NCE-Campus manages switches on the campus network, functions as a RADIUS server and a Portal server for user authentication, and also functions as a CA server for certificate management.
- An independent DHCP server is deployed in the network management zone to dynamically allocate IP addresses to user terminals.
- Core provides the native WAC function to manage APs.

It is required that Core function as a DHCP relay agent and a user gateway for wireless users. In addition, the laptop is required to access the campus network through 802.1X authentication. The detailed requirements are as follows:

- Core serves as the authentication control point for wireless users.
- The Boarding function needs to be enabled on iMaster NCE-Campus, allowing the laptop to download a Boarding client for automatically configuring 802.1X access parameters. User terminals connect to the same SSID to download a Boarding client and for Internet access.

Figure 1 Boarding-based 802.1X authentication with a single SSID and the built-in CA server



[Collapse All](#)

- Table 3**
- Boarding management data plan

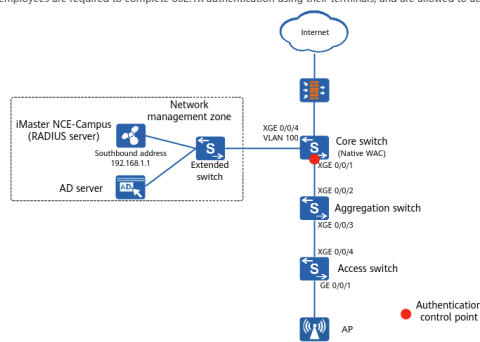
Table 4 WLAN service data plan (configured on the WAC's web system)

Parameter	Value
SSID profile	<ul style="list-style-type: none"> Profile name: wlan-guest SSID name: wlan-guest
Security profile	<ul style="list-style-type: none"> Profile name: wlan-security Security policy: WPA2 <ul style="list-style-type: none"> Authentication mode: Dot1x Encryption mode: AES
VAP profile	<ul style="list-style-type: none"> Profile name: wlan-guest-vap Forwarding mode: tunnel forwarding Service VLAN: VLAN 10 SSID profile: profile named wlan-guest Security profile: profile named wlan-guest-security Authentication profile: Use the profile delivered by iMaster NCE-Campus. You need to check the profile name on iMaster NCE-Campus.

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100413634&id=EN-US_TOPIC_0298429464

Networking Scenario

An enterprise campus network connects to the Internet as shown in the following figure. On the enterprise campus network, the AP is connected to a switch and functions as a wireless access point, the firewall functions as the egress gateway, and employee accounts are saved on the AD server. To improve network security, employees are required to complete 802.1X authentication using their terminals, and are allowed to access the wireless network after passing authentication.



Size: 572.13MB

Enter keywords 0 / 256 Advanced Search

High-Quality 10 Gbps CloudCampus Solution & iMaster NCE-Campus Product Documentation (Euler&Kylin) > NCE Typical Configuration Examples > Examples for Configuring Access Authentication (NETCONF-based Device Management, VLAN Networking)

Connect with Author 2886 / 12981

Contents

- Configuring Portal Authentication for Wireless Users (Standalone WAC, Third-party Server)
- Configuring Portal Authentication for Wired Users (Username and Password Authentication)
- Configuring Portal Authentication for Wired Users (Username and Password Authentication)
- Configuring Portal Authentication for Wired Users (Authentication Component)
- Configuring 802.1X Authentication for Wireless Users (Native WAC, Using AD Accounts)**
- Configuring 802.1X Authentication for Wireless Users in Boarding Mode (Native WAC, Standalone WAC)
- Configuring 802.1X Authentication for Wireless Users in Boarding Mode (Native WAC, Standalone WAC)
- Configuring 802.1X Authentication (Native WAC, Interconnection with a Third-Party Server)
- Configuring 802.1X Authentication for Wireless Users (Cloud Managed Standalone WAC)
- Configuring 802.1X Authentication for Wireless Users (Cloud Managed Standalone WAC)
- Configuring 802.1X Authentication for Wired Users (Using AD Accounts)
- Configuring 802.1X Authentication for Wired Users (with Multiple Authentication Components)
- Configuring 802.1X Certificate-based EAP-TLS Authentication (Native WAC, Built-in CA Server)
- Configuring Certificate-based 802.1X Authentication Using EAP-TLS (Native WAC, External CA Server)
- Configuring Host Name-based Certificate Authentication and User Name-based Certificate Authentication
- Configuring Automatic MAC Address Authentication for Wireless Users Through Terminal
- Configuring MAC Address Authentication for Wireless Users (Cloud Managed Standalone WAC)
- Configuring MAC Address Authentication for Wired Users (Using MAC Accounts)

Data Plan

Table 1 User access data plan

Parameter	Value	Description
User group	ADUsers	This user group stores accounts synchronized from the AD server to iMaster NCE-Campus.
SSID	wlan-guest	-
ACL	3001	This ACL is used for user authorization.
RADIUS server template	iMaster_RADIUS	The built-in RADIUS server needs to be specified in the RADIUS server template.

Table 2 AD server data plan

Parameter	Value	Description
Name	DemoAD	-
Primary server address	xx.xx.xx.xx	Set this parameter based on the actual situation.
Authentication port	389	By default, this port is used when TLS is disabled.
AD domain name	global.campus.net	-
Base DN	DC=global,DC=campus,DC=net	-
Synchronization account	CN=Administrator,CN=Users,DC=global,DC=campus,DC=net	Account for connecting to the AD server.

Conforme demonstrado, é possível configurar em cada SSID uma forma diferente de autenticação, inclusive via Radius.

Diante do exposto, fica comprovado o atendimento ao item 3.5.6. do Anexo I – Especificação Técnica.

4.25) Do suposto não atendimento ao subitem 3.6.2 do Anexo I – Especificação Técnica

Aduz a Recorrente **TELESUL** que a Recorrida **3CORP**, apontou três links que exigem login com usuário na página de suporte da Huawei, tornando a verificação impossível para a Comissão de Licitação, o que prejudica a avaliação de cumprimento do subitem abaixo.

- 3.6.2. Deve possibilitar o upload de plantas baixas e dispor de ferramenta de simulação de visualização do sinal Wi-Fi com sobreposição de dados como canais, interferência e movimentação de usuários, mapa de calor;

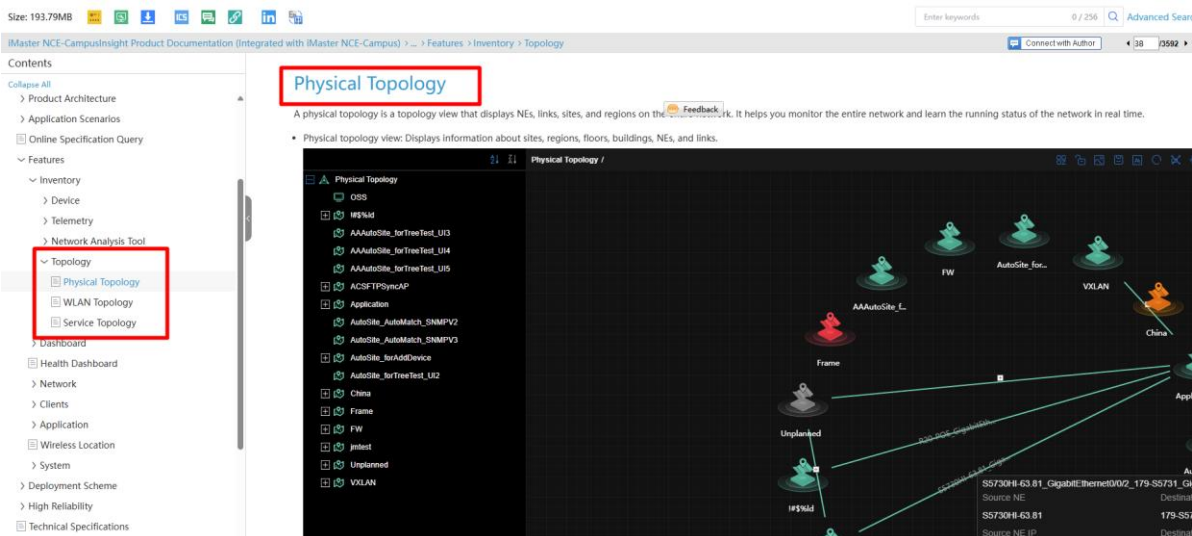
No entanto, esclarecemos que, o link disponibilizado para validação das informações técnicas apresentadas pode sofrer alterações ao longo do tempo, em função de atualizações periódicas realizadas na base de dados e no portal oficial do fabricante. Especificamente, no intervalo compreendido entre a data de envio das comprovações técnicas e a data de acesso/leitura por parte da Comissão de Licitação, houve atualização da base documental da Huawei, o que pode ter impactado a estrutura, disponibilidade ou localização dos conteúdos originalmente referenciados.

Ressaltamos que tais alterações são inerentes à política de manutenção e evolução contínua dos repositórios digitais do fabricante, não implicando em qualquer modificação das características técnicas dos produtos ou soluções ofertadas. Dessa forma, eventuais divergências de acesso aos links previamente informados não comprometem a veracidade das informações apresentadas, podendo, quando necessário, ser fornecidas versões atualizadas ou caminhos alternativos para consulta às documentações oficiais correspondentes.

Abaixo novos links para validação das informações de comprovação de atendimento ao item 3.6.2.

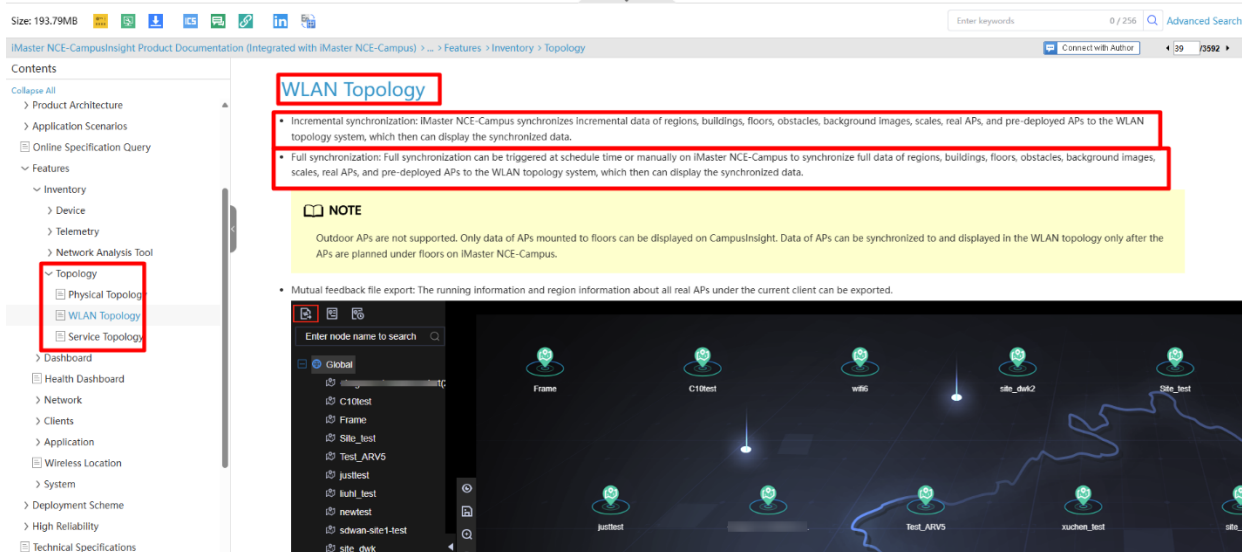
Physical Topology

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100405834&id=EN-US_TOPIC_0000001568226077



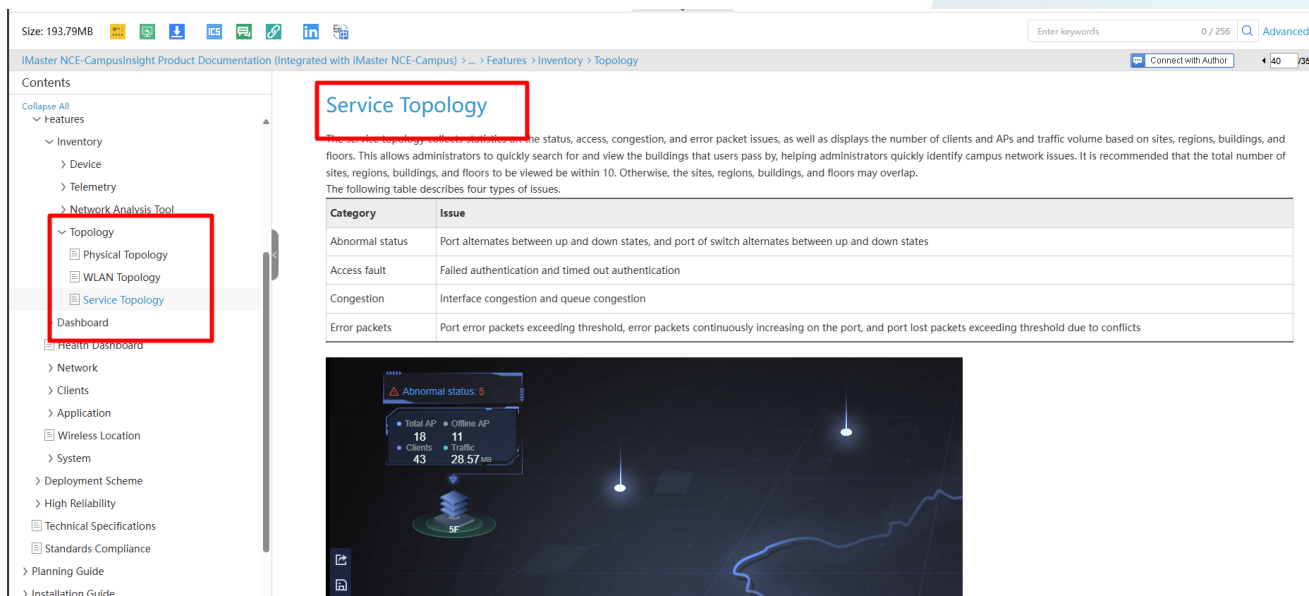
WLAN Topology

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100405834&id=EN-US_TOPIC_0199779722



Service Topology

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100405834&id=EN-US_TOPIC_0262960106



Category	Issue
Abnormal status	Port alternates between up and down states, and port of switch alternates between up and down states
Access fault	Failed authentication and timed out authentication
Congestion	Interface congestion and queue congestion
Error packets	Port error packets exceeding threshold, error packets continuously increasing on the port, and port lost packets exceeding threshold due to conflicts

Diante do exposto, fica comprovado o atendimento ao item 3.6.2. do Anexo I – Especificação Técnica.

4.26) Do suposto não atendimento ao subitem 3.6.4.3 do Anexo I – Especificação Técnica

Aduz a Recorrente **TELESUL** que a Recorrida **3CORP**, apontou um link que exige login com usuário na página de suporte da Huawei, tornando a verificação impossível para a Comissão de Licitação, o que prejudica a avaliação de cumprimento do subitem abaixo.

3.6.4.3. Lista de pontos de acesso do tipo rogue; Deve permitir autenticar e enviar perfis dos APs

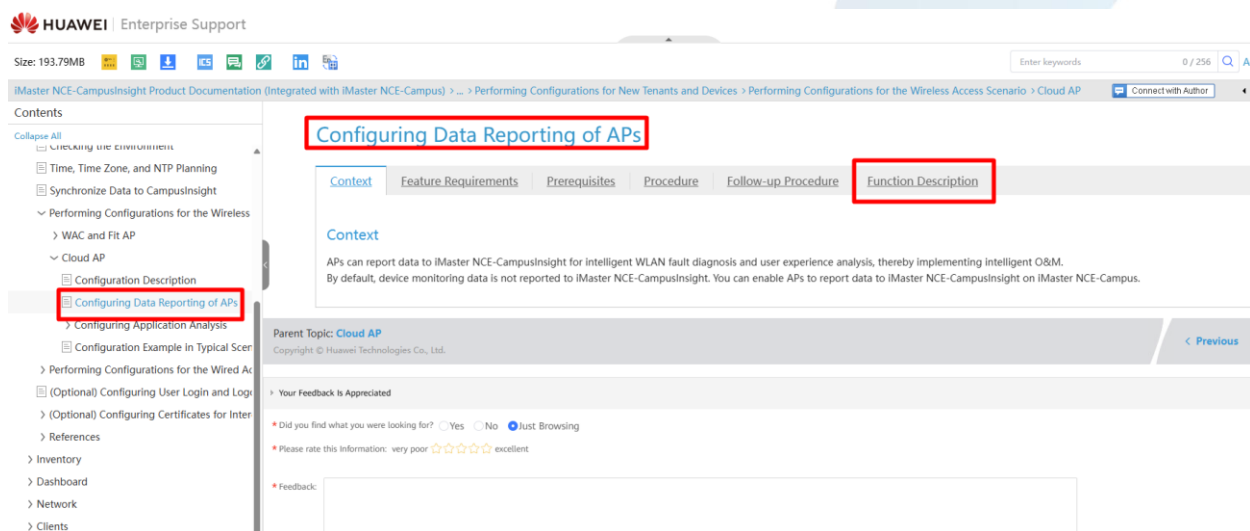
No entanto, esclarecemos que, o link disponibilizado para validação das informações técnicas apresentadas pode sofrer alterações ao longo do tempo, em função de atualizações periódicas realizadas na base de dados e no portal oficial do fabricante. Especificamente, no intervalo compreendido entre a data de envio das comprovações técnicas e a data de acesso/leitura por parte da Comissão de Licitação, houve atualização da base documental da Huawei, o que pode ter impactado a estrutura, disponibilidade ou localização dos conteúdos originalmente referenciados.

Ressaltamos que tais alterações são inerentes à política de manutenção e evolução contínua dos repositórios digitais do fabricante, não implicando em qualquer modificação das características técnicas dos produtos ou soluções ofertadas. Dessa forma, eventuais divergências de acesso aos links previamente informados não comprometem a veracidade das informações apresentadas, podendo, quando necessário, ser fornecidas versões atualizadas ou caminhos alternativos para consulta às documentações oficiais correspondentes.

Abaixo novo link para validação das informações de comprovação de atendimento ao item 3.6.4.3.

