



PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
PROCESSO Nº 2020.0000.604.5301  
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

---

**EMPRESA: COMPWIRE INFORMATICA LTDA**  
**FABRICANTE: HUAWEI**

**SEDUC/GO**  
**CADERNO DE TESTES**

Itens que não utilizam configuração como comprovação:

**5.6 Ponto de Acesso sem fio Tipo 1**

5.6.2.1 Possuir capacidade de montagem em parede e teto, devendo ser fornecidos todos os acessórios necessários para estas montagens;

Comprovação visual – Documentação complementar:

Super Tópico - Installing Indoor Settled Aps

[https://support.huawei.com/hedex/hdx.do?docid=EDOC1100210441&id=EN-US\\_TOPIC\\_0000001408815222&lang=en](https://support.huawei.com/hedex/hdx.do?docid=EDOC1100210441&id=EN-US_TOPIC_0000001408815222&lang=en)

Understanding Mounting Brackets e Installation Scenarios

[https://support.huawei.com/hedex/hdx.do?docid=EDOC1100210441&id=EN-US\\_TOPIC\\_0000001458975033&lang=en](https://support.huawei.com/hedex/hdx.do?docid=EDOC1100210441&id=EN-US_TOPIC_0000001458975033&lang=en)

Determining the Installation Position

[https://support.huawei.com/hedex/hdx.do?docid=EDOC1100210441&id=EN-US\\_TOPIC\\_0000001408815234&lang=en](https://support.huawei.com/hedex/hdx.do?docid=EDOC1100210441&id=EN-US_TOPIC_0000001408815234&lang=en)

5.6.2.2 Deve suportar a utilização de sistema antifurto do tipo Kensington ou similar;

Comprovação visual - Documentação complementar:

Hardware Information (AirEngine 5761-11) - Ports

[https://support.huawei.com/hedex/hdx.do?docid=EDOC1100210441&id=EN-US\\_CONCEPT\\_0000001388948464&lang=en](https://support.huawei.com/hedex/hdx.do?docid=EDOC1100210441&id=EN-US_CONCEPT_0000001388948464&lang=en)

Anti-Theft e Removal

[https://support.huawei.com/hedex/hdx.do?docid=EDOC1100210441&id=EN-US\\_TOPIC\\_0000001458855053&lang=en](https://support.huawei.com/hedex/hdx.do?docid=EDOC1100210441&id=EN-US_TOPIC_0000001458855053&lang=en)

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
PROCESSO Nº 2020.0000.604.5301  
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

---

5.6.2.3 Deve acompanhar todos os recursos necessários para não permitir a retirada do equipamento por pessoas não autorizadas (podendo ser utilizado cabo de segurança com chave ou similar);

Equipamento de segurança fornecido junto a proposta - Documentação complementar:

Anti-Theft e Removal

[https://support.huawei.com/hedex/hdx.do?docid=EDOC1100210441&id=EN-US\\_TOPIC\\_0000001458855053&lang=en](https://support.huawei.com/hedex/hdx.do?docid=EDOC1100210441&id=EN-US_TOPIC_0000001458855053&lang=en)

5.6.2.6 Deve possuir um ou mais Leds indicadores de estado de operação;

Comprovação visual – Documentação complementar:

Product description – Indoor Settled AP - AirEngine 5761-11 – Hardware information – Indicators e Buttons

[https://support.huawei.com/hedex/hdx.do?docid=EDOC1100210441&id=EN-US\\_CONCEPT\\_0000001388948464&lang=en](https://support.huawei.com/hedex/hdx.do?docid=EDOC1100210441&id=EN-US_CONCEPT_0000001388948464&lang=en)

5.6.2.7 Não deve possuir antenas aparentes, que sejam rosqueáveis, evitando a remoção das antenas;

Product description – Indoor Settled AP - AirEngine 5761-11 – Hardware information – Appearance

[https://support.huawei.com/hedex/hdx.do?docid=EDOC1100210441&id=EN-US\\_CONCEPT\\_0000001388948464&lang=en](https://support.huawei.com/hedex/hdx.do?docid=EDOC1100210441&id=EN-US_CONCEPT_0000001388948464&lang=en)

## **5.7 Ponto de Acesso sem fio Tipo 2**

5.7.2.1 Possuir capacidade de montagem em parede, teto e mastro, devendo ser fornecidos todos os acessórios necessários para estas montagens;

5.7.2.2 Deve acompanhar kit para montagem em parede, o kit deve ter recursos necessários para não permitir a retirada do equipamento por pessoas não autorizadas (podendo ser utilizado cabo de segurança com chave ou similar);

5.7.2.4 Possui grau de proteção mínimo IP67, outdoor;



PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
PROCESSO Nº 2020.0000.604.5301  
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

---

Comprovação documental

Product description – Outdoor AP - AirEngine 6760R-51 – Hardware information – Technical Specifications

[https://support.huawei.com/hedex/hdx.do?docid=EDOC1100210441&id=EN-US\\_CONCEPT\\_0000001439108181&lang=en](https://support.huawei.com/hedex/hdx.do?docid=EDOC1100210441&id=EN-US_CONCEPT_0000001439108181&lang=en)

Ingress protection level (dustproof/waterproof) - IP68

5.7.2.7 Deve possuir um ou mais Leds indicadores de estado de operação;

Comprovação visual – Documentação complementar:

Product description – Outdoor AP - AirEngine 6760R-51 – Hardware information – Appearance

[https://support.huawei.com/hedex/hdx.do?docid=EDOC1100210441&id=EN-US\\_CONCEPT\\_0000001439108181&lang=en](https://support.huawei.com/hedex/hdx.do?docid=EDOC1100210441&id=EN-US_CONCEPT_0000001439108181&lang=en)

Itens que necessitam de configuração:

**Access point sem fio, funcionalidades básicas**

**PoE power capacity**

5.6.2.5 Possuir capacidade de alimentação PoE 802.3af, 802.3at ou 802.3bt;


5.7.2.5 Possuir capacidade de alimentação PoE 802.3af, 802.3at ou 802.3bt;

5.8.1 Possuir capacidade de fornecer alimentação PoE 802.3af, 802.3at ou 802.3bt;

5.8.2 Deve possuir capacidade de energizar no mínimo 2 Access Point Tipo 2 e 10 Access Point Tipo 1 ou 12 Access Point Tipo 1 simultaneamente;

5.8.3 O Switch deve ser capaz de alimentar os Access Points Tipo 1 sem a necessidade de componentes adicionais;

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

<b>Item de teste</b>	<b>Capacidade de alimentação PoE</b>
<b>Objetivo do teste</b>	Validar que o access point sem fio esteja de acordo com 802.3 bt/at
<b>Configuração de teste</b>	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
<b>Procedimento de teste</b>	1) Verifique o estado do AP quando alimentado no modo 802.3bt. Resultado esperado 1; 2) Mude o modo de alimentação do AP para o modo 802.3at. Resultado esperado 1;
<b>Resultado esperado</b>	1) O AP está operacional; o status de energia é mostrado. 2) O AP está operacional; o status de energia é mostrado.
<b>Resultado</b>	

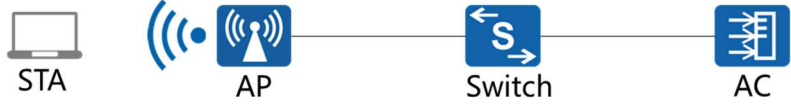
### Negociação de portas

5.6.3.1 Possuir no mínimo 1 interface 10/100/1000 Base-T ou superior;

5.7.3.1 Possuir no mínimo 1 interface 10/100/1000 Base-T ou superior;

<b>Item de teste</b>	<b>Port rate negotiation</b>
----------------------	------------------------------


**PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO**  
**PROCESSO Nº 2020.0000.604.5301**  
**INTERESSADO: GERÊNCIA DE SUPORTE DE REDES**