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100405834&id=EN-US_TOPIC_0000001237134206

Ao abrir o link, clicar em Function Description, localizar "rogue":



HUAWEI | Enterprise Support

Size: 193.79MB

Enter keywords 0 / 256 Advanced

iMaster NCE-CampusInsight Product Documentation (Integrated with iMaster NCE-Campus) > ... > Performing Configurations for New Tenants and Devices > Performing Configurations for the Wireless Access Scenario > Cloud AP

Contents

- Collapse All
- Checking the Environment
 - Time, Time Zone, and NTP Planning
 - Synchronize Data to CampusInsight
- Performing Configurations for the Wireless
 - WAC and Fit AP
 - Cloud AP
 - Configuration Description
 - Configuring Data Reporting of APs**
 - Configuring Application Analysis
 - Configuration Example in Typical Scenario
- Performing Configurations for the Wired Access
 - (Optional) Configuring User Login and Logout
 - (Optional) Configuring Certificates for Interference
- References
- Inventory
- Dashboard
- Network
- Clients
- Application
- Wireless Location

Configuring Data Reporting of APs

Context Feature Requirements Prerequisites Procedure Follow-up Procedure **Function Description**

Function Description

Table 2 Function description

Function	Collection Item	Minimum Collection Precision
Report performance data	Device/Card <ul style="list-style-type: none"> CPU usage Memory usage Rated power, real-time power, and average power (wireless device) <p>NOTE: iMaster NCE-Campus can deliver the power consumption data configuration to V200 APs and APs running V600R023C00 and later versions so that the APs can report performance data such as real-time power, average power, and rated power to iMaster NCE-CampusInsight.</p>	1 minute
	Radio <ul style="list-style-type: none"> Radio information, including the radio ID, radio MAC address, device status, frequency band, noise, channel utilization, interference rate, and transmit power. Number of access clients 	1 minute

Size: 193.79MB

Enter keywords 0 / 256 Advanced

iMaster NCE-CampusInsight Product Documentation (Integrated with iMaster NCE-Campus) > ... > Performing Configurations for New Tenants and Devices > Performing Configurations for the Wireless Access Scenario > Cloud AP

Contents

- Collapse All
- Checking the Environment
 - Time, Time Zone, and NTP Planning
 - Synchronize Data to CampusInsight
- Performing Configurations for the Wireless
 - WAC and Fit AP
 - Cloud AP
 - Configuration Description
 - Configuring Data Reporting of APs**
 - Configuring Application Analysis
 - Configuration Example in Typical Scenario
- Performing Configurations for the Wired Access
 - (Optional) Configuring User Login and Logout
 - (Optional) Configuring Certificates for Interference
- References
- Inventory
- Dashboard
- Network
- Clients
- Application
- Wireless Location
- System Management
- Maintenance Guide
- Troubleshooting

Configuring Data Reporting of APs

Function Collection Item Minimum Collection Precision

Report WIDS data	WIDS data <p>After the function is enabled, choose Network Configuration > Site Configuration > Site Configuration from the main menu, click the Traditional View tab, and configure the data items to be reported on the WLAN Security tab page under AP > Security.</p> <ul style="list-style-type: none"> Security check: <ul style="list-style-type: none"> Detection of brute force key cracking attacks Spoofing attack detection Rogue device detection Flood attack detection Weak IV detection Security protection: <ul style="list-style-type: none"> Defense using dynamic blacklist Manual device containment Countermeasure against rogue APs Countermeasure against ad-hoc devices Open device countermeasure Terminal protection 	1 minute
Information about rogue Wi-Fi devices	<ul style="list-style-type: none"> MAC addresses of rogue devices BSSIDs of rogue devices SSIDs of rogue devices Rogue device type First occurrence time Detection field strength Detection channel 	1 minute

Diante do exposto, fica comprovado o atendimento ao item 3.6.4.3. do Anexo I – Especificação Técnica.

4.27) Do suposto não atendimento ao subitem 4.1.1.1. do Anexo I – Especificação Técnica

Aduz a Recorrente **TELESUL** que a Recorrida **3CORP**, apontou um link que não comprova a compatibilidade com hypervisors e Clouds, limitando a integração da solução em ambientes virtualizados e de nuvem, não sendo possível atestar o cumprimento do subitem abaixo.

- 4.1.1. A solução ofertada deverá fazer parte do catálogo de produtos comercializados pelo fabricante e não constar como End-of-Support, End-of-Sales ou End-of-Life até a data de entrega da proposta. A comprovação se dará por meio de documentação oficial constante de site público da fabricante ou de declaração emitida pelo fabricante, não sendo aceita solução em roadmap;

No entanto, esclarecemos que, foi enviado durante o processo em epígrafe documentos de comprovação de que os produtos ofertados estão em linha de produção, ou seja, não constam em listas de End-of-Support, End-of-Sales ou End-of-Life.

Os documentos enviados foram:

iMaster NCE-CloudCampus_EOM_EOS.pdf

iMaster NCE-CloudCampusInsight_EOM_EOS.pdf

iMaster NCE-CloudCampus

Product EOM Time (New Site): 2028-12-31

Product EOM Time: 2028-12-31

Product EOS Time:2033-12-31

iMaster NCE-CloudCampusInsight

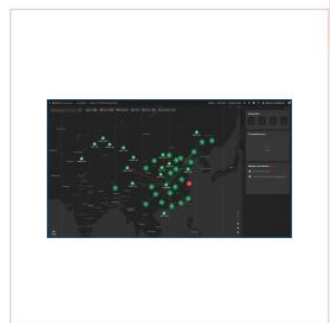
Product EOM Time (New Site): 2028-12-31

Product EOM Time: 2035-12-31

Product EOS Time:2033-12-31

Abaixo imagens dos arquivos enviados com as comprovações solicitadas:

Product Details



iMaster NCE-Campus

iMaster NCE-Campus — Huawei's next-generation autonomous driving network management and control system for campus networks — integrates management, control, analysis, and Artificial Intelligence (AI) functions, providing full-lifecycle automation of campus networks. Intelligent fault closure is also implemented through network digital maps, big data analytics and AI. Helping enterprises reduce both Operating Expenditure (OPEX) and Operations and Maintenance (O&M) costs, iMaster NCE-Campus accelerates enterprise cloudification and digital transformation by achieving automated and intelligent network management.

[For more information, visit the official website. >>](#)

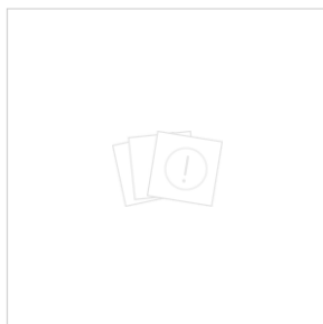
NEW [Bidding Document Finder >>](#)

Product EOM Time (New Site): 2028-12-31

Product EOM Time: 2028-12-31

Product EOS Time: 2033-12-31

Product Details



iMaster NCE-CampusInsight

The iMaster NCE-CampusInsight uses the Telemetry technology to dynamically capture fault data in seconds, perceiving the full-journey experience for each user. It proactively identifies four types of wireless network problems, helping administrators quickly demarcate faults and eliminate risks.

[For more information, visit the official website. >>](#)

NEW [Bidding Document Finder >>](#)

Product EOM Time (New Site): 2028-12-31

Product EOM Time: 2035-12-31

Product EOS Time: 2033-12-31

[Add to Cart](#)

[Configure](#)

Os documentos enviados declaram que a Plataforma atende ao especificado no item 4.1.1. e de acordo com a forma que foi solicitada.

Diante do exposto, fica comprovado o atendimento ao item 4.1. do Anexo I – Especificação Técnica.

4.28) Do suposto não atendimento ao subitem 4.1.5. do Anexo I – Especificação Técnica

Aduz a Recorrente **TELESUL** que a Recorrida **3CORP**, não comprovou o atendimento de integração com GOV.BR. apresentou apenas OIDC baseado em OAuth 2.0, que não atende a todos os requerimentos específicos da integração com GOV.BR. sendo necessário também comprovar que fará validação de CPF (item fundamental no processo de autenticação do GOV.BR) e o redirecionamento da identidade do usuário para o portal do governo, assim alega que padece de comprovação o subitem abaixo.

4.1.5. Deve ser compatível com o serviço de autenticação do GOV.BR;

No entanto, esclarecemos que, a evidência enviada atende o item 4.1.5., onde foi apontada a utilização do protocolo OAUTH, por meio do documento iMaster NCE-Campus Product Brochure.pdf, página 7.

PowerPoint 演示文稿 7 / 8 140%

Key feature	Value
User access authentication	<ul style="list-style-type: none"> Supports the new authentication protocol HTTP/2, centrally manages a vast number of devices, authenticates users' network access. Provides multiple user authentication modes, such as 802.1X, Portal, SMS, and social media authentication, flexibly meeting user policy control requirements. Decouples users from IP addresses, allowing users to access the network anytime, anywhere with consistent permissions. This enables free mobility and consistent user experience, as well as ensures better user experience while meeting permission control requirements. Supports HWTACACS authentication and authorization for device administrators upon device logins. Supports 5G terminal access authentication capabilities, ensuring that 5G terminals can access enterprises' campus networks in a secure and reliable mode. Supports OIDC based on OAuth 2.0.
Intelligent terminal management	<ul style="list-style-type: none"> Provides built-in terminal fingerprint databases to accurately identify terminal types through multiple methods such as intelligent identification. Supports intelligent access of a vast number of IoT terminals, automatically matches and delivers policies, achieving plug-and-play of IoT terminals. Supports fast access of IoT terminals on the IoT sensing network, improving access security of IoT terminals. Supports AI clustering identification for unknown terminals. Unknown terminals with similar fingerprints are clustered into one group. After an administrator marks their terminal type, subsequent terminals of this type can be automatically identified.

O **Huawei iMaster NCE-CloudCampus** é uma plataforma de gerenciamento e orquestração de redes baseada em nuvem que suporta integração com provedores externos de identidade (IdP) por meio de padrões abertos de autenticação e autorização, como o protocolo **OAuth 2.0**.

Nesse contexto, é tecnicamente viável a integração com o serviço de autenticação do **gov.br**, que disponibiliza mecanismos de federação de identidade baseados em OAuth 2.0 e **OpenID Connect**.

Funcionamento da Integração

A integração ocorre com base no modelo de **delegação de autenticação**, no qual:

- O NCE-CloudCampus atua como **cliente OAuth (Relying Party)**;

- O GOV.BR atua como **provedor de identidade (IdP)**;
- O processo de autenticação é redirecionado para o ambiente seguro do GOV.BR;
- Após a autenticação do usuário, o GOV.BR retorna ao NCE-CloudCampus um **token de acesso (access token)** e, opcionalmente, um **ID token**, contendo as credenciais e atributos do usuário autenticado.

Fluxo Técnico Simplificado

1. O usuário tenta acessar o portal/captive portal gerenciado pelo NCE-CloudCampus;
2. A plataforma redireciona o usuário para o endpoint de autorização do GOV.BR;
3. O usuário realiza autenticação utilizando suas credenciais oficiais;
4. O GOV.BR valida a identidade e retorna um **authorization code**;
5. O NCE-CloudCampus troca o código por um **access token** via backend seguro;
6. O token é validado e utilizado para autorizar o acesso do usuário à rede.

Benefícios da Integração

- **Autenticação centralizada e confiável**, baseada na identidade digital oficial do governo brasileiro;
- **Melhoria na experiência do usuário**, eliminando a necessidade de credenciais locais;
- **Aumento do nível de segurança**, com suporte a autenticação multifator (MFA) do GOV.BR;
- **Aderência a padrões abertos**, garantindo interoperabilidade e escalabilidade da solução;
- **Facilidade de auditoria e conformidade**, especialmente em ambientes públicos e regulados.

Abaixo evidência de configuração de usuário para implementação da autenticação:

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100516678&id=EN-US_TOPIC_0306208405

Size: 621.61MB

High-Quality 10 Gbps CloudCampus Solution & iMaster NCE-Campus Product Documentation

System > System Management > Third-Party Service > RESTful Settings

Contents

- System > User Management > User Management
- Resource Center > MSP Management
- System > System Management > Third-Party Service
 - System > System Management > Third-Party Service > Email Server
 - System > System Management > Third-Party Service > SMS Server
 - System > System Management > Third-Party Service > SMS Platform
 - System > System Management > Third-Party Service > AD Domain Conf
 - System > System Management > Third-Party Service > Map URL Settings
 - System > System Management > Third-Party Service > Registration Cent
 - System > System Management > Third-Party Service > Syslog Configur
 - System > System Management > Third-Party Service > RESTful Settings
 - System > System Management > Third-Party Service > Signature Databa
 - System > System Management > Third-Party Service > File Server
 - System > System Management > Third-Party Service > Manage Notified
 - System > System Management > Third-Party Service > Kafka
 - System > System Management > Third-Party Service > Huawei Online Up
 - System > System Management > Third-Party Service > WLAN Planner
 - System > System Management > Third-Party Service > Third-Party App S
- Analysis > CampusInsight
- System > System Management > System Information
- System > Log Management > Logs > Log Overflow Dump
- System > Southbound Access > Southbound Access Configuration

Table 1 RESTful settings

Parameter	Parameters
General Settings	Timeout interval (s) Value range: 1 to 60
	Retry times Value range: 0 to 10
	Inform interval (ms) Value range: 0 to 60000
	Heartbeat timeout (min) Value range: 1 to 30
	System ID ID of the source which sends heartbeat packets. It is used together with the system name to uniquely identify a source.
	System name Name of the source which sends heartbeat packets. It is used together with the system ID to uniquely identify a source.
	Enable HTTP If Enable HTTP is set to Yes , HTTP and HTTPS can be used. Otherwise, only HTTPS can be used. NOTE: HTTPS is recommended because it is more secure than HTTP.
Third-Party Server Settings	Channel ID ID of the target channel used by iMaster NCE-Campus to report data, which is user-defined.
	Authentication mode The options include Token and Certificate .
	Server IP address IP address of the third-party management server.
	Port number Port number used for communication between the third-party management system and iMaster NCE-Campus.
	Username Username and password created in the third-party management system for logging in to iMaster NCE-Campus.
	Password

Diante do exposto, fica comprovado o atendimento ao item 4.1.5. do Anexo I – Especificação Técnica.

4.29) Do suposto não atendimento aos subitens 4.1.5.1. e 4.1.5.2. do Anexo I – Especificação Técnica

Aduz a Recorrente **TELESUL** que a Recorrida **3CORP**, não disponibilizou informação, deixando lacunas críticas na compreensão da solução, alegando que padece de comprovação do subitem abaixo.

- 4.1.5.1. São de responsabilidade do CONTRATADA as customizações necessárias para a integração com o serviço de autenticação do GOV.BR;
- 4.1.5.2. Pode ser fornecido componente adicional para possibilitar a integração com o GOV.BR;

No entanto, esclarecemos que, cumpre esclarecer que os itens **4.1.5.1** e **4.1.5.2** não se configuram como requisitos técnicos intrínsecos aos equipamentos ou à solução base ofertada, tampouco demandam comprovação por meio de datasheets, manuais ou certificações de fabricante.

Os referidos itens tratam, na realidade, de **obrigações de natureza operacional e de responsabilidade da CONTRATADA**, no contexto da implementação da solução, conforme detalhado a seguir:

- **Item 4.1.5.1:** estabelece que eventuais customizações necessárias para viabilizar a integração com o serviço de autenticação GOV.BR são de responsabilidade da CONTRATADA. Trata-se, portanto, de atividade de **serviços profissionais**, envolvendo configuração, desenvolvimento de integrações (por exemplo, via protocolos como OAuth 2.0/OpenID Connect) e adequações de ambiente, não sendo característica nativa obrigatória e previamente embarcada na solução.
- **Item 4.1.5.2:** prevê explicitamente a possibilidade de fornecimento de **componente adicional** para viabilizar tal integração. Este dispositivo reforça o entendimento de que a integração com o GOV.BR pode ser implementada por meio de elementos complementares (middleware, gateways de identidade, proxies de autenticação, entre outros), afastando a obrigatoriedade de suporte nativo direto pela solução principal.

Dessa forma, resta claro que:

1. **Não se trata de requisito técnico de produto**, mas sim de **escopo de implementação**;
2. **Não há exigência de comprovação técnica prévia**, uma vez que a responsabilidade recai sobre a CONTRATADA no momento da execução contratual;
3. O edital foi devidamente estruturado para permitir **flexibilidade arquitetural**, inclusive com o uso de componentes adicionais, garantindo ampla competitividade e aderência às melhores práticas de integração com serviços de identidade federada.

Portanto, não procede a interpretação de que tais itens demandariam comprovação técnica em fase de habilitação ou proposta, devendo ser compreendidos como **obrigações contratuais de entrega da solução plenamente integrada**.

Diante do exposto, fica comprovado o atendimento aos itens 4.1.5.1. e 4.1.5.2. do Anexo I – Especificação Técnica.

4.30) Do suposto não atendimento ao subitem 4.1.11. do Anexo I – Especificação Técnica

Aduz a Recorrente **TELESUL** que a Recorrida **3CORP**, não disponibilizou informação, deixando lacunas críticas na compreensão da solução, alegando que padece de comprovação do subitem abaixo.

4.1.11. Deve suportar mecanismo de alta disponibilidade para as funções de administração e monitoração;

No entanto, esclarecemos que, a plataforma Huawei NCE-CloudCampus, quando utilizada na modalidade em nuvem, é projetada com arquitetura distribuída e resiliente, garantindo mecanismos robustos de **redundância e alta disponibilidade (HA – High Availability)**.

Nesse modelo, os serviços de gerenciamento são hospedados em infraestrutura de data centers geograficamente distribuídos, com **replicação de dados em múltiplas zonas de disponibilidade (AZs)**. Isso assegura que, em caso de falha de um nó, instância ou até mesmo de um data center completo, as demais instâncias assumam automaticamente a operação, sem interrupção perceptível dos serviços.

A solução utiliza conceitos como:

- **Clusterização de serviços:** múltiplas instâncias ativas do sistema operando em paralelo (active-active), eliminando pontos únicos de falha;
- **Balanceamento de carga dinâmico:** distribuição automática das requisições entre os nós disponíveis, garantindo desempenho e continuidade;
- **Failover automático:** comutação transparente em caso de falhas, mantendo a operação da rede gerenciada;
- **Sincronização contínua de banco de dados:** replicação em tempo real das informações de configuração, autenticação e telemetria.

Adicionalmente, os dispositivos de rede, como pontos de acesso e switches gerenciados, mantêm suas configurações operacionais localmente, permitindo que continuem funcionando normalmente mesmo em cenários de perda temporária de conectividade com a nuvem, reforçando a **resiliência da solução como um todo**.

Dessa forma, a arquitetura em nuvem da plataforma atende plenamente aos requisitos de **alta disponibilidade, continuidade operacional e tolerância a falhas**, sendo adequada para ambientes corporativos críticos que demandam elevada confiabilidade.

Vale ressaltar que a plataforma proposta está hospedada na Huawei Cloud, plataforma de computação em nuvem pública da Huawei, projetada para fornecer recursos de TI sob demanda por meio da internet, seguindo os princípios de **cloud computing** como elasticidade, escalabilidade e pagamento conforme o uso (*pay-as-you-go*).

Do ponto de vista técnico, o Huawei Cloud oferece um conjunto abrangente de serviços estruturados em camadas, incluindo:

1. Infraestrutura como Serviço (IaaS)

Disponibiliza recursos básicos de computação, como máquinas virtuais (ECS – Elastic Cloud Server), redes virtuais (VPC – Virtual Private Cloud) e armazenamento (OBS – Object Storage Service). Esses recursos são provisionados dinamicamente, permitindo rápida alocação e ajuste conforme a demanda da aplicação.

2. Plataforma como Serviço (PaaS)

Fornece ambientes gerenciados para desenvolvimento, teste e execução de aplicações, incluindo bancos de dados (RDS), containers (CCE – Cloud Container Engine) e serviços de middleware. Essa camada abstrai a complexidade da infraestrutura subjacente, permitindo maior foco no desenvolvimento de software.

3. Software como Serviço (SaaS)

Oferece aplicações prontas hospedadas na nuvem, acessíveis via navegador ou APIs, eliminando a necessidade de instalação local.

Arquitetura e características técnicas relevantes:

- **Alta disponibilidade e redundância:**
A plataforma é baseada em múltiplas zonas de disponibilidade (*Availability Zones – AZs*), com replicação de dados e balanceamento de carga, garantindo continuidade dos serviços mesmo em caso de falhas.
- **Escalabilidade elástica:**
Recursos computacionais podem ser automaticamente expandidos ou reduzidos conforme a carga, suportando variações dinâmicas de tráfego.
- **Segurança integrada:**
Inclui mecanismos como controle de identidade e acesso (IAM), criptografia de dados em repouso e em trânsito, além de conformidade com padrões internacionais de segurança.
- **Virtualização e isolamento:**
Utiliza tecnologias avançadas de virtualização para garantir isolamento entre tenants, permitindo ambientes multiusuário com segurança e desempenho.
- **Automação e orquestração:**
APIs e ferramentas de automação permitem provisionamento rápido de infraestrutura (Infraestrutura como Código – IaC), integração com pipelines DevOps e gerenciamento centralizado.

- **Integração com soluções corporativas Huawei:**

O Huawei Cloud integra-se a soluções como o Huawei CloudCampus, possibilitando gerenciamento centralizado de redes, dispositivos e políticas, especialmente em cenários de campus corporativo e redes definidas por software (SDN).

Atualmente Huawei Cloud Brasil está distribuído em 03 (três) locais distintos, conforme link e imagem abaixo:

https://support.huaweicloud.com/intl/pt-br/productdesc-dc/dc_01_0004.html#:~:text=A%20Direct%20Connect%20fornece%20uma%20s%C3%A9rie%20de,acesso%20%C3%A0%20Huawei%20Cloud%20em%20uma%20regi%C3%A3o.

América latina	México	LA-Mexico City1	Johannesburg-Ieraco	Ieraco
			Mexico City1-COM Ixtlahuaca	COM Ixtlahuaca
		LA-Mexico City2	Mexico-KIO MEX 5	KIO MEX 5
			Mexico-Tultitlan	Data center neutro para operadora
	Brasil (São Paulo)	LA-Sao Paulo1	Sao Paulo-Telefonica	Telefonica
			Sao Paulo-Equinix	Equinix
			Sao Paulo-ODATA	OData
	Santiago	LA-Santiago	Santiago-Paine	Paine
			Santiago-Claro	Claro

Diante do exposto, comprova-se o atendimento ao item 4.1.11. do Anexo I – Especificação Técnica.

4.31) Do suposto não atendimento ao subitem 4.5.11. do Anexo I – Especificação Técnica

Aduz a Recorrente **TELESUL** que é exigido que o autenticador realize a validação do formato dos campos como CPF, e-mail e telefone, e ainda, que a licitante **3CORP** em sua resposta não apresentou a comprovação de validador de campos, em especial do CPF, um requisito de segurança e conformidade para dados pessoais, incluindo atendimento do LGPD e marco civil da internet, conforme exigido no subitem abaixo.

- 4.5.11. Deve permitir a validação de campos como:
- 4.5.11.1. Conferir se o CPF digitado é um número válido;
 - 4.5.11.2. Conferir se o e-mail está no formato adequado;
 - 4.5.11.3. Conferir se o telefone está no formato adequado;

No entanto, esclarecemos que, no contexto do **iMaster NCE-CloudCampus**, o processo de autenticação de usuários do tipo *guest* é flexível e orientado a políticas, permitindo que diferentes atributos de identificação sejam utilizados como credencial de acesso à rede.

Nesse modelo, o campo “usuário” (**username**) do portal de autenticação pode ser configurado para receber informações como **CPF, endereço de e-mail, número de telefone ou qualquer outro identificador definido pela política da organização**. Dessa forma, o valor inserido nesse campo passa a representar o identificador único do usuário convidado no sistema.

Durante o fluxo de cadastro e/ou autenticação, a plataforma realiza a validação das informações fornecidas com base nas regras previamente configuradas, que podem incluir:

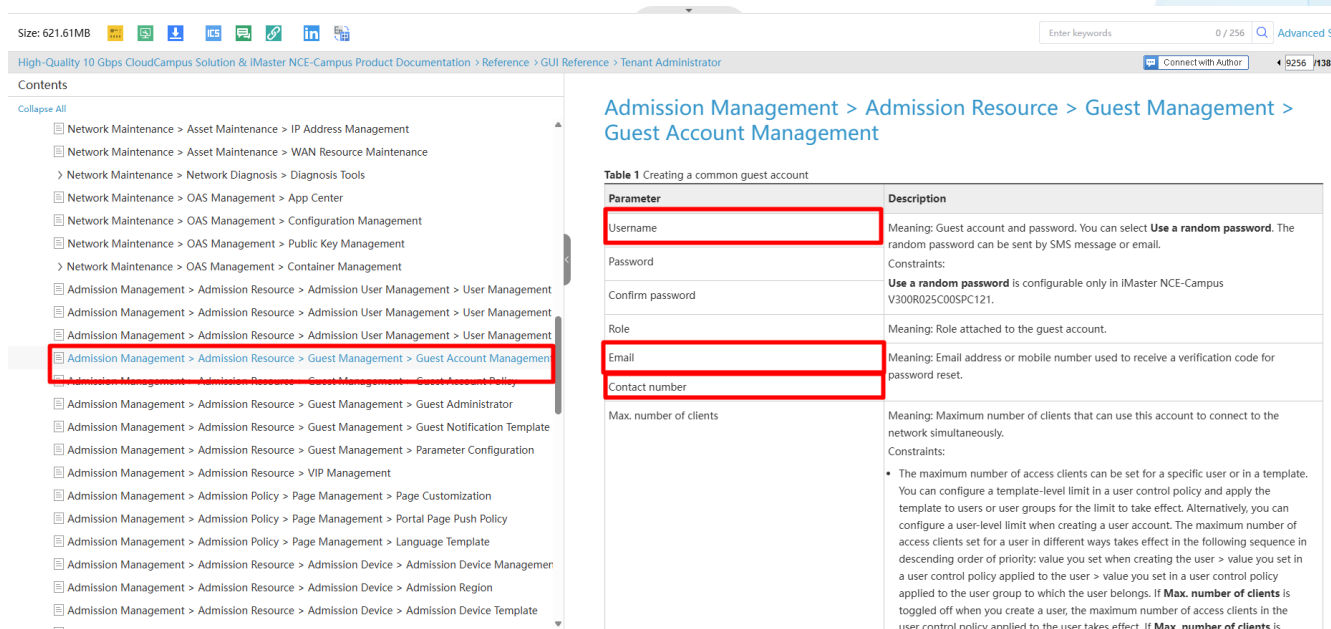
- Verificação de formato (por exemplo, estrutura válida de CPF, e-mail ou telefone);
- Aplicação de políticas de unicidade e consistência dos dados;
- Integração com bases externas ou sistemas de terceiros para validação adicional, quando aplicável;
- Associação do identificador a mecanismos de autenticação complementar, como envio de código via SMS ou e-mail.

Dessa forma, a validação de dados como CPF, e-mail, telefone ou outros atributos ocorre de maneira indireta, por meio da utilização dessas informações no campo de usuário, aliada às políticas de autenticação implementadas na solução.

Essa abordagem garante maior flexibilidade operacional, permitindo que a identificação e o controle de acesso de usuários *guest* sejam adaptados às necessidades específicas da organização, mantendo rastreabilidade, segurança e aderência a requisitos regulatórios, sem a obrigatoriedade de campos dedicados para cada tipo de informação.

Abaixo link com as evidências dos campos configuráveis no cadastro da conta:

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100516678&id=EN-US_TOPIC_0159771045



Size: 621.61MB

High-Quality 10 Gbps CloudCampus Solution & iMaster NCE-Campus Product Documentation > Reference > GUI Reference > Tenant Administrator

Contents

- Network Maintenance > Asset Maintenance > IP Address Management
- Network Maintenance > Asset Maintenance > WAN Resource Maintenance
- Network Maintenance > Network Diagnosis > Diagnosis Tools
- Network Maintenance > OAS Management > App Center
- Network Maintenance > OAS Management > Configuration Management
- Network Maintenance > OAS Management > Public Key Management
- Network Maintenance > OAS Management > Container Management
- Admission Management > Admission Resource > Admission User Management > User Management
- Admission Management > Admission Resource > Admission User Management > User Management
- Admission Management > Admission Resource > Admission User Management > User Management
- Admission Management > Admission Resource > Guest Management > Guest Account Management**
- Admission Management > Admission Resource > Guest Management > Guest Account Policy
- Admission Management > Admission Resource > Guest Management > Guest Administrator
- Admission Management > Admission Resource > Guest Management > Guest Notification Template
- Admission Management > Admission Resource > Guest Management > Parameter Configuration
- Admission Management > Admission Resource > VIP Management
- Admission Management > Admission Policy > Page Management > Page Customization
- Admission Management > Admission Policy > Page Management > Portal Page Push Policy
- Admission Management > Admission Policy > Page Management > Language Template
- Admission Management > Admission Resource > Admission Device > Admission Device Manager
- Admission Management > Admission Resource > Admission Device > Admission Region
- Admission Management > Admission Resource > Admission Device > Admission Device Template

Admission Management > Admission Resource > Guest Management > Guest Account Management

Table 1 Creating a common guest account

Parameter	Description
Username	Meaning: Guest account and password. You can select Use a random password . The random password can be sent by SMS message or email.
Password	Constraints:
Confirm password	Use a random password is configurable only in iMaster NCE-Campus V300R025C00SPC121.
Role	Meaning: Role attached to the guest account.
Email	Meaning: Email address or mobile number used to receive a verification code for password reset.
Contact number	
Max. number of clients	Meaning: Maximum number of clients that can use this account to connect to the network simultaneously. Constraints: <ul style="list-style-type: none"> The maximum number of access clients can be set for a specific user or in a template. You can configure a template-level limit in a user control policy and apply the template to users or user groups for the limit to take effect. Alternatively, you can configure a user-level limit when creating a user account. The maximum number of access clients set for a user in different ways takes effect in the following sequence in descending order of priority: value you set when creating the user > value you set in a user control policy applied to the user > value you set in a user control policy applied to the user group to which the user belongs. If Max. number of clients is toggled off when you create a user, the maximum number of access clients in the user control policy applied to the user takes effect. If Max. number of clients is

Diante do exposto, comprova-se o atendimento aos itens 4.5.11.1., 4.5.11.2. e 4.5.11.3. do Anexo I – Especificação Técnica.

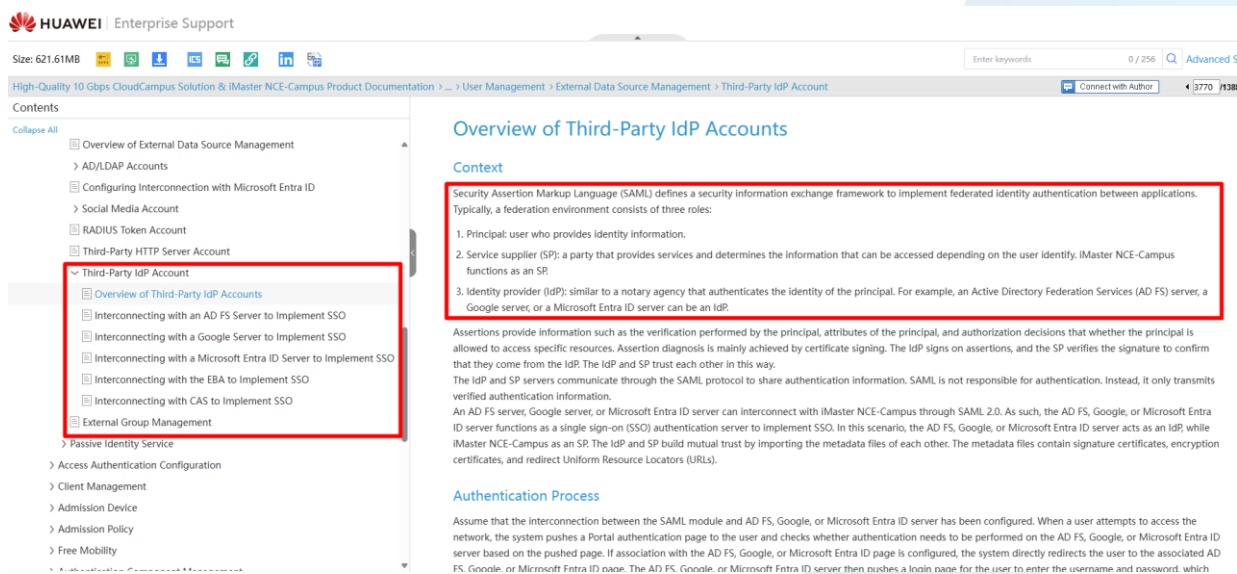
4.32) Do suposto não atendimento ao subitem 4.2.9. do Anexo I – Especificação Técnica

Aduz a Recorrente **TELESUL** que não existe comprovação técnica para este item, deixando uma lacuna completa na aderência a esta especificação, conforme exigido no subitem abaixo.

4.2.9. Deve possibilitar aplicar regras diferenciadas por grupos de usuários e máquinas, além das políticas definidas no Microsoft Active Directory;

No entanto, esclarecemos que, a Plataforma de Gerência ofertada atende ao descrito no item 4.2.9. conforme link e imagem abaixo:

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100516678&id=EN-US_TOPIC_0000002527508733



https://support.huawei.com/hedex/hdx.do?docid=EDOC1100516678&id=EN-US_TOPIC_0195851391

HUAWEI | Enterprise Support

Size: 621.61MB

High-Quality 10 Gbps CloudCampus Solution & iMaster NCE-Campus Product Documentation > ... > User Management > External Data Source Management > AD/LDAP Accounts

Contents

- ▼ User Management
 - Overview of User Management
 - > Local User Management
 - > Guest Management
 - > VIP Management
 - ▼ External Data Source Management
 - Overview of External Data Source Management
 - ▼ AD/LDAP Accounts
 - AD/LDAP Overview**
 - AD/LDAP Feature Requirements
 - AD/LDAP Synchronization Mode
 - (Optional) Adding the Controller to an AD Domain
 - (Optional) Importing an AD-LDAP Trust Certificate
 - Configuring Interconnection with an AD Server
 - Configuring Interconnection with an LDAP Server
 - Interconnecting with the Google LDAP Server
 - Configuring Interconnection with Microsoft Entra ID
 - > Social Media Account
 - RADIUS Token Account
 - Third-Party HTTP Server Account

AD/LDAP Overview

Context

iMaster NCE-Campus can synchronize user groups and users with an AD/LDAP server and supports multiple synchronization modes to adapt to diversified storage structures of different AD/LDAP servers.

Basic Concepts

Table 1 Basic concepts

Concept	Description
DC	Domain controller, which stores AD/LDAP data and identifies an AD/LDAP server. Generally, one AD/LDAP server is a domain controller.
DN	Distinguished name (DN), which identifies the location of an object on an AD/LDAP server. You can find the storage location of an object based on its DN. A DN includes the information about the object, its upper-layers, and the root node. In Figure 1 , the DN of the user Lucas is CN=Lucas,OU=Accounting Dept,OU=Company,OU=Mode1,DC=example,DC=huawei,DC=com .
Base DN	DN of the root node. For example, the base DN in Figure 1 is DC=example,DC=huawei,DC=com .
AD domain name	Identifier of an AD server. An LDAP server has no domain name. You can log in to an AD server and access Active Directory Users and Computers to view the AD domain name.
CN	Common name, which specifies the name of an object, such as a group or user. For example, in Figure 1 , CN=Lucas indicates that the user name is Lucas , and CN=VIP_Group indicates that the group name is VIP_Group .
OU	Organization unit (OU) that stores data in a tree structure. As a container, an OU can contain objects such as OUs, groups, and users. For example, in Figure 1 , the user Lucas belongs to the OU Accounting Dept .

HUAWEI | Enterprise Support

Size: 621.61MB

High-Quality 10 Gbps CloudCampus Solution & iMaster NCE-Campus Product Documentation > ... > User Management > External Data Source Management > AD/LDAP Accounts

Contents

- ▼ User Management
 - Overview of User Management
 - > Local User Management
 - > Guest Management
 - > VIP Management
 - ▼ External Data Source Management
 - Overview of External Data Source Management
 - ▼ AD/LDAP Accounts
 - AD/LDAP Overview
 - AD/LDAP Feature Requirements**
 - AD/LDAP Synchronization Mode
 - (Optional) Adding the Controller to an AD Domain
 - (Optional) Importing an AD-LDAP Trust Certificate
 - Configuring Interconnection with an AD Server
 - Configuring Interconnection with an LDAP Server
 - Interconnecting with the Google LDAP Server

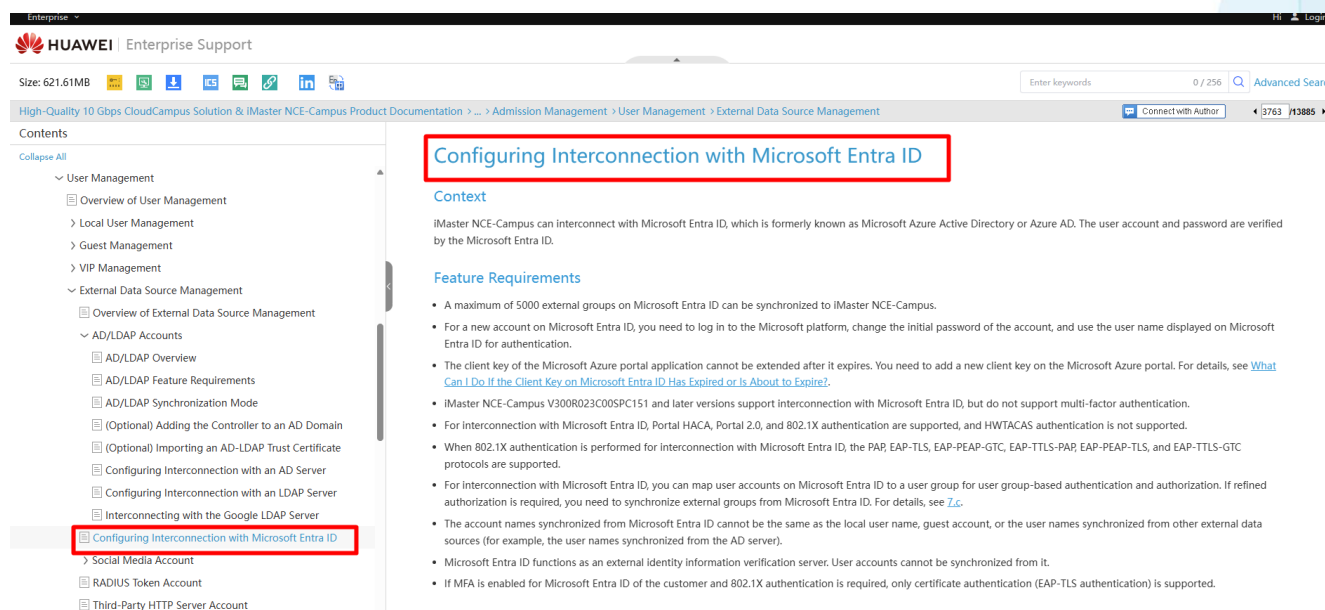
AD/LDAP Feature Requirements

Feature Requirements

- Accounts on an LDAP server cannot have duplicate usernames. If an LDAP server has accounts with the same username, an account synchronized later overwrites the account with the same username that has been synchronized earlier. That is, only the account synchronized last can be synchronized successfully. Authentication fails when **Synchronization mode** is set to **Unsynchronized account/organization structure** or **Fast synchronization** is enabled.
- If different AD/LDAP servers have accounts with the same username, subsequent accounts will fail to be synchronized after an account with the same username has been synchronized successfully. That is, only the account synchronized first can be synchronized successfully.
- A maximum of 128 synchronization scopes can be created for an AD/LDAP server.
- In the Huawei public cloud and MSP-owned cloud scenarios, the controller cannot be added to an AD domain and the EAP-PEAP-MSCHAPv2 protocol is not supported when an AD/LDAP data source is interconnected.
- In the Huawei public cloud deployment scenario, the synchronization function is not supported, and the value of **Synchronization mode** is **Unsynchronized account/organization structure** by default and cannot be changed. In this case, user accounts and passwords are directly verified on AD/LDAP servers.
- For an LDAP account that has been added to the **Match accounts** list in authentication and authorization rules, if the user group of this account is changed on the LDAP server, this account will be deleted from the **Match accounts** list in the corresponding authentication and authorization rules after user groups and accounts are re-synchronized on the AD/LDAP data source list page. If this account still needs to be matched, you need to add the account to the **Match accounts** list again.