<b>Objetivo do teste</b>	Validar que o access point sem fio tenha pelo menos 1 interface 10/100/1000 Base-T ou acima;
<b>Configuração de teste</b>	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
<b>Procedimento de teste</b>	1) Verifique a velocidade da portacabeada no AP. Resultado esperado 1;
<b>Resultado esperado</b>	1) O AP está operacional; a velocidade da porta é mostrada.
<b>Resultado</b>	

### Múltiplas VLANs

5.6.3.2 Suportar VLANs conforme o padrão IEEE 802.1Q;

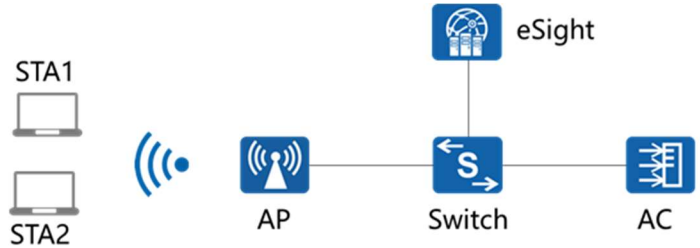
5.7.3.2 Suportar VLANs confirme o padrão IEEE 802.1Q;

<b>Item de teste</b>	<b>Múltiplas VLANs</b>
<b>Objetivo do teste</b>	Validar que o access point sem fio suporte VLANs de acordo com o padrão IEEE 802.1Q; e que suporte aciação de pelo menos 16 (Dezesseis) VLANs;
<b>Configuração de teste</b>	Topologia da rede: 

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

	Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
<b>Procedimento de teste</b>	1) Configure ac corretamente, Configurar no AP o SSID “SSID-Temp1” usando uma determinada vlan. Capture o pacote viacabo. Resultado esperado 1; 2) Crie 16 VLANs e add use them as service vlan for SSIDs.
<b>Resultado esperado</b>	1) O pacote mostra a marcação de vlan 802.1q. 2) 16 VLANs estão disponíveis no AP.
<b>Resultado</b>	

**Sistema de WLAN suporta a função de SNMP**

<b>Item de teste</b>	WLAN system supports SNMP function
<b>Objetivo do teste</b>	Validar que o sistema de WLAN suporta a função de SNMP
<b>Configuração de teste</b>	Topologia da rede:  <p>Condições iniciais:</p> 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
<b>Procedimento de teste</b>	1) Habilite a função SNMP na WAC, 2) Configure NMS para gerenciar a WAC;


PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

	3) Determine um evento (por exemplo: AP fica online ou fica offline). Resultado esperado 1.		
<b>Resultado esperado</b>	1) NMS gerencia ac com sucesso; 2) Verifica-se informação de alarme no NMS.		
<b>Resultado</b>			
<b>Observação</b>			
<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	

### Layer 2 CAPWAP AC Discovery | Descoberta de AC por CAPWAP na camada 2

5.6.3.6. Deve implementar cliente DHCP, para configuração automática de rede;

5.7.3.6. Deve implementar cliente DHCP, para configuração automática de rede;

<b>Item de teste</b>	Layer 2 CAPWAP WAC Discovery
<b>Objetivo do teste</b>	Validar que o Sistema WLAN suporta descoberta da AC por CAPWAP na camada 2
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <p>3) Todos os dispositivos funcionando normalmente</p> <p>4) Montar o ambiente de teste de acordo com a topologia acima</p>
<b>Procedimento de teste</b>	3) Verifique o estado do AP na AC antes que o AP seja ligado. Resultado esperado 1;


**PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO**  
**PROCESSO Nº 2020.0000.604.5301**  
**INTERESSADO: GERÊNCIA DE SUPORTE DE REDES**

	4) Configure o AP, switch e AC: o AP obtém endereço IP do servidor DHCP ( o Switch atua como um servidor DHCP para atribuir um endereço IP ao AP), o AP e ac estão na mesma subrede;  5) Verifique o estado do AP após um tempo. Resultado esperado 2.		
<b>Resultado esperado</b>	1) O AP não aparece como online na AC;  5) O AP está online;		
<b>Resultado</b>			
<b>Observação</b>			
<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	

**Layer 3 CAPWAP ac Discovery (DHCP Option 43) | Descoberta de AC por CAPWAP na camada 3 usando DHCP Option 43**

5.6.3.6. Deve implementar cliente DHCP, para configuração automática de rede;

5.7.3.6. Deve implementar cliente DHCP, para configuração automática de rede;

<b>Item de teste</b>	Descoberta de WAC por CAPWAP na camada 3 usando DHCP Option 43
<b>Objetivo do teste</b>	Validar que o Sistema WLAN suporta Descoberta de AC por CAPWAP na camada 3 usando DHCP Option 43
<b>Configuração de teste</b>	Topologia da rede:  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>




PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Verifique o estado do AP na AC antes que o AP conecte ao Switch (PoE Switch). Resultado esperado 1;</li> <li>2) Configure o Switch para operar como um servidor DHCP para atribuir endereço IP ao AP. A AC e o AP estão em redes distintas;</li> <li>3) Configure a funcionalidade Option43 no servidor DHCP, seu valor deve ser o endereço IP da AC;</li> <li>4) Conecte o AP ao Switch, após alguns instantes, verifique o estado do AP. Resultado esperado 2.</li> </ol>		
<b>Resultado esperado</b>	<ol style="list-style-type: none"> <li>1) Não há AP online na AC;</li> <li>2) O AP está online.</li> </ol>		
<b>Resultado</b>			
<b>Observação</b>	<p>Exp. Configure o endereço 192.168.200.2 na AC, o Option 43 correspondente é 030D3139322E3136382E3230302E32, os primeiros dois caracteres "03" é o campo fixo, o hexadecimal 0D (correspondente ao decimal 13) representa o número de endereços IP. O valor hexadecimal 31 corresponde ao caractere ASCII "1", o valor hexadecimal 32 corresponde ao caractere ASCII "2", e assim por diante. O valor hexadecimal 2E corresponde ao caractere ASCII ponto ("."). Se for usado um equipamento Huawei como servidor DHCP, pode-se usar o comando "[L3-Switch-vlanif100] servidor DHCP option 43 sub-option 2 ip-endereço xxx.xxx.xxx.xxx" para configurar o endereço IP da AC.</p>		
<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	

**Layer 3 CAPWAP AC Discovery (static IP address) | Descoberta de AC por CAPWAP na camada 3 usando IP estático**

<b>Item de teste</b>	Layer 3 CAPWAP AC Discovery (static Endereço IP)
<b>Objetivo do teste</b>	Validar que o Sistema WLAN suporta descoberta de AC por CAPWAP na camada 3 usando IP estático

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

<b>Configuração de teste</b>	<p>Topologia da rede:</p> <div style="text-align: center;">  </div> <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>		
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Verifique o estado do AP nac antes que o AP conecte ao Switch. Resultado esperado 1;</li> <li>2) Conecte o AP ao Switch, configure o AP e ac para operar nacamada 2;</li> <li>3) Configure manualmente o endereço IP, gateway, IP da AC no AP antes de conectá-lo ao Switch;</li> <li>4) Garanta que a rede entre c e AP esteja funcionando bem;</li> <li>5) Verifique o estado do AP. Resultado esperado 2.</li> </ol>		
<b>Resultado esperado</b>	<ol style="list-style-type: none"> <li>1) Não há AP online;</li> <li>2) O AP está online;</li> </ol>		
<b>Resultado</b>			
<b>Observação</b>			
<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	