NOTICE

- In the Huawei public cloud deployment scenario, the public cloud is located on a public network. When the public cloud interconnects with an AD/LDAP server, the server



The screenshot shows the Huawei Enterprise Support portal. The breadcrumb trail is: High-Quality 10 Gbps CloudCampus Solution & iMaster NCE-Campus Product Documentation > ... > Admission Management > User Management > External Data Source Management. The left sidebar shows a tree view under 'External Data Source Management' with 'Configuring Interconnection with Microsoft Entra ID' selected. The main content area has a red box around the title 'Configuring Interconnection with Microsoft Entra ID'. Below the title, the 'Context' section states: 'iMaster NCE-Campus can interconnect with Microsoft Entra ID, which is formerly known as Microsoft Azure Active Directory or Azure AD. The user account and password are verified by the Microsoft Entra ID.' The 'Feature Requirements' section lists several bullet points: a maximum of 5000 external groups on Microsoft Entra ID; requirements for new accounts; client key expiration; support for iMaster NCE-Campus V300R023C00SPC151 and later versions; supported authentication protocols (HACA, Portal 2.0, 802.1X, PAP, EAP-TLS, EAP-PEAP-GTC, EAP-TTLS-PAP, EAP-PEAP-TLS, EAP-TTLS-GTC); user account mapping; and MFA requirements.

Diante do exposto, comprova-se o atendimento ao item 4.2.9. do Anexo I – Especificação Técnica.

4.33) Do suposto não atendimento ao subitem 4.4.6.6. do Anexo I – Especificação Técnica

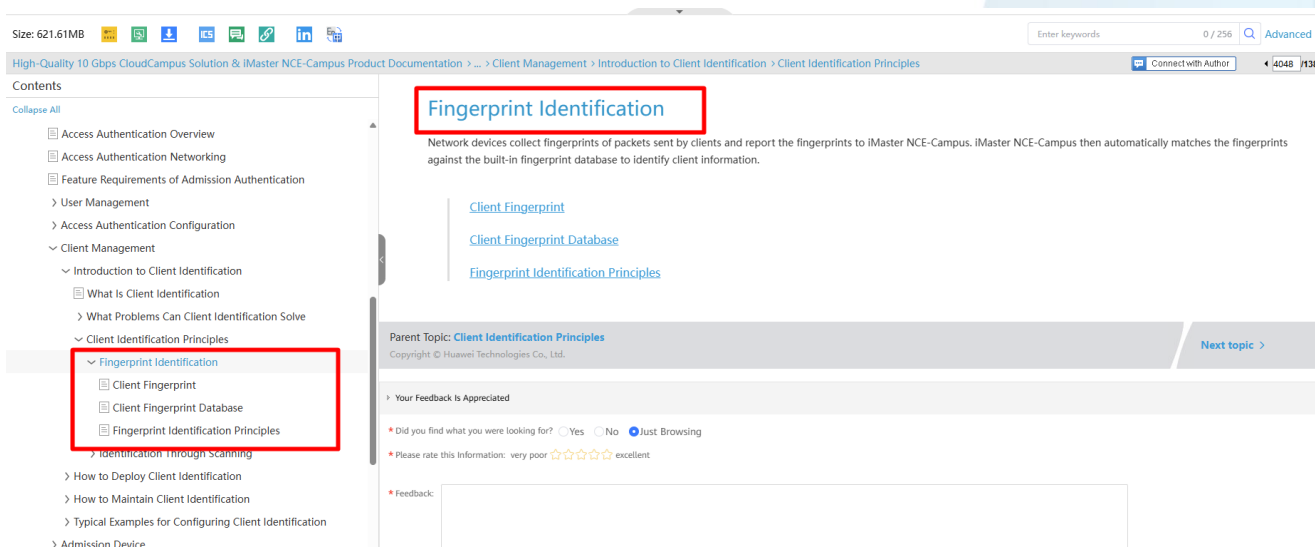
Aduz a Recorrente **TELESUL** que a comprovação técnica apresentada se refere como o captive portal é apresentado nos terminais, mas não comprova que a autorização de acesso à rede está condicionada ao tipo do terminal, sendo assim, a comprovação está incompleta, conforme exigido no subitem abaixo.

4.4.6.6. Tipo de dispositivo (IPAD, IPHONE, Android, Windows, MAC OS);

No entanto, esclarecemos que, além da evidência enviada, temos as informações abaixo que reforçam o atendimento ao item 4.4.6.6.

A Plataforma de Gerência ofertada utiliza o recurso “Fingerprint Identification”, que por meio de vários métodos identifica o tipo de dispositivo conectado à rede e com base nas políticas configuradas, permite ou não seu acesso.

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100516678&id=EN-US_TOPIC_000002346147385



The screenshot shows a web browser displaying a Huawei support article titled "Fingerprint Identification". The page is in English and contains the following content:

- Contents:** A list of topics on the left side of the page, including "Access Authentication Overview", "Access Authentication Networking", "Feature Requirements of Admission Authentication", "User Management", "Access Authentication Configuration", "Client Management", "Introduction to Client Identification", "What Is Client Identification", "What Problems Can Client Identification Solve", "Client Identification Principles", "Fingerprint Identification" (highlighted with a red box), "Identification Through Scanning", "How to Deploy Client Identification", "How to Maintain Client Identification", "Typical Examples for Configuring Client Identification", and "Admission Device".
- Fingerprint Identification:** The main content area, which includes a description of the feature: "Network devices collect fingerprints of packets sent by clients and report the fingerprints to iMaster NCE-Campus. iMaster NCE-Campus then automatically matches the fingerprints against the built-in fingerprint database to identify client information." Below this description are three links: "Client Fingerprint", "Client Fingerprint Database", and "Fingerprint Identification Principles".
- Parent Topic:** "Client Identification Principles".
- Copyright:** "Copyright © Huawei Technologies Co., Ltd."
- Your Feedback Is Appreciated:** A section for user feedback, including a question "Did you find what you were looking for?" with radio buttons for "Yes", "No", and "Just Browsing", and a star rating system for "Please rate this Information: very poor" to "excellent".

Size: 621.61MB

High-Quality 10 Gbps CloudCampus Solution & iMaster NCE-Campus Product Documentation > ... > Introduction to Client Identification > Client Identification Principles > Fingerprint Identification

Contents

Collapse All

- Access Authentication Overview
- Access Authentication Networking
- Feature Requirements of Admission Authentication
- User Management
- Access Authentication Configuration
- Client Management
 - Introduction to Client Identification
 - What Is Client Identification
 - What Problems Can Client Identification Solve
 - Client Identification Principles
 - Fingerprint Identification
 - Client Fingerprint**
 - Client Fingerprint Database
 - Fingerprint Identification Principles
 - Identification Through Scanning
 - How to Deploy Client Identification
 - How to Maintain Client Identification
 - Typical Examples for Configuring Client Identification
 - Admission Device
 - Admission Policy
 - Free Mobility
 - Authentication Component Management

Client Fingerprint

A client fingerprint is feature information used to uniquely identify a client (such as a computer or a mobile phone). Data from multiple dimensions, such as device hardware, software, and network configuration, is collected to generate a unique identifier, which is usually used for security verification, user tracing, and anti-spoofing.

A client fingerprint consists of the following elements:

- Hardware features: device model, CPU/GPU information, MAC address, and screen resolution
- Software features: OS type and version, browser type and plug-ins, font list, time zone, and language settings
- Network features: IP address, DNS configuration, proxy information, and network delay
- Behavior features: operation habit (such as mouse moving tracks) and application usage mode

The following table lists the client fingerprint types supported by iMaster NCE-Campus.

Fingerprint Type	Description
User-Agent	The User-Agent string identifies a web browser. The web server sends the most appropriate web page content based on the User-Agent of a client's web browser, ensuring content compatibility among different browsers. For example, if the User-Agent of a web browser contains "Windows NT 5.1", the kernel version of Microsoft Windows is Windows NT 5.1.
DHCP option	If a DHCP server automatically assigns IP addresses, clients (DHCP clients) obtain the DHCP option field from the DHCP server when requesting IP addresses from it or accessing the network. Different types of clients obtain different parameter values from the DHCP server so that each client type can be identified. DHCP Option 55 is a list of parameters that DHCP clients obtain from the DHCP server. If a DHCP client sends a DHCP message with 43,60 in DHCP Option 55 to request an IP address for a client from the DHCP server, it is highly possible that this client is an Apple PC using macOS. If a DHCP client sends a DHCP message with 43 in DHCP Option 55, the DHCP client reports its information as well as the vendor information to the DHCP server.
MAC OUI	A MAC address consists of six bytes. A MAC OUI is the leftmost three bytes of a MAC address and is the unique identifier of an organization. MAC OUIs are allocated to different organizations by the Institute for Electrical and Electronic Engineers (IEEE) and correspond to different NIC manufacturers. Therefore, the leftmost three bytes of a client MAC address, which can basically determine the client vendor.
mDNS	mDNS enables hosts on a LAN to discover and communicate with each other without the presence of a traditional DNS server. The default port number of mDNS is 5353. If the mDNS service is enabled on a host that accesses a LAN, the host multicasts a message to all the hosts on the LAN. The product information can be obtained from this message.

Size: 621.61MB

High-Quality 10 Gbps CloudCampus Solution & iMaster NCE-Campus Product Documentation > ... > Introduction to Client Identification > Client Identification Principles > Fingerprint Identification

Contents

Collapse All

- Access Authentication Overview
- Access Authentication Networking
- Feature Requirements of Admission Authentication
- User Management
- Access Authentication Configuration
- Client Management
 - Introduction to Client Identification
 - What Is Client Identification
 - What Problems Can Client Identification Solve
 - Client Identification Principles
 - Fingerprint Identification
 - Client Fingerprint
 - Client Fingerprint Database**
 - Fingerprint Identification Principles
 - Identification Through Scanning
 - How to Deploy Client Identification
 - How to Maintain Client Identification
 - Typical Examples for Configuring Client Identification
 - Admission Device
 - Admission Policy
 - Free Mobility
 - Authentication Component Management

Client Fingerprint Database

The client fingerprint database stores fixed client fingerprints corresponding to client types, vendors, models, and OSs. iMaster NCE-Campus presets the fingerprint database to provide fingerprint identification rules and this database is not perceived by users. iMaster NCE-Campus automatically sends collected fingerprints to the fingerprint database for comparison and identifies the types, vendors, models, and OSs based on the mappings in the fingerprint database.

Parent Topic: [Fingerprint Identification](#)

Copyright © Huawei Technologies Co., Ltd.

Your Feedback Is Appreciated

Did you find what you were looking for? ☐ Yes ☐ No ☒ Just Browsing

Please rate this information: very poor ☐ ☐ ☐ ☐ ☐ excellent

Feedback:

0 / 3000

Huawei may contact you to help you resolve the problem as soon as possible. Please enter your contact information:

Name: Email: Tel: Company:

☐ I have read and agree to the [Privacy Policy](#) of Huawei. I know that my personal information will be stored on a server in China.

Size: 621.61MB

High-Quality 10 Gbps CloudCampus Solution & iMaster NCE-Campus Product Documentation > ... > Introduction to Client Identification > Client Identification Principles > Fingerprint Identification

Contents

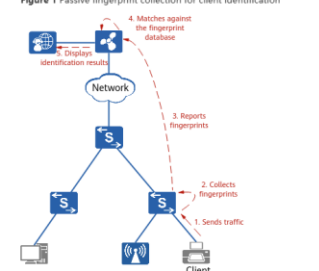
Collapse All

- Access Authentication Overview
- Access Authentication Networking
- Feature Requirements of Admission Authentication
- User Management
- Access Authentication Configuration
- Client Management
 - Introduction to Client Identification
 - What Is Client Identification
 - What Problems Can Client Identification Solve
 - Client Identification Principles
 - Fingerprint Identification
 - Client Fingerprint
 - Client Fingerprint Database
 - Fingerprint Identification Principles**
 - Identification Through Scanning
 - How to Deploy Client Identification
 - How to Maintain Client Identification
 - Typical Examples for Configuring Client Identification
 - Admission Device
 - Admission Policy
 - Free Mobility
 - Authentication Component Management

Fingerprint Identification Principles

Network devices collect client fingerprints and report them to iMaster NCE-Campus. iMaster NCE-Campus then automatically matches the fingerprints against the custom rules and built-in fingerprint database to identify types of unknown clients.

Figure 1 Passive fingerprint collection for client identification



1. When a client accesses a network, various protocol packets, such as DHCP and LLDP packets, are triggered.

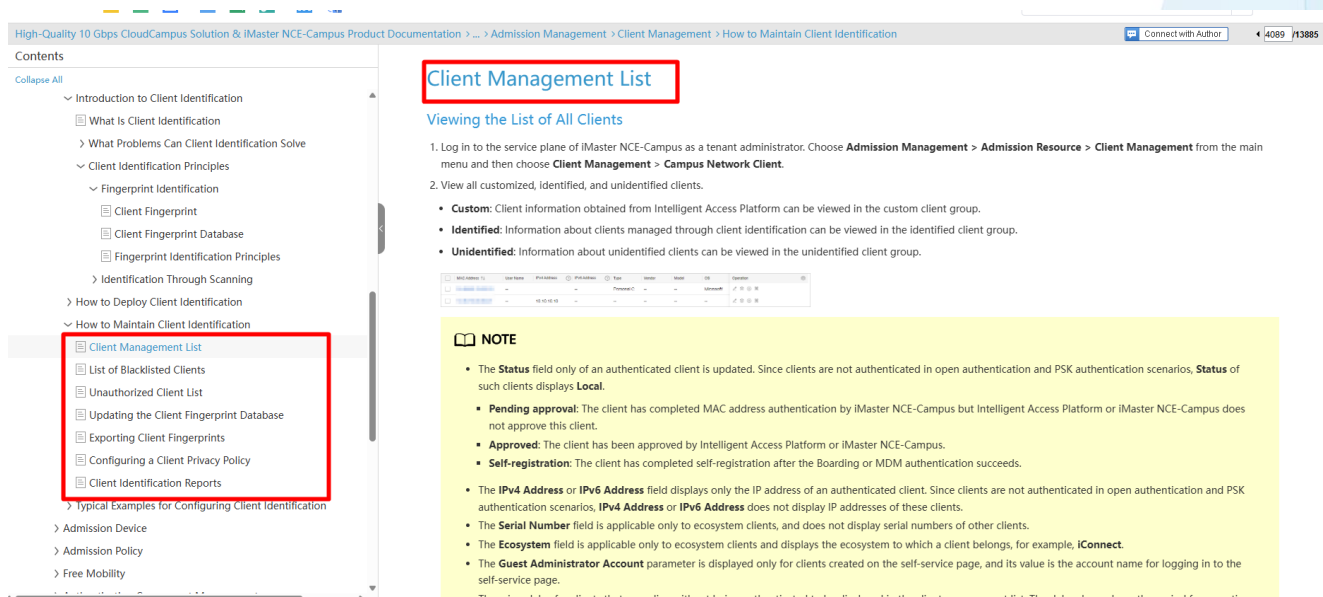
2. The device collects the protocol packets triggered by the clients as client fingerprints.

3. The device reports the fingerprints to iMaster NCE-Campus. In addition to device reporting, when a client is authenticated on iMaster NCE-Campus, iMaster NCE-Campus can obtain the client fingerprint information carried in authentication packets.

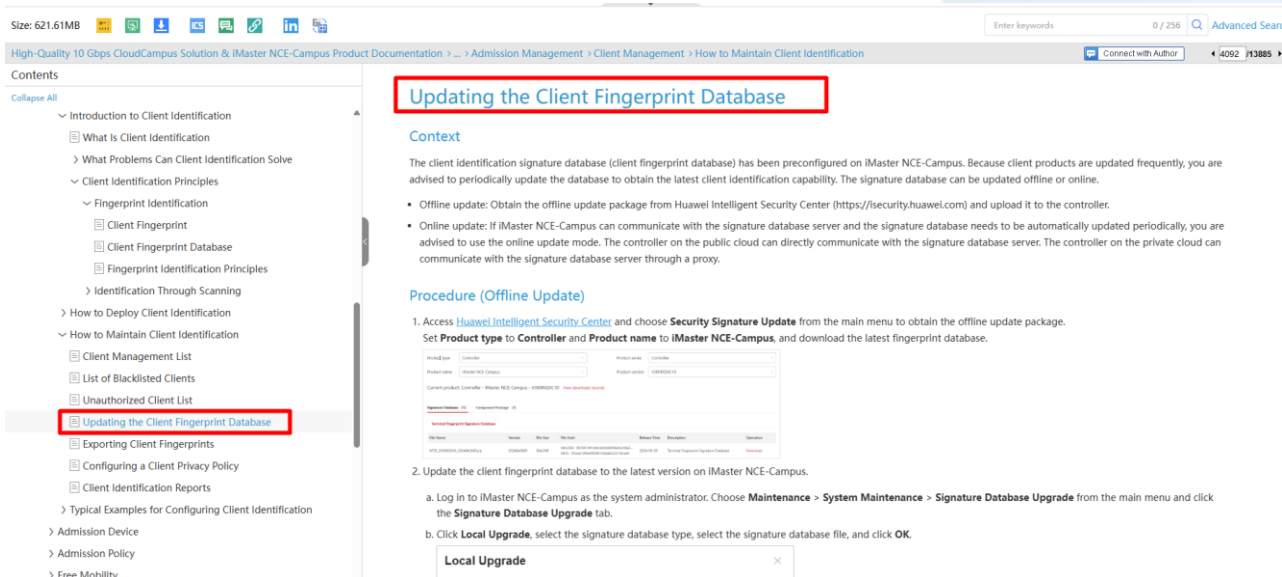
4. iMaster NCE-Campus automatically matches the clients' fingerprint information against the fingerprint database to identify the client types.