Segurança WLAN

**WLAN Security Policy (support WEP/WPA/WPA2)**

5.6.5 Implementar no mínimo as opções WPA2, WPA3, 802.1X;

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

5.7.5 Implementar no mínimo as opções WPA2, WPA3, 802.1X;

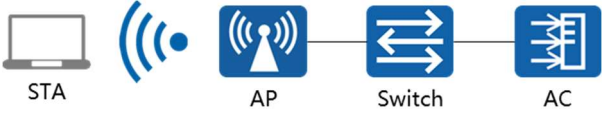
<b>Item de teste</b>	Políticas de segurança da rede WLAN (suporte aos protocolos WEP/WPA/WPA2)		
<b>Objetivo do teste</b>	Validar que o sistema WLAN suporta políticas de segurança ( WEP/WPA/WPA2)		
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>		
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Configure ac corretamente, o AP deve propagar três SSIDs: "SSID-WEP", "SSID-WPA-PSK", "SSID-WPA2-PSK", e as respectivas políticas de segurança devem ser WEP, WPA-PSK e WPA2-PSK;</li> <li>2) O dispositivo cliente (STA) conecta-se aos SSIDs "SSID-WEP", "SSID-WPA-PSK", "SSID-WPA2-PSK", respectivamente, usando a senha correta e consegue pingar o gateway. Resultado esperado 1.</li> </ol>		
<b>Resultado esperado</b>	1) O dispositivo cliente (STA) conecta-se aos três SSIDs e pinga o gateway com sucesso.		
<b>Resultado</b>			
<b>Observação</b>			
<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

**WPA3-SAE Autenticação**

5.6.5 Implementar no mínimo as opções WPA2, WPA3, 802.1X;

5.7.5 Implementar no mínimo as opções WPA2, WPA3, 802.1X;

<b>Item de teste</b>	Autenticação WPA3-SAE
<b>Objetivo do teste</b>	Validar que o Sistema WLAN suporta autenticação WPA3-SAE
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos estão funcionando normalmente.</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima.</li> <li>3) O dispositivo cliente (STA) suporta autenticação WPA3-SAE.</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Configure o serviço WLAN na AC: "SSID-WPA3-SAE", a política de segurança é autenticação WPA3-SAE, a qual é entregue ao AP;</li> <li>2) O dispositivo cliente (STA) conecta-se ao "SSID-WPA3-SAE" e efetua login com usuário e senha corretos. Resultado esperado 1;</li> <li>3) Verifique o método de autenticação do dispositivo cliente (STA) na AC. Resultado esperado 2.</li> </ol>
<b>Resultado esperado</b>	<ol style="list-style-type: none"> <li>1) O dispositivo cliente (STA) consegue conectar-se ao "SSID-WPA3-SAE", recebe endereço IP, e pinga o gateway com sucesso;</li> <li>2) O método de autenticação usado pelo dispositivo cliente (STA) é o WPA3-SAE.</li> </ol>

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

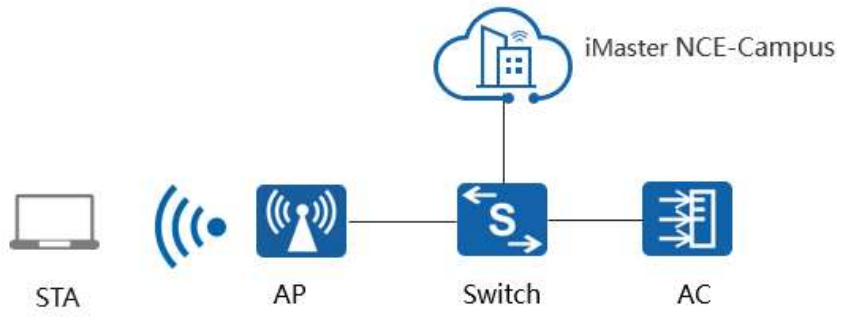
<b>Resultado</b>			
<b>Observação</b>			
<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	

### Autenticação 802.1x

5.6.5 Implementar no mínimo as opções WPA2, WPA3, 802.1X;

5.7.5 Implementar no mínimo as opções WPA2, WPA3, 802.1X;

5.10.26 Implantar autenticação de dispositivos e usuários via 802.1x, Web Portal e endereço MAC na rede sem fio;

<b>Item de teste</b>	Autenticação 802.1x
<b>Objetivo do teste</b>	Validar que o Sistema WLAN suporta Autenticação 802.1x
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

<b>Procedimento de teste</b>	1) Configure a autenticação 802.1x na AC WLAN: o SSID é “SSID-Dot1x”, use o servidor externo Radius: iMaster NCE-Campus. O AP implementa isso; 2) Configure autenticação 802.1x no servidor de autenticação ( iMaster NCE-Campus); 3) o dispositivo cliente (STA) conecta-se ao “SSID-Dot1x”, usando usuário e senhacorretos. Resultado esperado 1.		
<b>Resultado esperado</b>	1) o dispositivo cliente (STA) conecta-se ao “SSID-Dot1x” e pinga o gateway com sucesso.		
<b>Resultado</b>			
<b>Observação</b>			
<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	

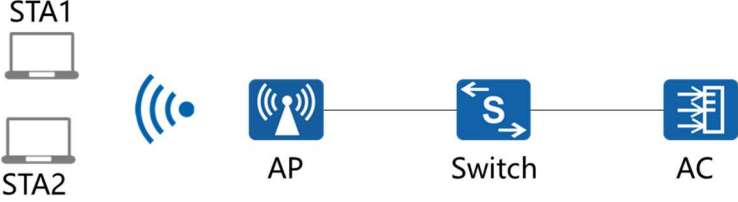
### Autenticação WPA/WPA2-PPSK

5.6.6 Implementar chave de compartilhada exclusiva (Exemplo: PPSK, Identity PSK, ePSK, MPSK, DPSK ou similar do fabricante)

5.7.6 Implementar chave de compartilhada exclusiva (Exemplo: PPSK, Identity PSK, ePSK, MPSK, DPSK ou similar do fabricante)

<b>Item de teste</b>	Autenticação WPA/WPA2-PPSK
<b>Objetivo do teste</b>	Validar que o Sistema WLAN suporta Autenticação WPA/WPA2-PPSK
<b>Configuração de teste</b>	Topologia da rede:

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

	<div style="text-align: center;">  <p>STA1 STA2</p> <p>AP</p> <p>Switch</p> <p>AC</p> </div> <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<p style="text-align: center;"><b>Procedimento de teste</b></p>	<ol style="list-style-type: none"> <li>1) Configure o serviço WLAN na AC: SSID é “SSID- WPA2-PPSK”, a política de segurança é WPA2-PPSK. O AP implementa esse sinal;</li> <li>2) Configure o parâmetro PPSK na AC: uma PPSK é permitida por um dispositivo de acesso, exporte a senha correspondente;</li> <li>3) o dispositivo cliente 1 (STA1) conecta-se ao “SSID- WPA2-PPSK”, insira a senha gerada no passo 2. Resultado esperado 1;</li> <li>4) o dispositivo cliente 1 (STA1) conecta-se ao “SSID- WPA2-PPSK”, insira a senha (diferente) gerada no passo 2. Resultado esperado 2</li> <li>5) o dispositivo cliente 2 (STA2) conecta-se ao “SSID- WPA2-PPSK”, insira a mesma senha que o dispositivo cliente 1 (STA1) usou. Resultado esperado 3;</li> </ol>
<p style="text-align: center;"><b>Resultado esperado</b></p>	<ol style="list-style-type: none"> <li>1) o dispositivo cliente 1 (STA1) conectou-se à rede sem fio com sucesso utilizando a senha PPSK exportada e pinga o gateway com sucesso;</li> <li>2) o dispositivo cliente 2 (STA2) conectou-se à rede sem fio com sucesso;</li> <li>3) o dispositivo cliente 2 (STA2) falha ao tentar se conectar à rede sem fio.</li> </ol>
<p style="text-align: center;"><b>Resultado</b></p>	

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

<b>Observação</b>			
<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	

### Radio


#### Fluxo 2.4Ghz e 5Ghz

5.6.7.1 Fluxo 2.4Ghz e 5Ghz: no mínimo 2x2

5.6.7.4 Implementar funcionamento simultâneo em 2,4GHz e 5GHz;

5.7.7.1 Fluxo 5Ghz: 4x4

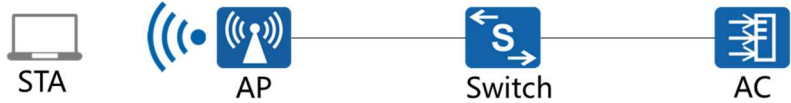
5.7.7.4 Implementar funcionamento simultâneo em 2,4GHz e 5GHz;

<b>Item de teste</b>	<b>Fluxo 2.4Ghz e 5Ghz</b>
<b>Objetivo do teste</b>	Validar que o AP 5761-11 tenha fluxo nas frequências 2.4Ghz e 5Ghz: em pelo menos 2x2; 6760r-51 tenha fluxo na frequência 5Ghz em 4x4
<b>Configuração de teste</b>	<p>Topologia da rede:</p> <div style="text-align: center;">  <p>STA      AP      Switch      AC</p> </div> <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	1) Verifique os spatial streams no AP. Resultado esperado 1;
<b>Resultado esperado</b>	1) AP está online; 5761-11 tem fluxos nas frequências 2.4Ghz e 5Ghz em pelo menos 2x2; 6760r-51 tem fluxo na frequência 5Ghz em 4x4
<b>Resultado</b>	



PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES


**Maximum access user | Máximo de usuários simultâneos**

Item de teste	Máximo de usuários simultâneos
<b>Objetivo do teste</b>	Validar que o access point sem fio suporta pelo menos 512 clientes por unidade de AP.
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	1) Configure ac corretamente, o AP propaga o SSID: "SSID-Temp"; os terminais conectam-se à rede sem fio.
<b>Resultado esperado</b>	2) O AP está online; mais de 512 terminais conseguem conectar-se à rede e permanecem conectados ao mesmo tempo.
<b>Resultado</b>	

**Bluetooth Low-Energy (BLE) radio | Rádio Bluetooth de baixo consumo energético (BLE)**

<b>Item de teste</b>	<b>Bluetooth Low-Energy (BLE) radio   Rádio Bluetooth de baixo consumo energético</b>
----------------------	---

**PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO**  
**PROCESSO Nº 2020.0000.604.5301**  
**INTERESSADO: GERÊNCIA DE SUPORTE DE REDES**

<b>Objetivo do teste</b>	<b>Validar que o a access point sem fio suporte rádio Bluetooth de baixo consumo energético (BLE)</b>
<b>Configuração de teste</b>	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
<b>Procedimento de teste</b>	1) Configure ac corretamente, AP fica online nac
<b>Resultado esperado</b>	1) O AP fica online; O funcionamento do BLE pode ser verificado.
<b>Resultado</b>	


**Funcionamento simultâneo em 2.4GHz e 5GHz;**

5.6.7.4 Implementar funcionamento simultâneo em 2,4GHz e 5GHz;

5.7.7.4 Implementar funcionamento simultâneo em 2,4GHz e 5GHz;

<b>Item de teste</b>	<b>Simultaneous operation at 2.4GHz e 5GHz;</b>
----------------------	---

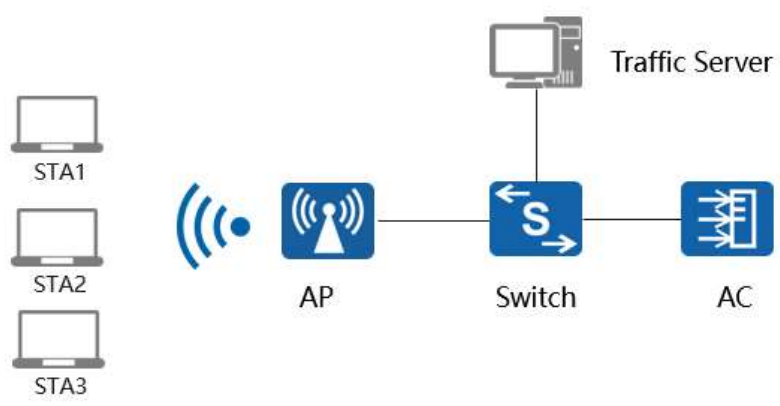
PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

<b>Objetivo do teste</b>	<b>Validar que o Sistema WLAN suporta funcionamento simultâneo em 2,4GHz e 5GHz</b>
<b>Configuração de teste</b>	<p>Topologia da rede:</p> <div style="text-align: center;">  </div> <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Configure ac corretamente, AP propaga dois SSIDs: "SSID-2.4G" no rádio de 2.4GHz, "SSID-5G," no rádio de 5 GHz.</li> <li>2) Escanear a rede sem fio no dispositivo cliente (STA). Resultado esperado 1;</li> <li>2) Conecte o dispositivo cliente 1 (STA1) ao "SSID-Temp1", o dispositivo cliente 2 (STA2) ao "SSID-Temp2", o dispositivo cliente 3 (STA3) ao "SSID-Temp3", pingar o gateway. Resultado esperado 2. A figura da topologia não mostra 3 STAs</li> </ol>
<b>Resultado esperado</b>	<ol style="list-style-type: none"> <li>1) Os SSIDs "SSID-2.4G" no rádio de 2.4GHz e "SSID-5G" no rádio de 5 GHz podem ser descobertos nos dispositivos clientes (STAs);</li> <li>2) Os dispositivos clientes (STAs) conectam-se aos "SSID-2.4G", "SSID-5G" respectivamente.</li> </ol>
<b>Resultado</b>	
<b>Observação</b>	

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	
------------------------------	--	---------------------------------	--

**Performance MU-MIMO**

<b>Item de teste</b>	Teste de Performance MU-MIMO
<b>Objetivo do teste</b>	Teste a performance do WiFi6 MU-MIMO.
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos clientes de STA1 a STAn suportam WiFi6 (recomendado n=3)</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Configure ac corretamente, AP propaga o SSID: "SSID-TEMP" no rádio 5GHz;</li> <li>2) Os dispositivos clientes conectam-se ao "SSID-TEMP". Tente pingar a partir do PC de Teste para todas os dispositivos clientes (STAs), e verifique a velocidade física. Resultado esperado 1;</li> <li>3) Utilizando o servidor de tráfego, testar o fluxo de dados entre o PC de Teste e os dispositivos clientes, continuar por 2 minutos,</li> </ol>

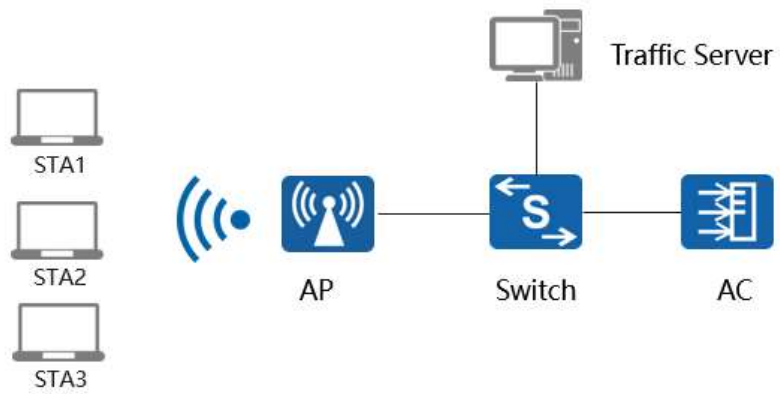
PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
PROCESSO Nº 2020.0000.604.5301  
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

	<p>registrar o resultado 1.</p> <p>4) Habilite a função MU-MIMO e associar novamente o SSID dos utilizadores: "SSID-TEMP". Use o servidor de tráfego para testar o fluxo de dados entre o PC de Teste e os dispositivos clientes, continuar por 2 minutos, registrar o resultado. Esperar o resultado 2.</p>		
<b>Resultado esperado</b>	<p>1) Os dispositivos clientes conectam-se ao "SSID-TEMP" e o PC de Teste pinga o usuário com sucesso.</p> <p>2) Os dispositivos clientes conectam-se ao "SSID-TEMP" e o PC de Teste pinga o usuário com sucesso. O throughput total fica acima que o resultado 1.</p>		
<b>Resultado</b>			
<b>Observação</b>			
<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	