Com o recurso “Client Identification”, é possível determinar que dispositivos possuem autorização para acesso à rede.

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100516678&id=EN-US_TOPIC_0000002346147417

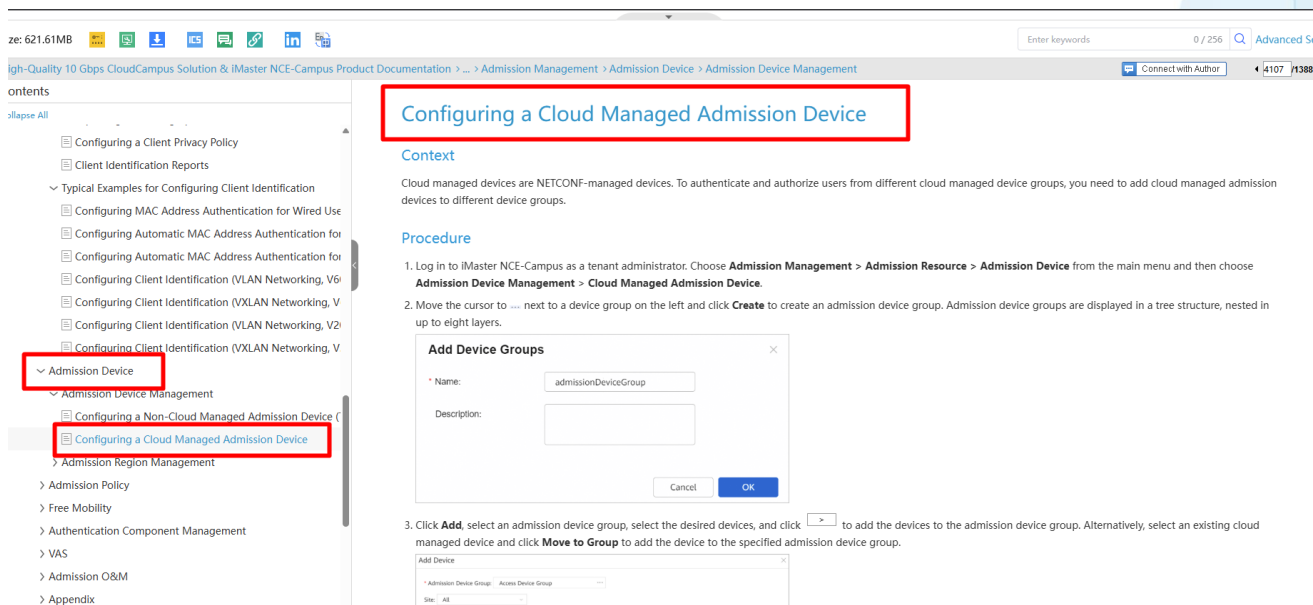


The screenshot shows the Huawei documentation page for 'Client Management List'. The left sidebar contains a table of contents with the following items: Introduction to Client Identification, What Is Client Identification, What Problems Can Client Identification Solve, Client Identification Principles, Fingerprint Identification, Client Fingerprint, Client Fingerprint Database, Fingerprint Identification Principles, Identification Through Scanning, How to Deploy Client Identification, How to Maintain Client Identification, Client Management List (highlighted), List of Blacklisted Clients, Unauthorized Client List, Updating the Client Fingerprint Database, Exporting Client Fingerprints, Configuring a Client Privacy Policy, Client Identification Reports, Typical Examples for Configuring Client Identification, Admission Device, Admission Policy, and Free Mobility. The main content area is titled 'Client Management List' and includes a section 'Viewing the List of All Clients' with steps 1 and 2. Step 1 is 'Log in to the service plane of iMaster NCE-Campus as a tenant administrator. Choose **Admission Management** > **Admission Resource** > **Client Management** from the main menu and then choose **Client Management** > **Campus Network Client**.' Step 2 is 'View all customized, identified, and unidentified clients.' Below the steps is a table with columns: ID, MAC Address, IP Address, Product Name, Product Version, Status, and Action. The table contains two rows of data. A 'NOTE' section follows, listing several points: The Status field only of an authenticated client is updated. Since clients are not authenticated in open authentication and PSK authentication scenarios, Status of such clients displays Local. Pending approval: The client has completed MAC address authentication by iMaster NCE-Campus but Intelligent Access Platform or iMaster NCE-Campus does not approve this client. Approved: The client has been approved by Intelligent Access Platform or iMaster NCE-Campus. Self-registration: The client has completed self-registration after the Boarding or MDM authentication succeeds. The IPv4 Address or IPv6 Address field displays only the IP address of an authenticated client. Since clients are not authenticated in open authentication and PSK authentication scenarios, IPv4 Address or IPv6 Address does not display IP addresses of these clients. The Serial Number field is applicable only to ecosystem clients, and does not display serial numbers of other clients. The Ecosystem field is applicable only to ecosystem clients and displays the ecosystem to which a client belongs, for example, iConnect. The Guest Administrator Account parameter is displayed only for clients created on the self-service page, and its value is the account name for logging in to the self-service page. There is a delay for clients that are not online without being authenticated to be displayed in the client management list. The delay depends on the period for reporting.



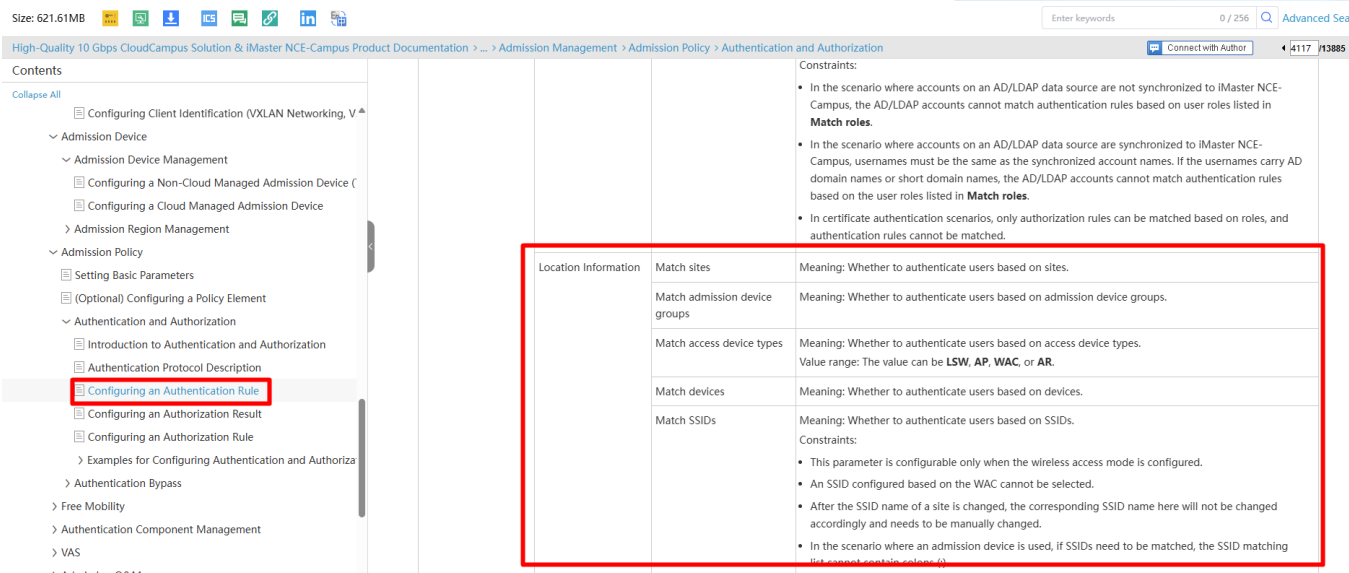
The screenshot shows the Huawei documentation page for 'Updating the Client Fingerprint Database'. The left sidebar contains a table of contents with the following items: Introduction to Client Identification, What Is Client Identification, What Problems Can Client Identification Solve, Client Identification Principles, Fingerprint Identification, Client Fingerprint, Client Fingerprint Database, Fingerprint Identification Principles, Identification Through Scanning, How to Deploy Client Identification, How to Maintain Client Identification, Client Management List, List of Blacklisted Clients, Unauthorized Client List, Updating the Client Fingerprint Database (highlighted), Exporting Client Fingerprints, Configuring a Client Privacy Policy, Client Identification Reports, Typical Examples for Configuring Client Identification, Admission Device, Admission Policy, and Free Mobility. The main content area is titled 'Updating the Client Fingerprint Database' and includes a section 'Context' with the following text: 'The client identification signature database (client fingerprint database) has been preconfigured on iMaster NCE-Campus. Because client products are updated frequently, you are advised to periodically update the database to obtain the latest client identification capability. The signature database can be updated offline or online.' Below the context is a section 'Procedure (Offline Update)' with step 1: 'Access **Huawei Intelligent Security Center** and choose **Security Signature Update** from the main menu to obtain the offline update package. Set **Product type** to **Controller** and **Product name** to **iMaster NCE-Campus**, and download the latest fingerprint database.' Below step 1 is a screenshot of the 'Security Signature Update' interface. Step 2 is 'Update the client fingerprint database to the latest version on iMaster NCE-Campus.' Below step 2 is a section 'Local Upgrade' with a sub-section 'Local Upgrade' and a sub-section 'Local Upgrade'.

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100516678&id=EN-US_TOPIC_0000002443715922



The screenshot shows a web browser displaying a Huawei support page. The page title is "Configuring a Cloud Managed Admission Device". The left sidebar contains a navigation menu with various topics, including "Admission Device" and "Admission Device Management". The main content area is titled "Configuring a Cloud Managed Admission Device" and includes a "Context" section explaining that cloud managed devices are NETCONF-managed. It also features a "Procedure" section with three steps: 1. Log in to iMaster NCE-Campus as a tenant administrator, 2. Move the cursor to the next device group and click "Create", and 3. Click "Add" to select an admission device group. A "Add Device Groups" dialog box is shown with fields for "Name" (admissionDeviceGroup) and "Description".

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100516678&id=EN-US_TOPIC_0191350369



The screenshot shows a web browser displaying a Huawei support page. The page title is "Configuring an Authentication Rule". The left sidebar contains a navigation menu with various topics, including "Authentication and Authorization". The main content area is titled "Configuring an Authentication Rule" and includes a table with constraints for authentication rules. The table has three columns: "Location Information", "Match sites", and "Meaning". The "Match sites" column lists various match criteria: Match admission device groups, Match access device types, Match devices, and Match SSIDs. The "Meaning" column provides detailed explanations for each match criterion, including constraints and scenarios where the match is applicable.

Location Information	Match sites	Meaning
	Match admission device groups	Meaning: Whether to authenticate users based on admission device groups.
	Match access device types	Meaning: Whether to authenticate users based on access device types. Value range: The value can be LSW , AP , WAC , or AR .
	Match devices	Meaning: Whether to authenticate users based on devices.
	Match SSIDs	Meaning: Whether to authenticate users based on SSIDs. Constraints: <ul style="list-style-type: none"> This parameter is configurable only when the wireless access mode is configured. An SSID configured based on the WAC cannot be selected. After the SSID name of a site is changed, the corresponding SSID name here will not be changed accordingly and needs to be manually changed. In the scenario where an admission device is used, if SSIDs need to be matched, the SSID matching list cannot contain roles.

Diante do exposto, comprova-se o atendimento ao item 4.4.6.6. do Anexo I – Especificação Técnica.

4.34) Do suposto não atendimento ao subitem 4.8.5. do Anexo I – Especificação Técnica

Aduz a Recorrente **TELESUL** que não há comprovação técnica do atendimento ao subitem abaixo.

- 4.8.5. Deve se integrar a solução de Next Generation Firewall (NGFW), provendo segmentação dinâmica de rede e compartilhamento de informações, para no mínimo o fabricante Fortinet via RSO ou Pxgrid;

No entanto, esclarecemos que, A plataforma **Huawei iMaster NCE-CloudCampus** possui arquitetura aberta e orientada à integração, permitindo interoperabilidade com soluções de segurança de terceiros, incluindo dispositivos que implementam mecanismos como **RSSO (RADIUS Single Sign-On)** e **pxGrid (Platform Exchange Grid)**, amplamente utilizados em ambientes de **Network Access Control (NAC)** e **Next Generation Firewall (NGFW)**.

Do ponto de vista técnico, o iMaster NCE-CloudCampus atua como um sistema de **controle centralizado de identidade e políticas**, sendo capaz de coletar, correlacionar e distribuir informações de autenticação, autorização e accounting (AAA). Essa capacidade é viabilizada por meio de múltiplos métodos e protocolos padronizados, tais como:

- **RADIUS (RFC 2865/2866)** para autenticação, accounting e integração com terceiros;
- **RESTful APIs abertas** para integração com sistemas externos;
- **Syslog e SNMP** para envio de eventos e telemetria;
- **SAML/OAuth2** para federação de identidade;
- **Compartilhamento de contexto de sessão de usuários (User-IP Binding)**.

Integração com RSO

A integração com soluções que utilizam **RSSO**, como firewalls da Fortinet, é suportada de forma indireta, porém plenamente funcional, por meio do compartilhamento de informações de autenticação baseadas em **RADIUS Accounting** e/ou logs de sessão.

Nesse modelo:

- O iMaster NCE-CloudCampus realiza a autenticação do usuário (por exemplo, via 802.1X, Portal ou MAC Authentication);
- As informações de sessão (usuário, IP, VLAN, horário) são exportadas via **RADIUS Accounting** ou **Syslog**;
- O firewall (ou coletor RSO) consome essas informações e associa o usuário ao endereço IP, permitindo aplicação de políticas baseadas em identidade.

Essa abordagem atende ao mesmo princípio funcional do RSO, ou seja, **propagação de identidade autenticada para enforcement de segurança em dispositivos de borda**.

Integração com pxGrid

No contexto de soluções que utilizam **pxGrid**, como o ecossistema da Cisco Systems com o **Cisco Identity Services Engine**, o iMaster NCE-CloudCampus também pode interoperar por meio de integração indireta baseada em padrões abertos.

Embora o pxGrid seja um protocolo proprietário da Cisco, sua função principal — **compartilhamento dinâmico de contexto de segurança e identidade** — pode ser atendida pelo iMaster NCE-CloudCampus através de:

- Exposição de dados de sessão via **APIs RESTful**;
- Integração com sistemas intermediários (SIEM, NAC de terceiros ou brokers de identidade);
- Exportação de eventos via **Syslog**;
- Compartilhamento de bindings usuário-IP e status de autenticação.

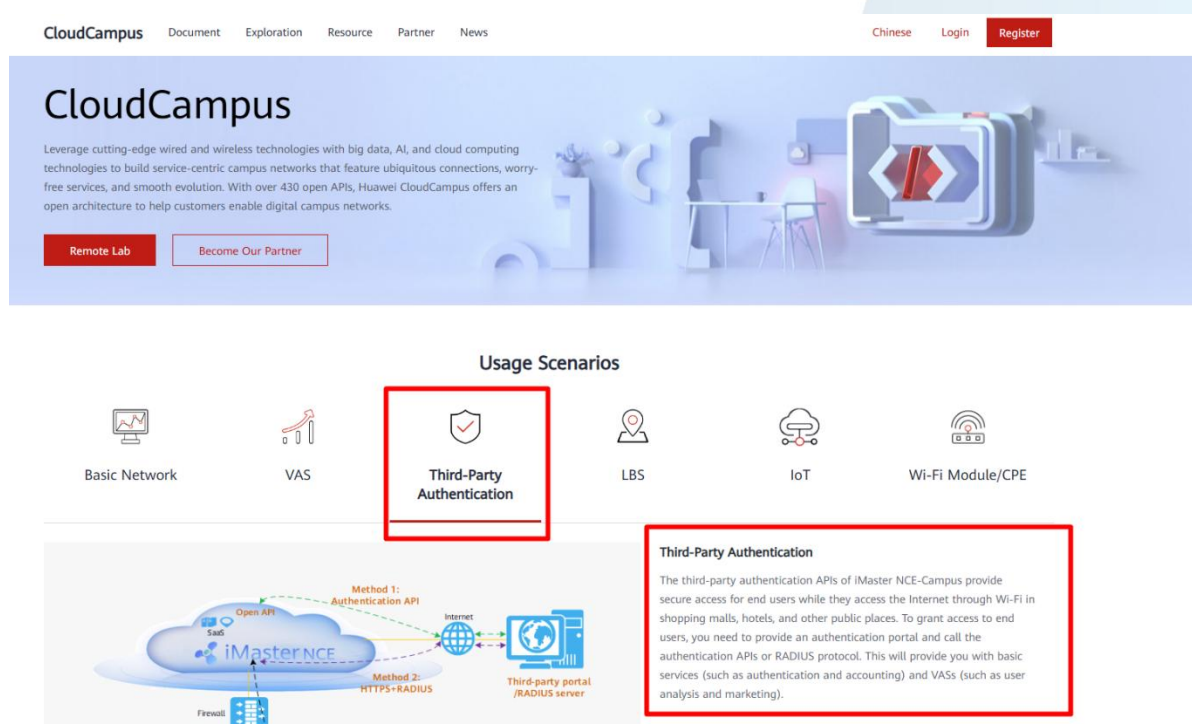
Dessa forma, um sistema que consome pxGrid pode ser alimentado indiretamente com dados provenientes do iMaster, desde que exista um componente intermediário de tradução ou correlação.

Evidências e Referências Técnicas (Huawei)

A capacidade de integração do iMaster NCE-CloudCampus é comprovada por documentação oficial da Huawei, destacando:

1. Huawei iMaster NCE-Campus Product Documentation – Open APIs

<https://intl.devzone.huawei.com/en/network/cloudcampus.html>



The screenshot displays the Huawei CloudCampus documentation page. At the top, there's a navigation bar with links like 'Document', 'Exploration', 'Resource', 'Partner', and 'News'. Below this, a large banner features the 'CloudCampus' title and a description of its capabilities. A section titled 'Usage Scenarios' lists various use cases: Basic Network, VAS, Third-Party Authentication (highlighted with a red box), LBS, IoT, and Wi-Fi Module/CPE. Below the scenarios, a diagram illustrates the 'Third-Party Authentication' process, showing the iMaster NCE cloud connected to a third-party portal/RADIUS server via the Internet. Two methods are shown: Method 1 (Authentication API) and Method 2 (HTTPS+RADIUS). A text box on the right provides a detailed description of the third-party authentication APIs, stating they provide secure access for end users in public places like shopping malls and hotels, and require an authentication portal to grant access.

<https://intl.devzone.huawei.com/en/enterprise/cloudcampus/quickStart.html#thirdAu>

th

CloudCampus Document Exploration Resource Partner News

Chinese Login Register

Getting Started

Displays the northbound open capabilities and resource overview of iMaster NCE-Campus to help developers quickly understand the CloudCampus developer community.

CloudCampus

Community Introduction

- Usage Scenarios
 - Basic Network
 - VAS
 - Third-Party Authentica...
 - LBS
 - IoT
- Resource

CloudCampus > Getting Started > Usage Scenarios > ThirdParty Authentication

Community Introduction

The CloudCampus developer community is a one-stop service platform that combines learning, development, testing, and communication for developers and partners across the datacom field. To help developers quickly develop, integrate, and roll out industry apps, CloudCampus provides more than 250 open APIs in five categories, secondary development videos and tutorials, API Explorer, API Studio, remote lab, DevOps IDE and SDK, among other resources.

iMaster NCE-Campus is an integral part of the CloudCampus solution. It is a next-generation campus and branch network controller launched by Huawei, and it supports innovative solutions such as network deployment automation, policy automation, and SD-WAN, thereby reducing OPEX and accelerating cloudification as well as digitalization for enterprises. It makes network management more convenient and network O&M more intelligent.

Usage Scenarios

Basic Network

iMaster NCE-Campus provides you with a group of RESTful APIs. External programs access the APIs through HTTPS for service provisioning, network management, and network monitoring.

Basic network APIs are used for network control, management, and O&M in MSP proxy scenarios. These APIs can be categorized as follows: basic service,

<https://intl.devzone.huawei.com/en/apistudio/sample/index.html?id=1539&categoryType=campus&language=us>

Third Party Authentication

The third-party authentication API of iMaster NCE-Campus is used to provide authentication services for end users who access the Internet through Wi-Fi in shopping malls, hotels, or other public places.

Enter an API document name. Q

Current version: V300R019C10

CloudCampus

- Getting Started
 - API Overview
- Relay Authentication (API Mode)
 - General Information
- About RESTful APIs
 - Examples
 - Java SDK Guide
 - Python SDK Guide
- Relay Authentication (RADIUS Mode)
 - Authentication Process
 - Supported Attributes in RADIUS Packets

Getting Started

API Overview

Third-party authentication is required for end users who access the Internet through Wi-Fi in shopping malls, supermarkets, hotels, airports, and other public places. To grant access to end users, you need to provide an authentication portal and call the authentication APIs or RADIUS protocol. This will provide you with basic services (such as authentication and accounting) and VASs (such as user analysis and marketing).

In third-party authentication, secondary development is required only for relay authentication. iMaster NCE-Campus supports the following relay authentication modes:

- API mode
- RADIUS mode

Relay Authentication (API Mode)

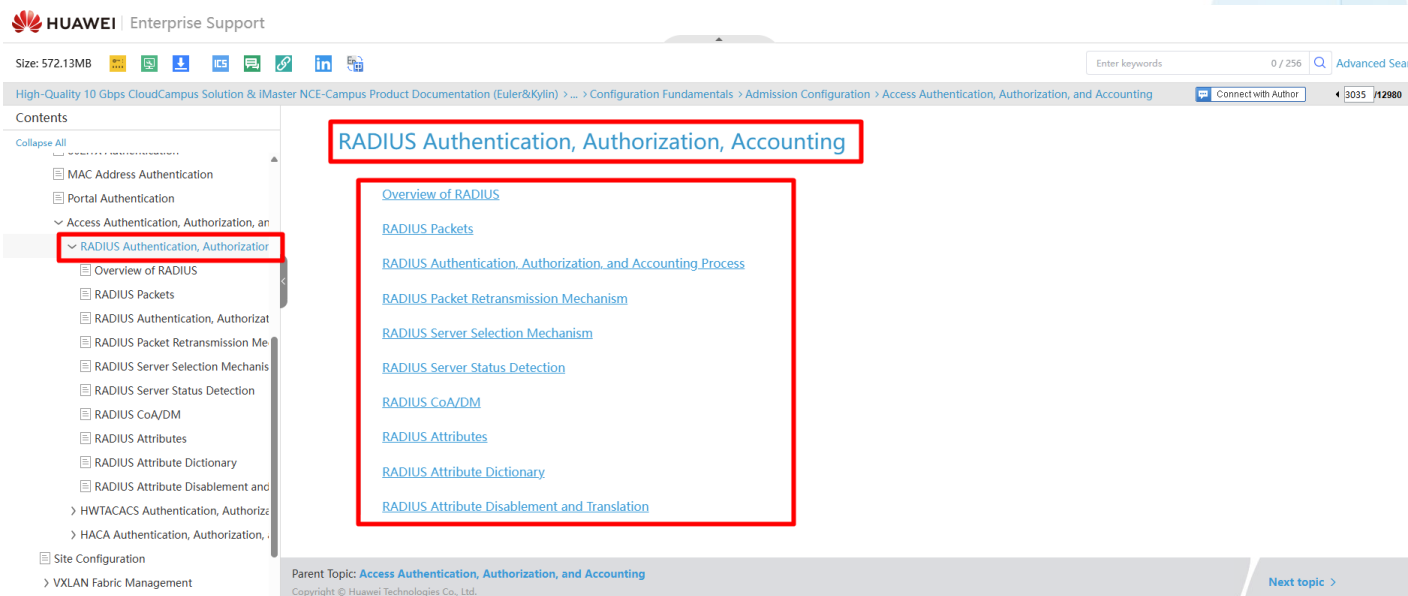
When a user attempts to access the Internet, the user connects to the SSID of a Wi-Fi network and logs in to the portal page pushed by a third-party system for authentication. The third-party system invokes the authorization APIs of Huawei iMaster NCE-Campus and authorizes the AP with the permission for the terminal to access the Wi-Fi network. In this way, the user terminal can access the Internet.

Interaction between iMaster NCE-Campus and a third-party system through APIs



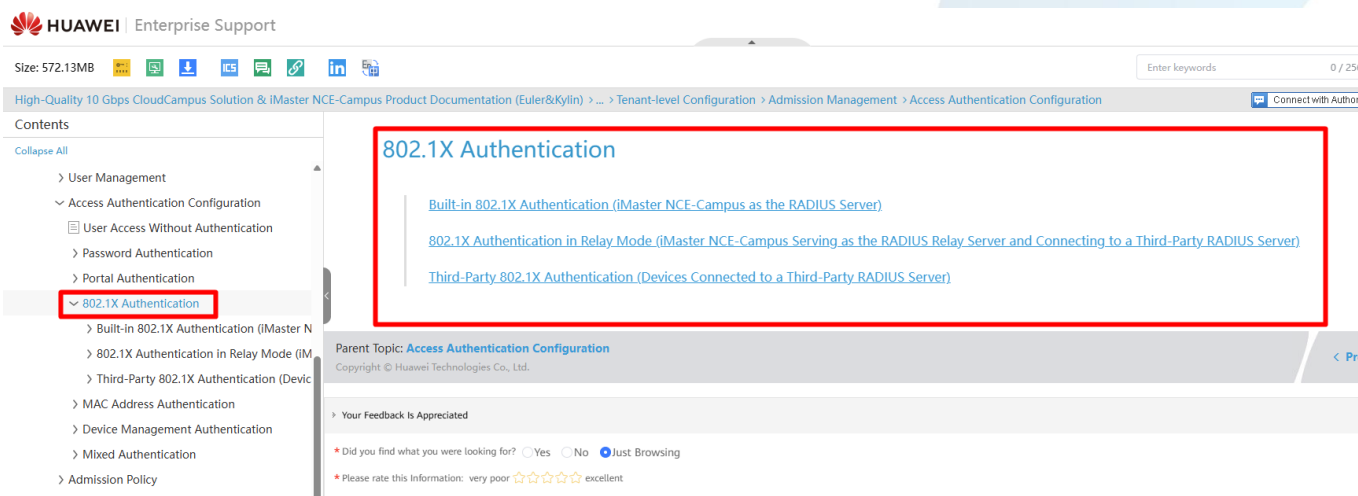
2. Huawei Campus Network Solution – Authentication and Authorization

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100413634&id=EN-US_TOPIC_000001399669260



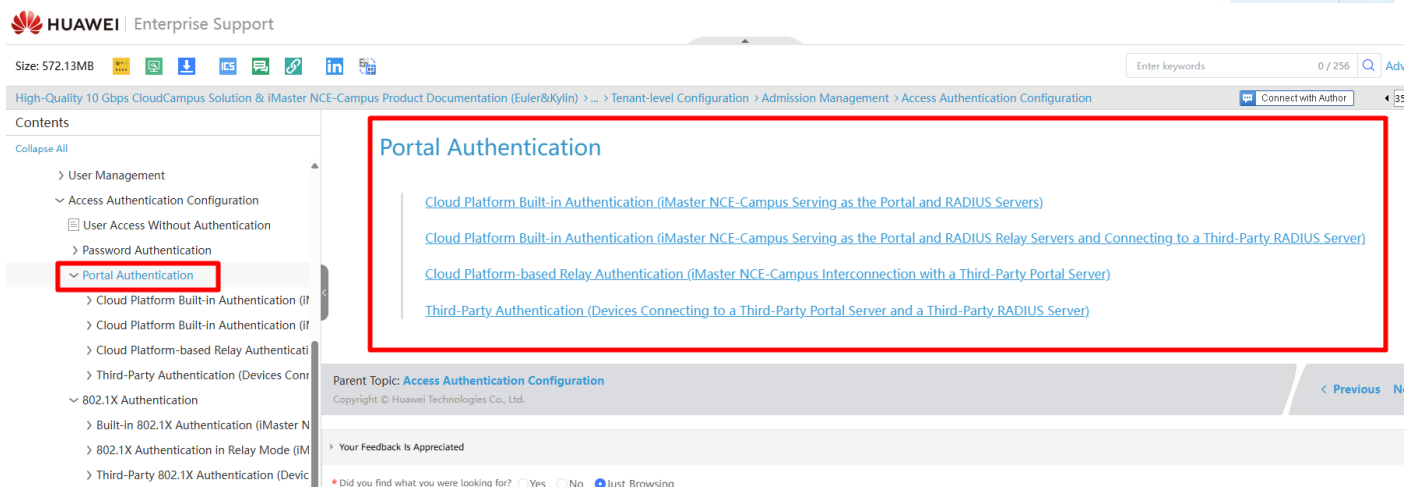
The screenshot shows the Huawei Enterprise Support page for the topic "RADIUS Authentication, Authorization, Accounting". The page is titled "RADIUS Authentication, Authorization, Accounting" and is part of the "Access Authentication, Authorization, and Accounting" parent topic. The left sidebar shows a navigation tree with "RADIUS Authentication, Authorization, Accounting" selected. The main content area lists several sub-topics: Overview of RADIUS, RADIUS Packets, RADIUS Authentication, Authorization, and Accounting Process, RADIUS Packet Retransmission Mechanism, RADIUS Server Selection Mechanism, RADIUS Server Status Detection, RADIUS CoA/DM, RADIUS Attributes, RADIUS Attribute Dictionary, and RADIUS Attribute Disabling and Translation. The page also includes a search bar, a "Connect with Author" button, and a "Next topic" link.

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100413634&id=EN-US_TOPIC_000001785091882



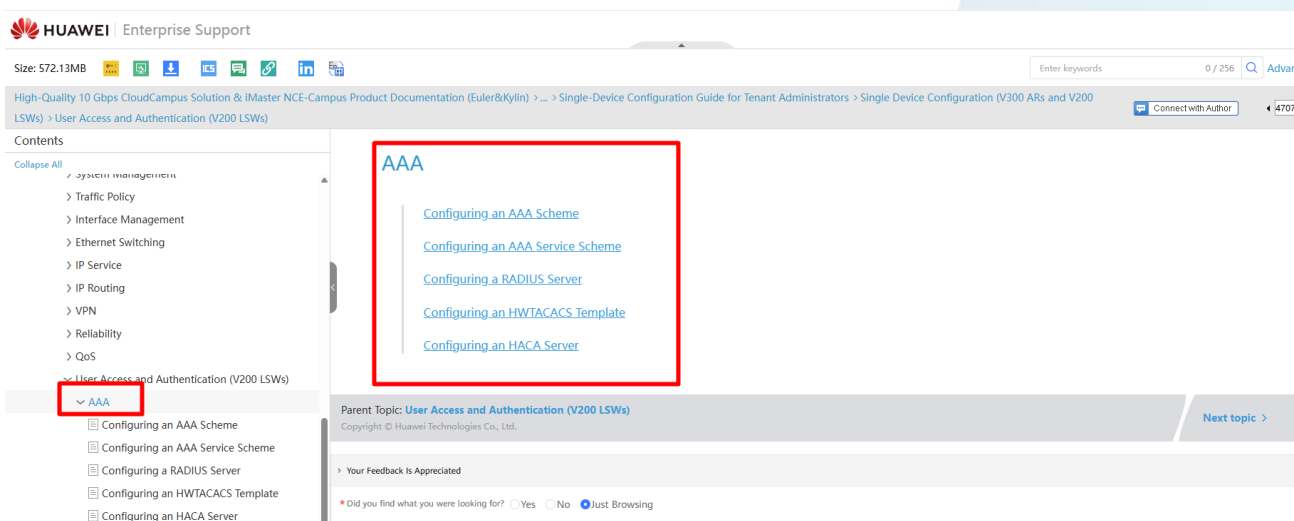
The screenshot shows the Huawei Enterprise Support page for the topic "802.1X Authentication". The page is titled "802.1X Authentication" and is part of the "Access Authentication Configuration" parent topic. The left sidebar shows a navigation tree with "802.1X Authentication" selected. The main content area lists several sub-topics: Built-in 802.1X Authentication (iMaster NCE-Campus as the RADIUS Server), 802.1X Authentication in Relay Mode (iMaster NCE-Campus Serving as the RADIUS Relay Server and Connecting to a Third-Party RADIUS Server), and Third-Party 802.1X Authentication (Devices Connected to a Third-Party RADIUS Server). The page also includes a search bar, a "Connect with Author" button, and a "Next topic" link.

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100413634&id=EN-US_TOPIC_0000001785082966



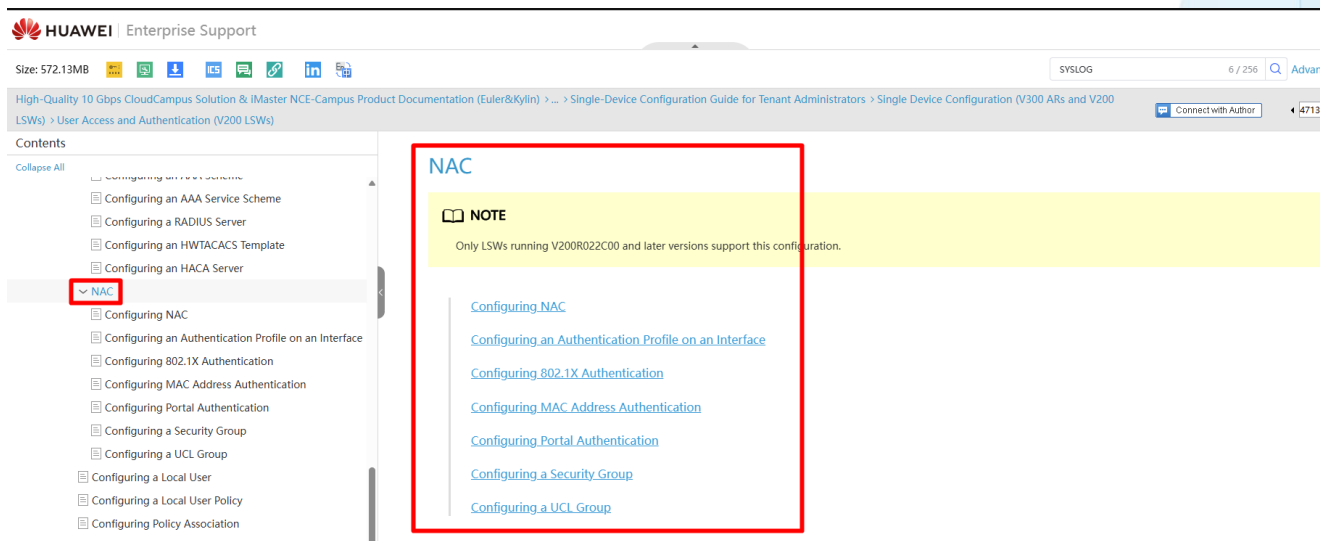
The screenshot shows the Huawei Enterprise Support website. The left sidebar contains a 'Contents' menu with 'Portal Authentication' highlighted. The main content area is titled 'Portal Authentication' and lists four links: 'Cloud Platform Built-in Authentication (iMaster NCE-Campus Serving as the Portal and RADIUS Servers)', 'Cloud Platform Built-in Authentication (iMaster NCE-Campus Serving as the Portal and RADIUS Relay Servers and Connecting to a Third-Party RADIUS Server)', 'Cloud Platform-based Relay Authentication (iMaster NCE-Campus Interconnection with a Third-Party Portal Server)', and 'Third-Party Authentication (Devices Connecting to a Third-Party Portal Server and a Third-Party RADIUS Server)'. The page footer includes a feedback section with a 'Just Browsing' button selected.

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100413634&id=EN-US_TOPIC_0000001689754585



The screenshot shows the Huawei Enterprise Support website. The left sidebar contains a 'Contents' menu with 'AAA' highlighted. The main content area is titled 'AAA' and lists five links: 'Configuring an AAA Scheme', 'Configuring an AAA Service Scheme', 'Configuring a RADIUS Server', 'Configuring an HWTACACS Template', and 'Configuring an HACA Server'. The page footer includes a feedback section with a 'Just Browsing' button selected.