**OFDMA**

<b>Item de teste</b>	OFDMA
<b>Objetivo do teste</b>	Validar que o AP suporta OFDMA
<b>Configuração de teste</b>	Topologia da rede:


PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

	 <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>3) Todos os dispositivos de (STA1) ao (STAn) suportam WiFi6 (recomendado n=3)</li> <li>4) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<p><b>Procedimento de teste</b></p>	<ol style="list-style-type: none"> <li>5) Configure ac corretamente, AP propaga o SSID: “SSID-TEMP” no rádio 5G;</li> <li>6) Os dispositivos de (STA1) ao (STAn) conectam ao “SSID-TEMP”. Tentar ping do PC de Teste a todos os dispositivos (STAs), e e verificar a velocidade física. Resultado esperado 1;</li> <li>7) Utilizando o servidor de tráfego, testar a banda de tráfego entre o PC de teste e STA1 a STAn, continuar por 2 minutos, resultado 1.</li> <li>8) Ativar a função MU-MIMO e associar novamente o SSID dos utilizadores: "SSID-TEMP". Utilizar o servidor de tráfego para testar a banda de tráfego entre o PC de teste e STA1~STAn. Continuar 2 minutos, capturar o pacote. Esperar o resultado 2.</li> </ol>
<p><b>Resultado esperado</b></p>	<ol style="list-style-type: none"> <li>3) Os dispositivos (STA1) ao (STAn) conectam-se ao “SSID-TEMP” e PC de Teste pingacada usuário com sucesso</li> <li>4) STA1~STAn ligam ao "SSID-TEMP" e o PC de teste pingacada usuário com êxito. O quadro Trigger MU-BAR pode ser identificado.</li> </ol>

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

<b>Resultado</b>			
<b>Observação</b>			
<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	

**802.11a/b/g/n/ac/ax multiple radio mode**


<b>Item de teste</b>	802.11a/b/g/n/ac/ax multiple radio mode
<b>Objetivo do teste</b>	Validar que o Sistema WLAN suporta 802.11a/b/g/n/ac/ax modo rádio múltiplo.
<b>Configuração de teste</b>	<p>Topologia da rede:</p> <div style="text-align: center;">  <p>STA      AP      Switch      AC</p> </div> <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Configurar corretamente ac, o AP fornece SSID: "SSID-Temp-2.4G" na banda de 2,4 GHz cujo modo de rádio é 802.11b/g/n e "SSID-Temp-5G" na banda de 5 GHz cujo modo de rádio é 802.11a/n/ac/ax;</li> <li>2) STA com adaptador sem fios 11b, STA com adaptador sem fios 11g, STA com adaptador sem fios 11n, STA com adaptador sem fios 11ax, ligam-se a "SSID-Temp-2.4g", respetivamente. Resultado esperado 1;;</li> <li>3) O STA com adaptador sem fios 11ax, STA com adaptador sem fios 11ac, STA com adaptador sem fios 11n ligam-se a "SSID-Temp-5g", respetivamente. Resultado esperado 2.</li> </ol>

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

<b>Resultado esperado</b>	1) A STA com adaptador sem fios 11b, a STA com adaptador sem fios 11g, a STA com adaptador sem fios 11n e a STA com adaptador sem fios 11ax ligam-se com êxito ao "SSID-Temp-2.4G"; 2) A STA com o adaptador sem fios 11ax, a STA com o adaptador sem fios 11ac e a STA com o adaptador sem fios 11n ligam-se ao "SSID-Temp-5G" com êxito.		
<b>Resultado</b>			
<b>Observação</b>	Se não houver STAs suficientes, é possível alterar o tipo de rádio do adaptador sem fios.		
<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	

### Multiplas SSIDs

5.6.7.8 Capacidade de implementar no mínimo 16 SSID;

<b>Item de teste</b>	Multi-SSIDs
<b>Objetivo do teste</b>	Validar que o Sistema WLAN suporta pelo menos 16 SSIDs
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>




PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

<b>Procedimento de teste</b>	1) Configurar corretamente ac, o AP fornece <b>Dezesseis</b> SSIDs: "SSID-Temp1", "SSID-Temp2", "SSID-Temp3"... "SSID-Temp16". 2) Escanear a rede sem fio no dispositivo STA. Resultado esperado 1; 3) Ligar STA1 a "SSID-Temp1", STA2 a "SSID-Temp2", STA3 a "SSID-Temp3" ... "SSID-Temp15", Pingar o gateway. Resultado esperado 2.		
<b>Resultado esperado</b>	1) Os sinais "SSID-Temp1", "SSID-Temp2", "SSID-Temp3" ... "SSID-Temp15" podem ser detectados nas STAs; 2) STA1, STA2, STA3 ligam-se a "SSID-Temp1", "SSID-Temp2", "SSID-Temp3", respetivamente.		
<b>Resultado</b>			
<b>Observação</b>			
<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	

### SSID oculto

5.6.7.9 Deve permitir habilitar e desabilitar a divulgação do SSID;

5.7.7.9 Deve permitir habilitar e desabilitar a divulgação do SSID;

<b>Item de teste</b>	SSID oculto
<b>Objetivo do teste</b>	Validar que o Sistema WLAN suporta SSID função oculto.
<b>Configuração de teste</b>	Topologia da rede: <div style="text-align: center;">  <p>STA      AP      Switch      AC</p> </div> Condições iniciais:

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

	1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima		
<b>Procedimento de teste</b>	1) Configure the ac corretamente, AP divulga SSID: "SSID-Temp"; 2) Analisar a rede sem fios na STA. Resultado esperado 1; 3) Conexão STA a "SSID-Temp". Resultado esperado 2; 4) Ativar a função SSID oculto no AC e aplicar a "SSID-Temp"; 5) Repetir a etapa 2. Resultado esperado 3; 6) Adicione manualmente "SSID-Temp" no adaptador sem fios da STA e, em seguida, faça ping à gateway após algum tempo. Resultado esperado 4.		
<b>Resultado esperado</b>	1) O "SSID-Temp" pode ser descoberto pelo STA; 2) A STA liga-se ao "SSID-Temp" e faz ping ao gateway com êxito; 3) O "SSID-Temp" não pode ser descoberto pelo STA; 4) A STA liga-se a "SSID-Temp" com êxito depois de adicionar manualmente a configuração SSID no adaptador sem fios.		
<b>Resultado</b>			
<b>Observação</b>			
<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	

**Calibração automática de rádios - Alocação dinâmica de canais e ajuste de potência**

**DCA &TPC**

5.6.7.10 Deve possuir capacidade de selecionar automaticamente o canal de transmissão;

5.6.7.11 Deve permitir o ajuste dinâmico de nível de potência de modo a otimizar o tamanho

**PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO**  
**PROCESSO Nº 2020.0000.604.5301**  
**INTERESSADO: GERÊNCIA DE SUPORTE DE REDES**

da célula de RF (rádio frequência) conforme as características do ambiente, evitando intervenção manual;

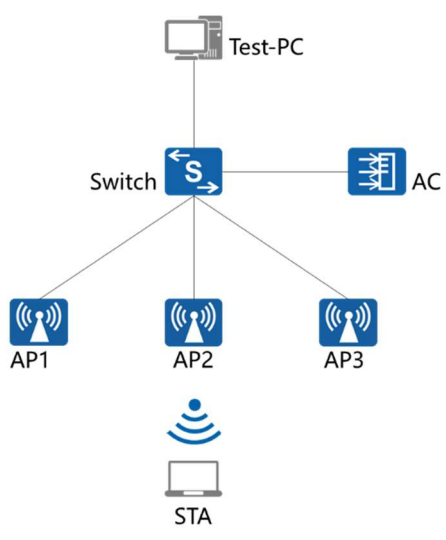
5.7.7.10 Deve possuir capacidade de selecionar automaticamente o canal de transmissão;

5.7.7.11 Deve permitir o ajuste dinâmico de nível de potência de modo a otimizar o tamanho da célula de RF (rádio frequência) conforme as características do ambiente, evitando intervenção manual;

5.10.19 Na ocorrência de inoperância de um Ponto de Acesso, a solução deverá ajustar automaticamente a potência dos Pontos de Acesso adjacentes, de modo a prover a cobertura da área não assistida;

5.10.20 Ajustar automaticamente a utilização de canais de modo a otimizar a cobertura de rede de acordo com as condições de RF;

5.10.21 Detectar interferência e ajustar parâmetros de RF, evitando problemas de cobertura de RF de forma automática;

<b>Item de teste</b>	Calibração de Rádio
<b>Objetivo do teste</b>	Validar que o Sistema WLAN suportacalibração de rádio
<b>Teste environment</b>	<p>Topologia da rede:</p>  <pre> graph TD     Test-PC --- Switch     Switch --- AC     Switch --- AP1     Switch --- AP2     Switch --- AP3     STA --- AP1             </pre> <p>Condições iniciais:</p>

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
PROCESSO Nº 2020.0000.604.5301  
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES


	1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima		
<b>Procedimento de teste</b>	1) Configure a AC corretamente, AP1, AP2, AP3 divulgam o SSID: "SSID-Temp"; 2) Verifique a informação do rádio AP. Resultado esperado 1; 3) Habilite a função Radio Calibration; 4) Repetir o passo 2. Resultado esperado 2;;		
<b>Resultado esperado</b>	1) Registrar informações de rádio sobre todos os APs; 2) O canal AP e a potência de trânsito foram ajustados de forma dinâmica.		
<b>Resultado</b>			
<b>Observação</b>			
<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	

#### Alteração da potência de transmissão

5.6.7.11 Deve permitir o ajuste dinâmico de nível de potência de modo a otimizar o tamanho da célula de RF (rádio frequência) conforme as características do ambiente, evitando intervenção manual;

5.7.7.11 Deve permitir o ajuste dinâmico de nível de potência de modo a otimizar o tamanho da célula de RF (rádio frequência) conforme as características do ambiente, evitando intervenção manual;

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

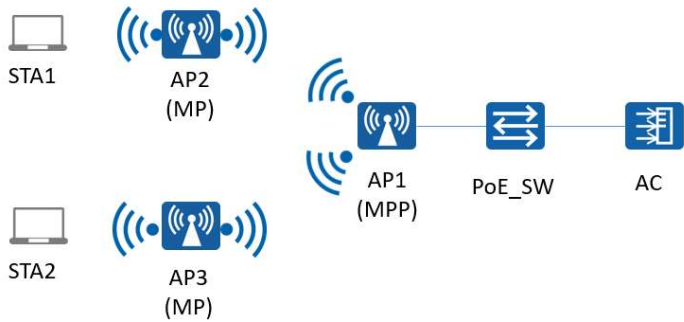
<b>Item de teste</b>	Alteração da potência de transmissão		
<b>Objetivo do teste</b>	Validar se a potência de transmissão do AP pode ser modificada e se o intervalo de potência está dentro da legislação local.		
<b>Configuração de teste</b>	<p>Topologia da rede:</p> <div style="text-align: center;">  </div> <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>		
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Configure ac corretamente, AP divulga SSID: "SSID1"</li> <li>2) Alterar o código do país para "BR" (Brasil)</li> <li>3) Desativar acalibração e alterar a potência de transmissão, resultado esperado 1</li> </ol>		
<b>Resultado esperado</b>	1) O rádio é transmitido na potência definida, a limitação de potência é regida pela legislação local do Brasil.		
<b>Resultado</b>			
<b>Observação</b>			
<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	

### Mesh Network

5.6.7.14 Deve permitir operação em modo Mesh, garantindo o estabelecimento da conexão por meio do rádio Wi-Fi com outros pontos de acesso;

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

5.7.7.14 Deve permitir operação em modo Mesh, garantindo o estabelecimento da conexão por meio do rádio Wi-Fi com outros pontos de acesso;

<b>Item de teste</b>	Rede Mesh
<b>Objetivo do teste</b>	Validar que o Sistema WLAN suporta Rede Mesh
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Configurar a função Mesh nac: o AP1 funciona como MPP, o AP2/AP3 funciona como MP, o AP1 estabelece ligações virtuais sem fios com eles na banda 5G</li> <li>2) Verificar as informações da conexão em Mesh nac. Resultado esperado 1;</li> <li>3) Configurar o AP2 para fornecer SSID: "SSID-Temp1", utilizando rádio de 2,4GHZ; Configurar o AP3 para fornecer SSID: "SSID-Temp2", utilizando rádio de 2,4GHZ</li> <li>4) STA1 liga-se a "SSID-Temp1". Espera-se o resultado 2;</li> </ol>


PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

	5) STA2 liga-se a "SSID-Temp2". Espera-se o resultado 3;		
<b>Resultado esperado</b>	1) Verificar informação de link mesh nac; 2) o dispositivo (STA1) conecta com sucesso ao "SSID-Temp1", Pinga o gateway com sucesso, o dado transmite-se do AP2 ao AP1 . 3) o dispositivo (STA2) conecta com sucesso ao "SSID-Temp2", Pinga o gateway com sucesso, o dado transmite-se do AP3 to AP1.		
<b>Resultado</b>			
<b>Observação</b>			
<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	

### Target Wake Time (TWT)

5.6.7.15 Deve implementar recurso de Target Wake Time (TWT);

5.7.7.15 Deve implementar recurso de Target Wake Time (TWT);

<b>Item de teste</b>	Target Wake Time (TWT)
<b>Objetivo do teste</b>	Validar que o Sistema WLAN suporta TWT
<b>Configuração de teste</b>	<p>Topologia da rede:</p> <div style="text-align: center;">  <p>STA      AP      Switch      AC</p> </div> <p>Condições iniciais:</p> <p>1) Todos os dispositivos funcionando normalmente</p>


**PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO**  
**PROCESSO Nº 2020.0000.604.5301**  
**INTERESSADO: GERÊNCIA DE SUPORTE DE REDES**

	2) Montar o ambiente de teste de acordo com a topologia acima		
<b>Procedimento de teste</b>	1) Configure ac corretamente, AP divulga SSID: "SSID1" 2) Habilite TWT, Resultado esperado 1		
<b>Resultado esperado</b>	1) O status TWT pode ser verificado nos detalhes de perfil SSID.		
<b>Resultado</b>			
<b>Observação</b>			
<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	

### BSS Coloring

5.6.7.17 Deve suportar BSS Coloring;

5.7.7.17 Deve suportar BSS Coloring;

<b>Item de teste</b>	<b>BSS Coloring</b>
<b>Objetivo do teste</b>	<b>Validar se o AP suporta coloração BSS</b>
<b>Configuração de teste</b>	Topologia da rede:  <p>Condições iniciais:</p> 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
<b>Procedimento de teste</b>	1) Configure ac corretamente, AP divulga SSID: "SSID-TEMP" no rádio 5G;





PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
PROCESSO Nº 2020.0000.604.5301  
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

	2) Verifique informação da estação nac, resultado 1. 3) Capturar o pacote, esperar resultado 2.		
<b>Resultado esperado</b>	1) o display do dispositivo (STA) mostra que BSS coloring é suportado. 2) O pacote tem o quadro BSS coloring incluído.		
<b>Resultado</b>			
<b>Observação</b>			
<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	

## Switch

Itens que não necessitam de configuração paracomprovação:

### 5.8 Switch Tipo 01

5.8.5 Possuir no mínimo 24(vinte e quatro) PoE portas Gigabit RJ45;

Comprovação visual – Documentação complementar:

CloudEngine S5735-L-V2 Series Switches Datasheet.pdf

- S5735-L24P4S-A-V2
- 24 x 10/100/1000Base-T ports
- 802.3af (15.4 W per port): 24
- 802.3at (30 W per port): 13

5.8.6 Possuir no mínimo 4(quatro) portas SFP 1 Gbps ou superior;

Comprovação visual – Documentação complementar:

CloudEngine S5735-L-V2 Series Switches Datasheet.pdf

- S5735-L24P4S-A-V2
- 4 x GE SFP ports

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
PROCESSO Nº 2020.0000.604.5301  
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

---

5.8.8 Possuir Leds indicativos de funcionamento da fonte de alimentação e status das portas;

Comprovação visual - Documentação complementar:

Product description – Hardware description – Chassis – S5735-L24P4S-A-V2 – Indicators e buttons

[https://support.huawei.com/hedex/hdx.do?docid=EDOC1100302331&id=EN-US\\_CONCEPT\\_0000001386247636&lang=en](https://support.huawei.com/hedex/hdx.do?docid=EDOC1100302331&id=EN-US_CONCEPT_0000001386247636&lang=en)

5.8.9 Deve ocupar 1U do Rack;

Comprovação Visual – Documentação complementar:

Product description – Hardware description – Chassis – S5735-L24P4S-A-V2 – Technical specifications:

[https://support.huawei.com/hedex/hdx.do?docid=EDOC1100302331&id=EN-US\\_CONCEPT\\_0000001386247636&lang=en](https://support.huawei.com/hedex/hdx.do?docid=EDOC1100302331&id=EN-US_CONCEPT_0000001386247636&lang=en)

Chassis height [U] 1 U

5.8.15 Possuir fonte de alimentação interna que trabalhe em 100V-240V, 50/60 Hz, com detecção automática de tensão e frequência;

Comprovação visual – Documentação complementar:

CloudEngine S5735-L-V2 Series Switches Datasheet.pdf

- ac input: 100 V ac to 240 V ac, 50/60 Hz

5.8.29 Deverá estar licenciado para a gerência e controle do item Solução de gerenciamento e controle;

Comprovação documental:

CloudCampus N1 Business Model Datasheet.pdf



PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
PROCESSO Nº 2020.0000.604.5301  
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

---

### 5.9 Switch Tipo 02

5.9.2 Possuir no mínimo 24 portas 10/100/1000 Base-T;

Comprovação visual - Documentação complementar:

CloudEngine S5735-L-V2 Series Switches Datasheet.pdf

- S5735-L24T4S-A-V2
- 24 x 10/100/1000Base-T ports

5.9.3 Possuir no mínimo 4(quatro) portas SFP 1 Gbps ou superior;

Comprovação visual - Documentação complementar:

CloudEngine S5735-L-V2 Series Switches Datasheet.pdf

- S5735-L24T4S-A-V2
- 4 x GE SFP ports

5.9.5 Possuir Leds indicativos de funcionamento da fonte de alimentação e status das portas;

Comprovação visual – Documentação complementar:

Product description – Hardware description – Chassis – S5735-L24T4S-A-V2 – Indicators e buttons:

[https://support.huawei.com/hedex/hdx.do?docid=EDOC1100302331&id=EN-US\\_CONCEPT\\_0000001386088048&lang=en](https://support.huawei.com/hedex/hdx.do?docid=EDOC1100302331&id=EN-US_CONCEPT_0000001386088048&lang=en)

5.9.6 Deve ocupar 1U do Rack;

Product description – Hardware description – Chassis – S5735-L24P4S-A-V2 – Technical specifications:

[https://support.huawei.com/hedex/hdx.do?docid=EDOC1100302331&id=EN-US\\_CONCEPT\\_0000001386088048&lang=en](https://support.huawei.com/hedex/hdx.do?docid=EDOC1100302331&id=EN-US_CONCEPT_0000001386088048&lang=en)

Chassis height [U] 1 U

5.9.12 Possuir fonte de alimentação interna que trabalhe em 100V-240V, 50/60 Hz, com detecção automática de tensão e frequência;

**PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO**  
**PROCESSO Nº 2020.0000.604.5301**  
**INTERESSADO: GERÊNCIA DE SUPORTE DE REDES**

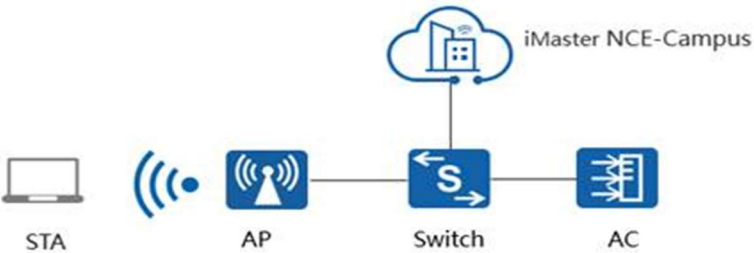
CloudEngine S5735-L-V2 Series Switches Datasheet.pdf

- ac input: 100 V ac to 240 V ac, 50/60 Hz

**Support autenticação to RADIUS servidores**

5.8.18 Suportar autenticação em servidores RADIUS ou TACACS;

5.9.15 Suportar autenticação em servidores RADIUS ou TACACS;

<b>Item de teste</b>	<b>Suporte de autenticação para servidores RADIUS (5.8.18 / 5.9.15)</b>
<b>Objetivo do teste</b>	Suporta autenticação para servidores RADIUS;
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p style="text-align: center;"> <span>STA</span>      <span>AP</span>      <span>Switch</span>      <span>AC</span> </p> <p>iMaster NCE-Campus</p> <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
PROCESSO Nº 2020.0000.604.5301  
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

<b>Procedimento de teste</b>	1) Selecione “Provision> Device > Site Configuration > Site > Device Login Configuration” no menu principal .Clique ”Create“; Depois, configure regras de autenticação, regras de autorização e os resultados da autorização. Resultado esperado 1 é obtido.		
<b>Resultado esperado</b>	1) A configuração é entregue e autenticada com sucesso.		
<b>Resultado</b>			
<b>Observação</b>			
<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	

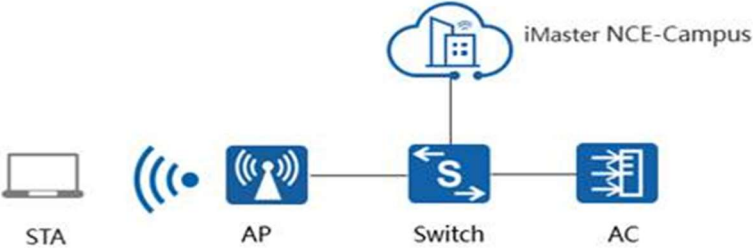
### LLDP e LLDP-MED

5.8.22. Implementar LLDP e LLDP-MED;

5.9.19. Implementar LLDP e LLDP-MED;

<b>Item de teste</b>	<b>LLDP e LLDP-MED (5.8. 22)</b>
<b>Objetivo do teste</b>	<b>Implementar LLDP e LLDP-MED;</b>