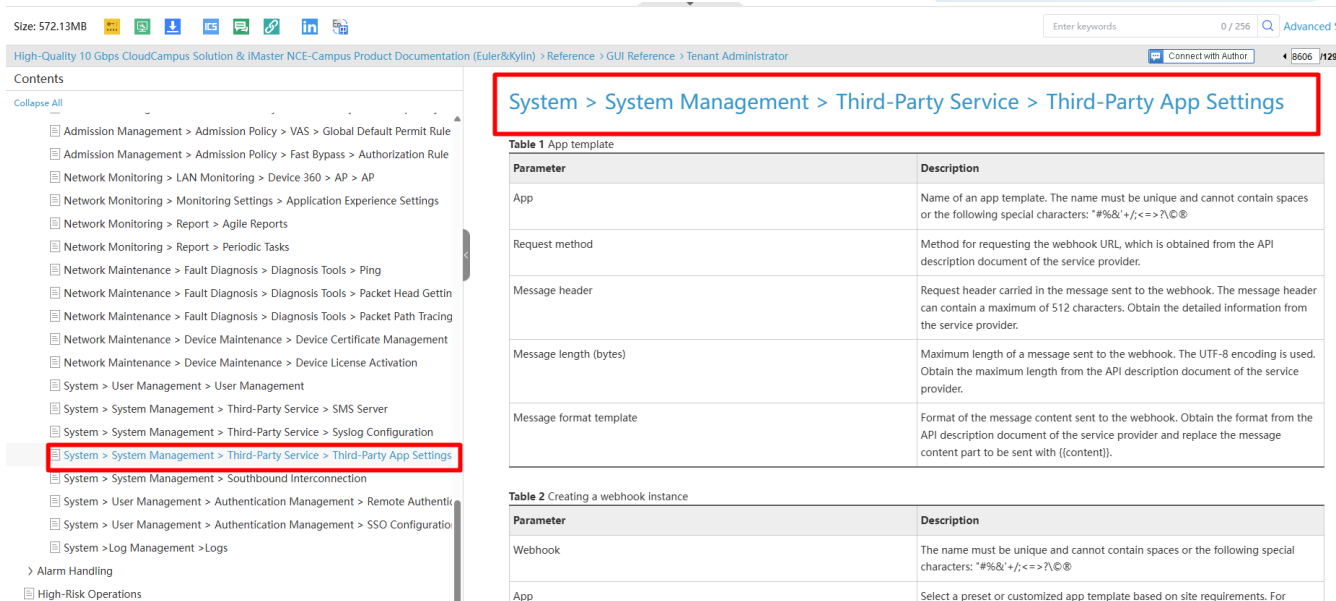
https://support.huawei.com/hedex/hdx.do?docid=EDOC1100413634&id=EN-US_TOPIC_0000001689633845



The screenshot shows the Huawei Enterprise Support page for NAC configuration. The left sidebar lists various configuration topics, with 'NAC' highlighted. The main content area shows a 'NOTE' stating that only LSUs running V200R022C00 and later versions support this configuration. Below the note, there are links to various NAC configuration topics: 'Configuring NAC', 'Configuring an Authentication Profile on an Interface', 'Configuring 802.1X Authentication', 'Configuring MAC Address Authentication', 'Configuring Portal Authentication', 'Configuring a Security Group', 'Configuring a UCL Group', 'Configuring a Local User', 'Configuring a Local User Policy', and 'Configuring Policy Association'.

3. Huawei Security White Papers – Ecosystem Integration

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100413634&id=EN-US_TOPIC_0000001792397093

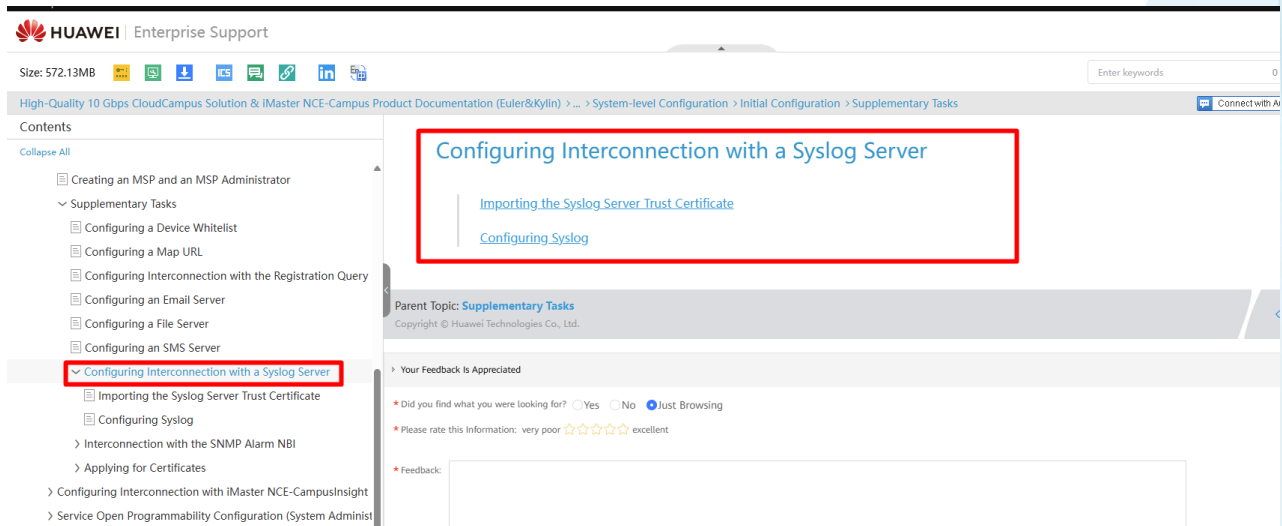


The screenshot shows the Huawei Enterprise Support page for Third-Party App Settings. The left sidebar lists various configuration topics, with 'System > System Management > Third-Party Service > Third-Party App Settings' highlighted. The main content area shows a table with parameters for creating a webhook instance. The table has two columns: 'Parameter' and 'Description'.

Parameter	Description
App	Name of an app template. The name must be unique and cannot contain spaces or the following special characters: "%&'+/;<=>?\\ @&".
Request method	Method for requesting the webhook URL, which is obtained from the API description document of the service provider.
Message header	Request header carried in the message sent to the webhook. The message header can contain a maximum of 512 characters. Obtain the detailed information from the service provider.
Message length (bytes)	Maximum length of a message sent to the webhook. The UTF-8 encoding is used. Obtain the maximum length from the API description document of the service provider.
Message format template	Format of the message content sent to the webhook. Obtain the format from the API description document of the service provider and replace the message content part to be sent with {content}.

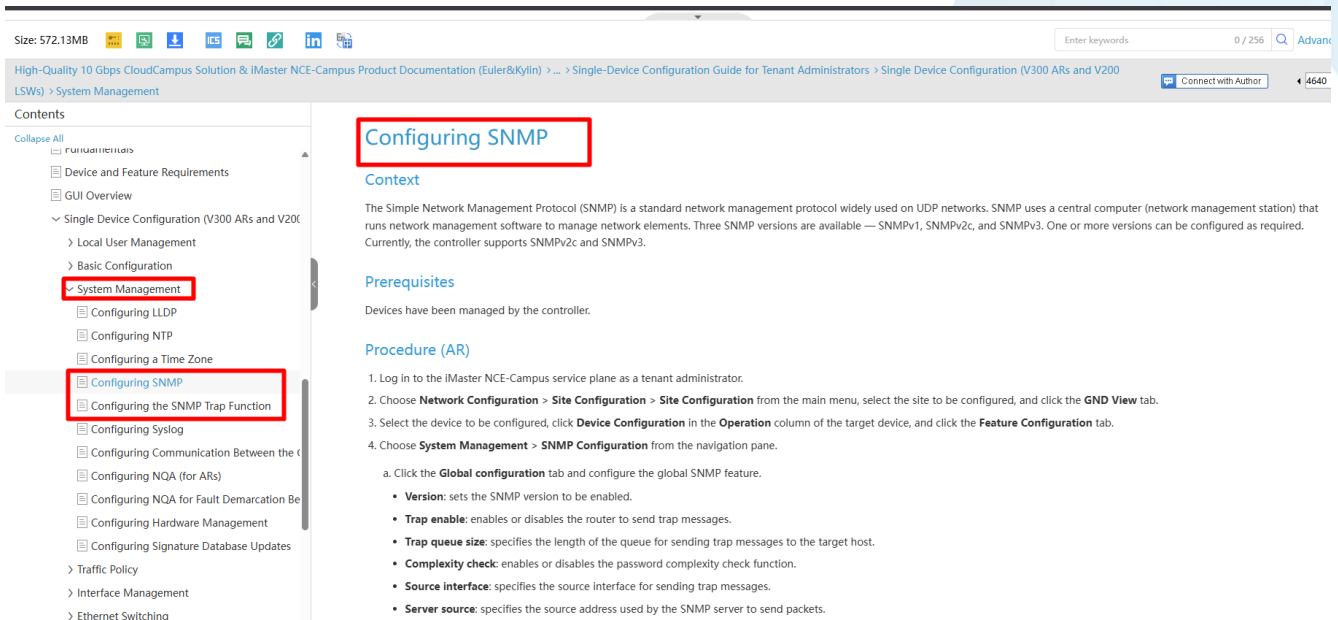
4. Huawei iMaster NCE-Campus – Southbound & Northbound Interfaces

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100413634&id=EN-US_TOPIC_000001162440633



The screenshot shows the Huawei Enterprise Support page. The breadcrumb trail is: High-Quality 10 Gbps CloudCampus Solution & iMaster NCE-Campus Product Documentation (Euler&Kylin) > ... > System-level Configuration > Initial Configuration > Supplementary Tasks. The left sidebar shows a tree of topics, with 'Configuring Interconnection with a Syslog Server' highlighted. The main content area shows the title 'Configuring Interconnection with a Syslog Server' and two sub-topics: 'Importing the Syslog Server Trust Certificate' and 'Configuring Syslog'. The 'Configuring Syslog' sub-topic is highlighted with a red box.

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100413634&id=EN-US_TOPIC_000001285380325



The screenshot shows the Huawei Enterprise Support page. The breadcrumb trail is: High-Quality 10 Gbps CloudCampus Solution & iMaster NCE-Campus Product Documentation (Euler&Kylin) > ... > Single-Device Configuration Guide for Tenant Administrators > Single-Device Configuration (V300 ARs and V200 LSWs) > System Management. The left sidebar shows a tree of topics, with 'Configuring SNMP' highlighted. The main content area shows the title 'Configuring SNMP' and a 'Context' section. Below the context, there is a 'Prerequisites' section and a 'Procedure (AR)' section. The 'Procedure (AR)' section lists four steps: 1. Log in to the iMaster NCE-Campus service plane as a tenant administrator. 2. Choose **Network Configuration** > **Site Configuration** > **Site Configuration** from the main menu, select the site to be configured, and click the **GND View** tab. 3. Select the device to be configured, click **Device Configuration** in the **Operation** column of the target device, and click the **Feature Configuration** tab. 4. Choose **System Management** > **SNMP Configuration** from the navigation pane. Below the steps, there is a list of configuration parameters: **Version**, **Trap enable**, **Trap queue size**, **Complexity check**, **Source interface**, and **Server source**.

Size: 572.13MB

Enter keywords 0 / 256

High-Quality 10 Gbps CloudCampus Solution & iMaster NCE-Campus Product Documentation (Euler&Kylin) > ... > Single-Device Configuration Guide for Tenant Administrators > Single Device Configuration (V300 ARs and V200 LSWs) > System Management

Connect with Author 4641

Contents

Collapse All

fundamentals

Device and Feature Requirements

GUI Overview

Single Device Configuration (V300 ARs and V200 LSWs)

Local User Management

Basic Configuration

System Management

Configuring LLDP

Configuring NTP

Configuring a Time Zone

Configuring SNMP

Configuring the SNMP Trap Function

Configuring Syslog

Configuring Communication Between the iMaster NCE-Campus and the Network Device

Configuring NQA (for ARs)

Configuring NQA for Fault Demarcation Between the iMaster NCE-Campus and the Network Device

Configuring Hardware Management

Configuring Signature Database Updates

Traffic Policy

Interface Management

Configuring the SNMP Trap Function

Context

You can configure devices to send specified SNMP traps to an NMS to facilitate fault locating.

Procedure

1. Log in to the iMaster NCE-Campus service plane as a tenant administrator.
2. Choose **Network Configuration** > **Site Configuration** > **Site Configuration** from the main menu, select the site to be configured, and click the **GND View** tab.
3. Select the device to be configured, click **Device Configuration** in the **Operation** column of the target device, and click the **Feature Configuration** tab.
4. Choose **System Management** > **SNMP Trap Configuration** from the navigation pane.
5. Specify the source interface for sending SNMP traps.
6. Click **Commit** to deliver the configuration to the target device. If the device is online, the configuration is delivered to the device. If the device is not online, the configuration will be delivered to the device after it goes online.
7. Click **Configuration Result** to view the configuration delivery result. If the device is online, the configuration status should be **Succeed**. If the device is offline, the configuration status should be **Pre-configuration**.

Parameter Description

Table 1 Parameters for configuring the SNMP trap function

Complementarmente, o **RADIUS Single Sign-On (RSSO)** é um recurso **proprietário da Fortinet**, não se tratando de um protocolo padronizado por entidades como o IETF.

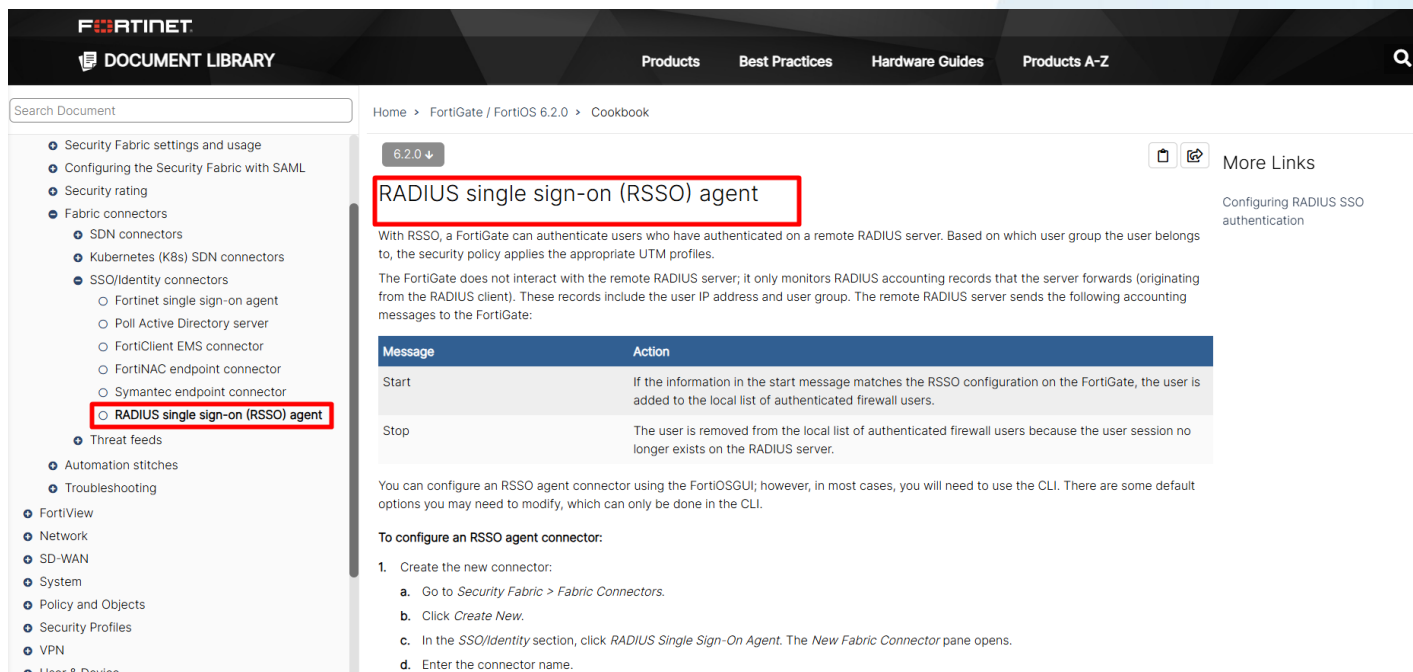
Tecnicamente, o RSSO consiste em uma funcionalidade implementada nos equipamentos da Fortinet, como o FortiGate, que utiliza mensagens de **RADIUS Accounting** — estas sim baseadas em um protocolo aberto — para identificar e correlacionar usuários autenticados na rede. A partir dessas informações, o dispositivo cria sessões de usuário e aplica políticas de segurança baseadas em identidade.

Importante destacar que:

- O termo **RSSO (RADIUS Single Sign-On)** é uma denominação exclusiva da Fortinet, não existindo como padrão formal em RFCs;
- A lógica de processamento, correlação de identidade e aplicação de políticas é **definida e implementada pela própria Fortinet**;
- Não há interoperabilidade garantida entre fabricantes utilizando o conceito de RSSO, justamente por se tratar de uma implementação proprietária.

Abaixo evidência do portal da Fortinet:

<https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/85730/radius-single-sign-on-rsso-agent>



The screenshot shows the Fortinet Document Library interface. The left sidebar contains a search bar and a navigation menu with categories like Security Fabric, Fabric connectors, and Threat feeds. The main content area displays the document 'RADIUS single sign-on (RSSO) agent' for FortiGate / FortiOS 6.2.0. The document title is highlighted with a red box. The content includes an introduction to RSSO, a table of messages and actions, and configuration instructions.

Message	Action
Start	If the information in the start message matches the RSSO configuration on the FortiGate, the user is added to the local list of authenticated firewall users.
Stop	The user is removed from the local list of authenticated firewall users because the user session no longer exists on the RADIUS server.

To configure an RSSO agent connector:

1. Create the new connector:
 - a. Go to *Security Fabric > Fabric Connectors*.
 - b. Click *Create New*.
 - c. In the *SSO/Identity* section, click *RADIUS Single Sign-On Agent*. The *New Fabric Connector* pane opens.
 - d. Enter the connector name.

O **pxGrid (Platform Exchange Grid)** por sua vez, é um protocolo e framework de integração **proprietário da Cisco Systems**, desenvolvido como parte da arquitetura de segurança da própria fabricante.

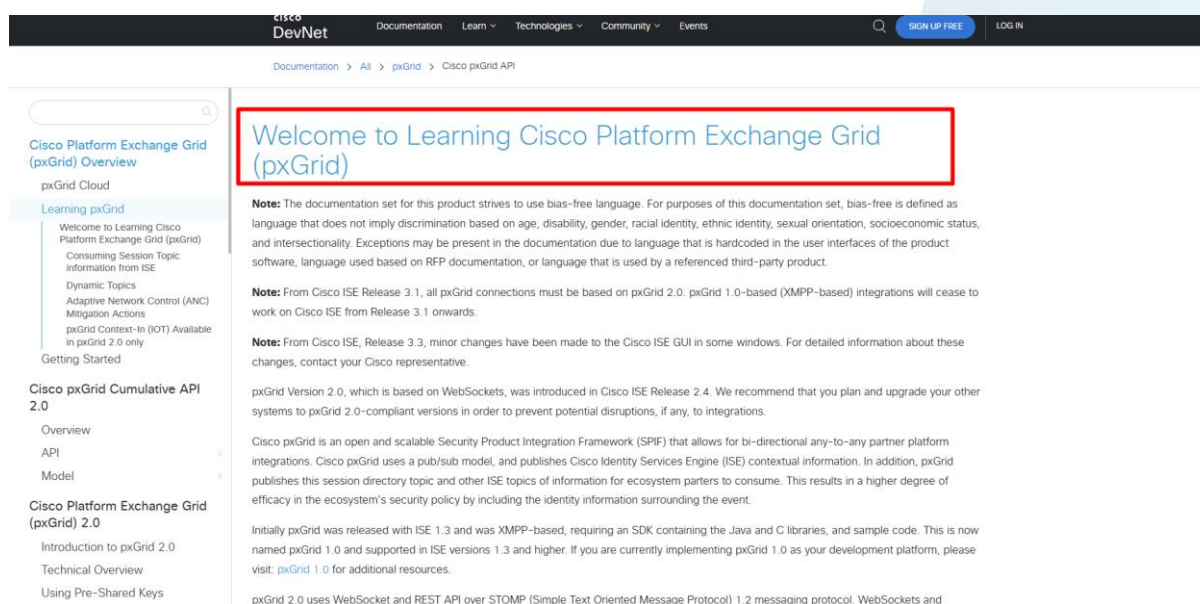
Trata-se de um mecanismo criado pela Cisco para permitir o **compartilhamento dinâmico de contexto de segurança** entre diferentes soluções, sendo amplamente utilizado em conjunto com o **Cisco Identity Services Engine (ISE)**. Por meio do pxGrid, sistemas de terceiros podem se integrar ao ecossistema Cisco para troca de informações como identidade de usuários, postura de dispositivos, eventos de segurança e políticas de controle de acesso.

Do ponto de vista técnico e comercial, o pxGrid não é um padrão aberto definido por organismos de padronização como o IETF ou o IEEE. Sua especificação, evolução e implementação são **controladas exclusivamente pela Cisco**, sendo disponibilizadas através de documentação oficial e APIs próprias da fabricante.

Dessa forma, pode-se afirmar que o pxGrid é um **protocolo proprietário da Cisco**, ainda que permita integração com soluções de terceiros mediante uso de suas APIs e documentação técnica fornecida pela própria empresa.

Abaixo evidência do Portal Cisco:

<https://developer.cisco.com/docs/pxgrid/learning-pxgrid/>



The screenshot shows the Cisco DevNet Learning page for Cisco Platform Exchange Grid (pxGrid). The page title is "Welcome to Learning Cisco Platform Exchange Grid (pxGrid)". The left sidebar shows a navigation menu with "Cisco Platform Exchange Grid (pxGrid) Overview" and "Learning pxGrid" highlighted. The main content area contains several "Note" sections and a "Getting Started" section. A red box highlights the title "Welcome to Learning Cisco Platform Exchange Grid (pxGrid)".

Note: The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Note: From Cisco ISE Release 3.1, all pxGrid connections must be based on pxGrid 2.0. pxGrid 1.0-based (XMPP-based) integrations will cease to work on Cisco ISE from Release 3.1 onwards.

Note: From Cisco ISE, Release 3.3, minor changes have been made to the Cisco ISE GUI in some windows. For detailed information about these changes, contact your Cisco representative.

pxGrid Version 2.0, which is based on WebSockets, was introduced in Cisco ISE Release 2.4. We recommend that you plan and upgrade your other systems to pxGrid 2.0-compliant versions in order to prevent potential disruptions, if any, to integrations.

Cisco pxGrid is an open and scalable Security Product Integration Framework (SPIF) that allows for bi-directional any-to-any partner platform integrations. Cisco pxGrid uses a pub/sub model, and publishes Cisco Identity Services Engine (ISE) contextual information. In addition, pxGrid publishes this session directory topic and other ISE topics of information for ecosystem partners to consume. This results in a higher degree of efficacy in the ecosystem's security policy by including the identity information surrounding the event.

Initially pxGrid was released with ISE 1.3 and was XMPP-based, requiring an SDK containing the Java and C libraries, and sample code. This is now named pxGrid 1.0 and supported in ISE versions 1.3 and higher. If you are currently implementing pxGrid 1.0 as your development platform, please visit: [pxGrid 1.0](#) for additional resources.

pxGrid 2.0 uses WebSocket and REST API over STOMP (Simple Text Oriented Message Protocol) 1.2 messaging protocol. WebSockets and

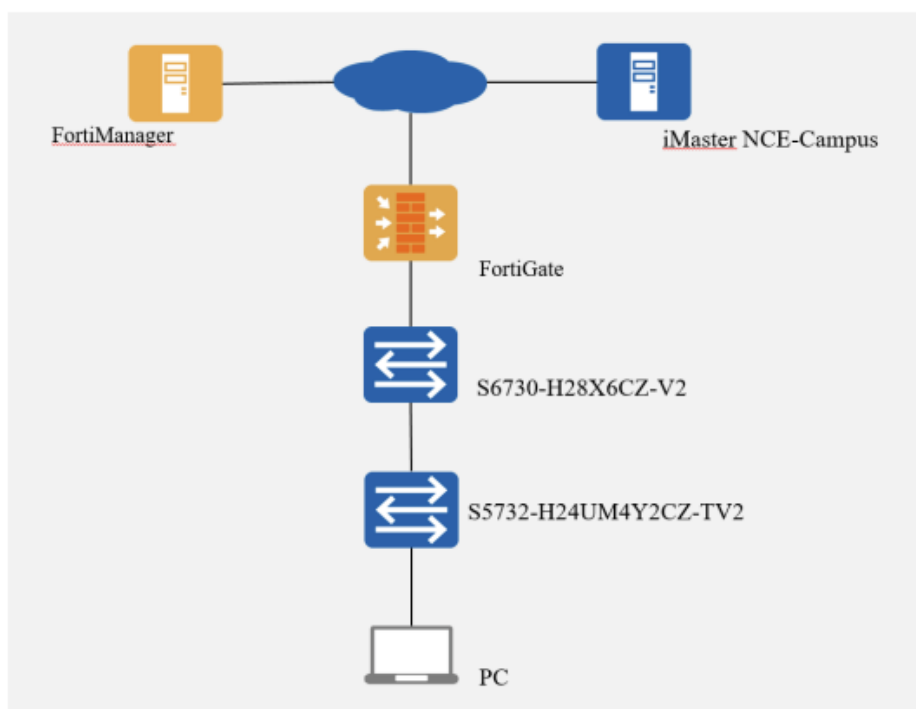
Para comprovação da integração entre a Plataforma de Gerência NCE-CaloluCampus e solução Fortinet, temos o documento iMaster NCE-Campus V300R025C00 Interoperability With Fortinet Test Report R25.0.pdf, que demonstra a configuração das duas soluções utilizando pxGRID nos equipamentos Fortinet e AAA Server na Solução Huawei.

Contents

1 Overview	1
2 Test Environment	2
2.1 Topology	2
2.2 Devices and Software	3
3 Configuring iMaster NCE-Campus	4
3.1 Configuring Authentication and Authorization	4
4 Interconnecting iMaster NCE-Campus with FortiManager	8
4.1 Applying for and Importing the Certificate	8
4.2 Configuring Interconnection	12
4.3 Configuring a Security Policy	15
5 Test Cases	20
5.1 Interconnecting iMaster NCE-Campus with FortiManager	20
5.2 Reporting User Login and Logout Messages	22
5.3 Changing the Authorized Security Group	26
5.4 Communication Failure Between FortiManager and iMaster NCE-Campus	28

Página 02 (dois), Topologia:

2.1 Topology



Página 03 (três), equipamentos utilizados:

2.2 Devices and Software

Device	Model	Software Version	Quantity	Remarks
Fortinet-Forti Manager	FortiManager	FortiManager-v7.4.6	1	pxGrid client
Fortinet-Forti Gate	FortiGate	FortiGate-200F v7.2.9	1	pxGrid client
Huawei Switch	S6730-H28X6CZ-V2	V600R025C00SPC500	1	Border
	S5732-H24UM4Y2CZ-TV2	V600R025C00SPC500	1	Edge
iMaster NCE-Campus	iMaster NCE-Campus	V300R025C00SPC100	1	AAA Server

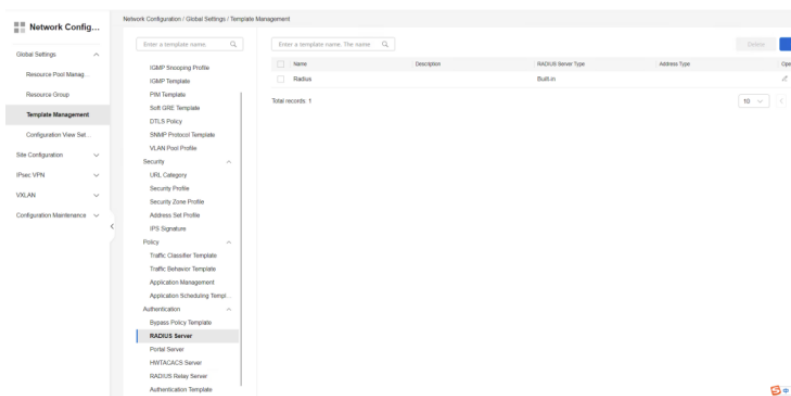
Página 07 (sete), procedimento de configuração do iMaster NCE-Campus:

3 Configuring iMaster NCE-Campus

3.1 Configuring Authentication and Authorization

3.1 Configuring Authentication and Authorization

1. Configure authentication.



Página 11 (onze), Procedimento para importação de certificado e configuração dos equipamentos Fortinet:

4 Interconnecting iMaster NCE-Campus with FortiManager

[4.1 Applying for and Importing the Certificate](#)

[4.2 Configuring Interconnection](#)

[4.3 Configuring a Security Policy](#)

4.1 Applying for and Importing the Certificate

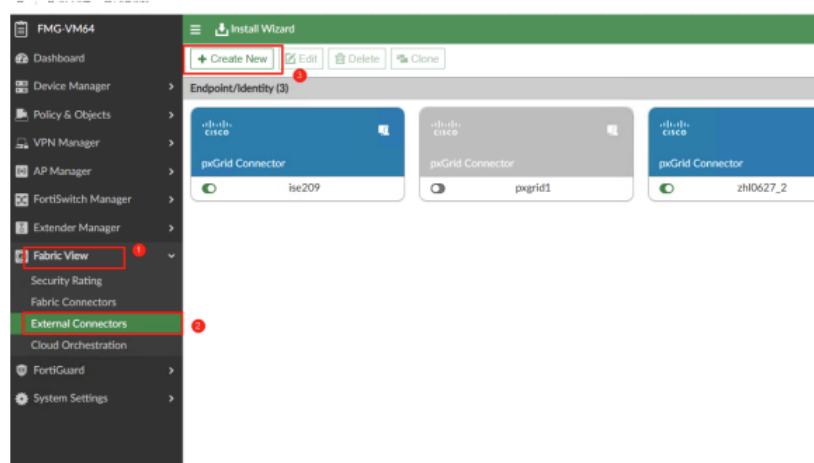
1. Apply for and import certificates through iMaster NCE-Campus and a third-party client (iMaster NCE-Campus as the CA).
 - a. Log in to iMaster NCE-Campus as the system administrator, choose **System > Security Management > Certificate Authority Service** from the main menu, and choose **PKI Management > CA** from the navigation pane. Click **Add**, enter the required information, and click **Next**.
 - b. On the **Set Associate Profile** page, select **END_ENTITY_PREDEFINED_MULTI_KEY_TYPES_50YEARS**, and select the check box before the profile on the right to set it as the default profile. Click **Next**.

Página 15 (dezesseis), configuração da interconexão conexão nos equipamentos Fortinet:

4.2 Configuring Interconnection

1. Go to *Fabric View > External Connectors*, Under *Endpoint/Identity*, select *User pxGrid*, and click *Create New*. The *Create New Fabric Connector* wizard is displayed.

Configure the following options and click *OK*

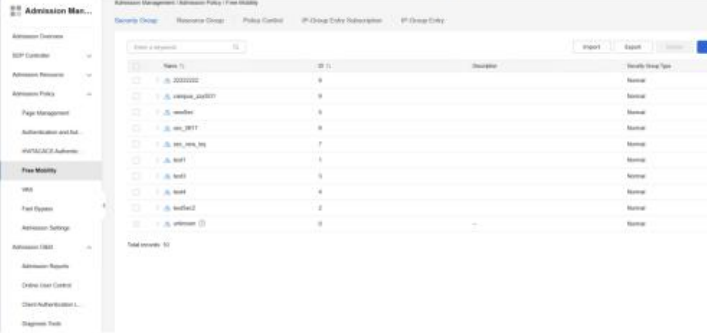


Página 23 (vinte e três), realização de testes da integração:

5 Test Cases

- 5.1 Interconnecting iMaster NCE-Campus with FortiManager
- 5.2 Reporting User Login and Logout Messages
- 5.3 Changing the Authorized Security Group
- 5.4 Communication Failure Between FortiManager and iMaster NCE-Campus



5.1 Interconnecting iMaster NCE-Campus with FortiManager

Test Scenario	Interconnecting iMaster NCE-Campus with FortiManager
Test Objective	To verify that iMaster NCE-Campus is successfully interconnected with FortiManager.
Test Procedure	<p>1. Configure the interconnection by referring to section 4.2. Expected result 1 is achieved.</p> <p>2. A security group is created and online users are generated on the controller.</p> 

Página 26 (vinte e seis), apresentação do relatório de resultados:

5.2 Reporting User Login and Logout Messages

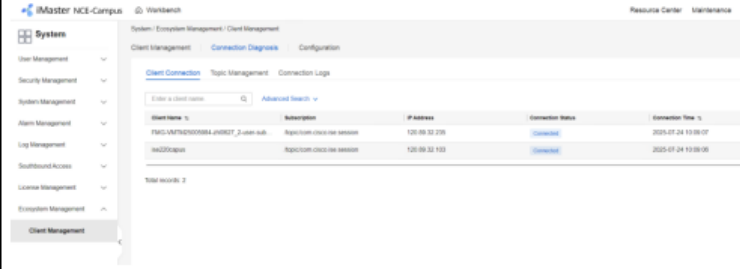
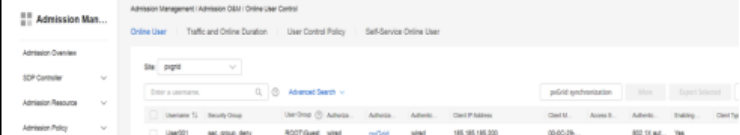
Test Scenario	Reporting new online users and offline users on iMaster NCE-Campus in real time
Test	To verify that new online users and offline users can be reported in real time on

Objective	iMaster NCE-Campus.
Test Procedure	<p>1. Configure security policies by referring to section 4.3.</p> <p>2. Add an online user on iMaster NCE-Campus and authorize the security group sec_group_permit (the security group has been synchronized to FortiManager). Expected result 1 is achieved.</p>  <p>3. Modify the security policy and the endpoint cannot access the network. Expected result 2 is achieved.</p> 

Página 32 (trinta e dois), simulação de falha na conexão entre soluções Huawei e Fortinet:

5.4 Communication Failure Between FortiManager and iMaster NCE-Campus

Test	Communication failure between FortiManager and iMaster NCE-Campus
------	---

Scenario	
Test Objective	To verify that the users who go online during the communication failure between FortiManager and iMaster NCE-Campus can be synchronized to FortiManager after the fault is rectified.
Test Procedure	<p>1. Simulate a communication failure between FortiManager and iMaster NCE-Campus.</p>  <p>2. Add an online user on iMaster NCE-Campus and authorize the security group. Rectify the fault. Expected result 1 is achieved.</p> 

Diante do exposto, comprova-se o atendimento ao item 4.8.5. do Anexo I – Especificação Técnica.

5) DO MÉRITO

Restou-se evidente que a Recorrente **TELESUL** teve como intuito tumultuar o processo, fazendo inúmeras alegações de supostos descumprimentos às exigências do Edital e TR pela Recorrida **3CORP**, o que ficou demonstrado ser improcedente, vez que comprovado o integral cumprimento as disposições do editalícias e legislação vigente.

Novamente, os pontos trazidos pela Recorrente **TELESUL** não passaram de meras alegações desprovidas e infundadas na tentativa de alterar o resultado do certamente para se beneficiar, bem como desacreditar a decisão da comissão de licitação deste estimado Órgão, o que não merece prosperar.

É pacífico na melhor doutrina pátria que, se por um lado a vinculação ao instrumento convocatório constitui princípio basilar das licitações, não menos verdadeiro é que tal vinculação é instrumental, constituindo ferramenta posta à disposição do Administrador, bem como dos interessados, para assegurar o fim que se busca obter, qual seja, a busca do melhor negócio para a Administração.

Ademais, em que pese a Recorrente tentar desclassificar a Recorrida **3CORP**, faz desvirtualizando a brilhante atuação deste i. Agente de Contratação e sua equipe, ao tentar fazer crer que houve violação ao Edital.

Outrossim, conforme dispõe o Edital, caso ainda reste alguma dúvida sobre os apontamentos, o Agente de Contratação e sua equipe ou autoridade superior poderá em qualquer fase do processo, realizar diligências que considerem necessárias e úteis para esclarecer ou complementar a instrução.

Como se vê, os argumentos do recurso administrativo da Recorrente **TELESUL** são protelatórios, já que desprovido de qualquer fundamento e elemento apto a modificar a decisão. Assim, demonstrando total competência da equipe deste Órgão ao analisar toda a documentação exigida em Edital. Uma vez que o Órgão aceitou e habilitou a proposta,

documentação jurídica e técnica, causando espanto que a licitante tente desacreditar a capacidade de análise do Agente de Contratação e sua equipe.

Ademais, ainda que remotamente, a desclassificação de uma proposta somente poderá ocorrer na verificação de erro que comprometa a execução do objeto, o que não se observa no presente caso. A tendência do direito tem sido a de relevar aspectos redundantes e formais que provoquem a desclassificação de empresas idôneas, destacamos:

“TC 000.175/95-1: Que no julgamento de contas e na fiscalização que lhe incumbe, o TCU decidirá não só quanto a legalidade e legitimidade, mas também sobre a economicidade dos atos de gestão praticados pelos responsáveis sujeitos à sua jurisdição (cf. art. 1º, § 1º, da Lei nº 8.443/92)”

Inquestionável que a alegação trazida é facilmente superada com a análise correta do Edital e Anexos, bem como documentos apresentados e das evidências apresentadas, não podendo de modo algum constituir motivo suficiente para reforma da decisão proferida.

Vale ressaltar que a Recorrente demonstra, nada mais do que um relutante inconformismo neste procedimento licitatório, o qual foi vencido pela Recorrida **3CORP** de acordo com os princípios constitucionais da legalidade, da impessoalidade, da moralidade, da publicidade e da eficiência (art. 37, CF).

Em virtude disso, a Recorrente tenta, por todos os meios, induzir esta r. comissão ao erro, tumultuando o procedimento licitatório, com o intuito de reverter a decisão exarada, o que não deve prosperar.

6) DA CONCLUSÃO

De qualquer forma, ante o exposto, evidencia-se que o pedido da empresa Recorrente **TELESUL não deve prosperar visto que a Recorrida 3CORP** atende plenamente aos requisitos do Edital e que o Agente de Contratação agiu no mais estrito cumprimento das regras Editalícias, procedendo com lisura o processo.

7) DO PEDIDO

Por todo o exposto, requer a **3CORP**, ora Recorrida, que sejam apreciadas as contrarrazões para confirmar a decisão prolatada no processo licitatório, **negando provimento ao recurso** da Recorrente e mantendo/confirmando a decisão que classificou a empresa Recorrida **3CORP** como vencedora deste certame licitatório.

Caso contrário solicitamos que tal decisão seja submetida à autoridade superior competente.

Termos em que, pede deferimento.

Santana de Parnaíba, 07 de abril de 2026.

RODRIGO ROSÁRIO CAVALCANTE

DIRETOR COMERCIAL

RG [REDACTED] / CPF [REDACTED]

3CORP TECHNOLOGY INFRAESTRUTURA DE TELECOM LTDA.