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

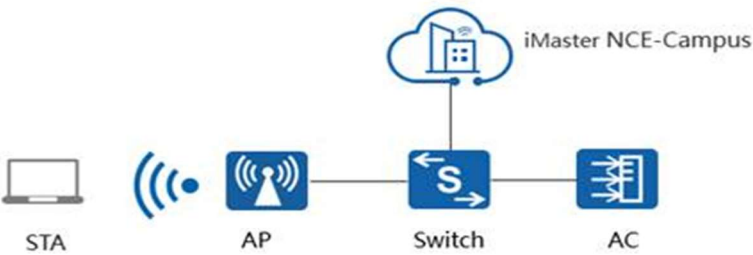
<p align="center"><b>Configuração de teste</b></p>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>		
<p align="center"><b>Procedimento de teste</b></p>	<ol style="list-style-type: none"> <li>1) Selecione "Provision&gt; Device &gt; Single Device Configuration no menu principal.</li> <li>2) Selecione o dispositivo a configurar e escolha "System Management &gt; LLDP "na árvore de navegação à esquerda.</li> <li>3) Clique na aba LLDP e active a função LLDP global. Obtém-se o resultado esperado 1.</li> </ol>		
<p align="center"><b>Resultado esperado</b></p>	<ol style="list-style-type: none"> <li>1) Aconfiguração é entregue com êxito e os dispositivos vizinhos podem ser descobertos</li> </ol>		
<p align="center"><b>Resultado</b></p>			
<p align="center"><b>Observação</b></p>			
<p align="center"><b>Assinatura do cliente</b></p>		<p align="center"><b>Assinatura do fabricante</b></p>	

**PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO**  
**PROCESSO Nº 2020.0000.604.5301**  
**INTERESSADO: GERÊNCIA DE SUPORTE DE REDES**

**ACL**

5.8.24. Deve Implementar ACL ou outra funcionalidade de filtragem de tráfego por porta TCP/UDP de origem/destino, por endereço MAC de origem/destino ou VLAN;

5.9.21. Deve Implementar ACL ou outra funcionalidade de filtragem de tráfego por porta TCP/UDP de origem/destino, por endereço MAC de origem/destino ou VLAN;

<b>Item de teste</b>	<b>ACL (5.8.24 / 5.9.21)</b>
<b>Objetivo do teste</b>	Deve implementar ACL ou outra funcionalidade de filtragem de tráfego por porta TCP/UDP de origem/destino, endereço MAC de origem/destino ou VLAN;
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
PROCESSO Nº 2020.0000.604.5301  
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

<b>Procedimento de teste</b>	<ol style="list-style-type: none"><li>1) Escolha "Planning &gt; Deployment &gt; Device Deployment &gt; Single Device Configuration" no menu principal.</li><li>2) Seleccione o dispositivo a configurar e escolha "Switch &gt; Traffic Policy" (Switch &gt; Política de tráfego) no painel de navegação.</li><li>3) Clique em Criar para configurar uma regra ACL. É obtido o resultado esperado 1.</li><li>4) Enviar dois fluxos, um dos quais está em conformidade com a política criada pela ACL e o outro não. É apresentado o resultado esperado 2.</li></ol>		
<b>Resultado esperado</b>	<ol style="list-style-type: none"><li>1) A configuração é entregue com sucesso.</li><li>2) O tráfego que corresponde às regras ACL é processado com base nas políticas correspondentes.</li></ol>		
<b>Resultado</b>			
<b>Observação</b>			
<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	

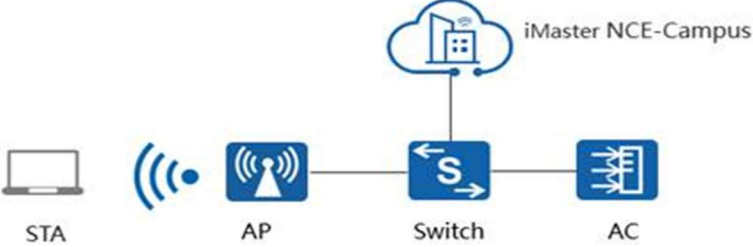
**IGMP snooping;(GUI 不支持下发相关配置)**

5.8.26. Implementar IGMP v1, IGMP v2 e IGMP v3 snooping;

5.9.23. Implementar IGMP v1, IGMP v2 e IGMP v3 snooping;



PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

<b>Item de teste</b>	<b>IGMP snooping (5.8.26 / 5.9.23)</b>
<b>Objetivo do teste</b>	<b>Implementar o snooping IGMP v1, IGMP v2 e IGMP v3;</b>
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) 1) O dispositivo testado é conectado ao testador através de duas interfaces. A função de IGMP snooping está ativada no dispositivo testado. A interface 1 do testador simula uma fonte de multicast e a interface 2 simula um cliente de multicast para se juntar a um grupo de multicast.</li> <li>2) 2) Envio de tráfego multicast da porta 1 do testador e observe o recebimento do tráfego multicast.</li> </ol>

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
PROCESSO Nº 2020.0000.604.5301  
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

	3) Habilite IGMP snooping na exibição do sistema e na exibição VLAN do DUT. Defina a versão para v1, v2 e v3 respectivamente. Repita os passos 1 a 2. Os resultados esperados 1 a 2 são obtidos.		
<b>Resultado esperado</b>	1) Tport_2 do testador junta-se ao grupo multicast e tem uma tabela de encaminhamento multicast da camada 2. Tport_2 do testador recebe fluxos de dados multicast.  2) Tport_2 no testador não pode receber dados multicast.		
<b>Resultado</b>			
<b>Observação</b>			
<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	

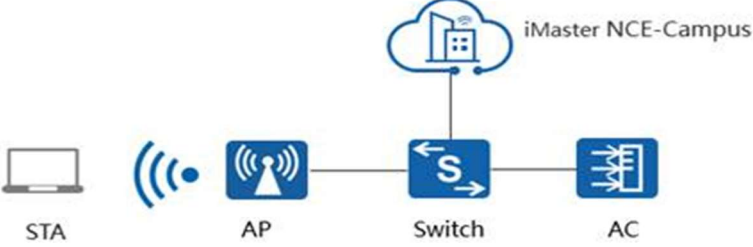
### Autenticação 802.1x

5.8.28 Implementar IEEE 802.1x para autenticação do usuário, permitindo à associação dinâmica do usuário a determinada VLAN;

5.10.26 Implantar autenticação de dispositivos e usuários via 802.1x, Web Portal e endereço MAC na rede sem fio;

<b>Item de teste</b>	<b>Autenticação 802.1x (5.8.28)</b>
----------------------	-------------------------------------

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

<b>Objetivo do teste</b>	Implementar IEEE 802.1x para autenticação de usuários, permitindo a associação dinâmica de utilizadores a uma determinada VLAN;
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Selecione "Provision &gt; Device &gt; Site Configuration &gt; Switch &gt; Authentication &gt; Wired Authentication", clique "Create", insira o nome, selecione modo de Autenticação como "Secure network", selecione servidor radius, a interface do dispositivo, clique em "OK ". Escolha "Provision &gt; Admission Policy &gt; Authentication and Authorization ", clique "Create", selecione vlan. Resultado esperado 1;</li> <li>2) O usuário conecta o terminal à porta do switch, insere usuário e senhacorretos. Resultado esperado 2;</li> <li>3) O usuário conecta o terminal à porta do switch, insere the usuário e senha incorretos. Resultado esperado 3.</li> </ol>



PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
PROCESSO Nº 2020.0000.604.5301  
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

<b>Resultado esperado</b>	1) As configurações são implementadas com sucesso; 2) A autenticação 802.1X é bem sucedida e o usuário pode acessar a rede; 3) A autenticação 802.1X falha, o utilizador não pode acessar à rede.		
<b>Resultado</b>			
<b>Observação</b>			
<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	

**Management e Control Solution**

Comprovações sem configuração:

5.10.2 A solução deve ser do mesmo fabricante dos demais itens ofertados no Lote 02;

Comprovação visual - Documentação complementar

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES


**iMaster NCE-Campus Product Documentation**

Product Version: V300R021C00 | Library Version: 03 | Date: 2023-02-13

## iMaster NCE-Campus

iMaster NCE-Campus is a centralized management and web-based control system designed for the CloudCampus solution. It supports a wide range of functions, including network service management, network security management, network access management, network monitoring, network quality analysis, network application analysis, alarm management, report management. As well as these, it supports big data analytics and open application programming interfaces (APIs) to facilitate integration with other platforms. Enterprise users can use iMaster NCE-Campus to implement service provisioning, configuration, and routine maintenance for multiple tenant networks separately, enabling management of large-scale devices on the cloud.

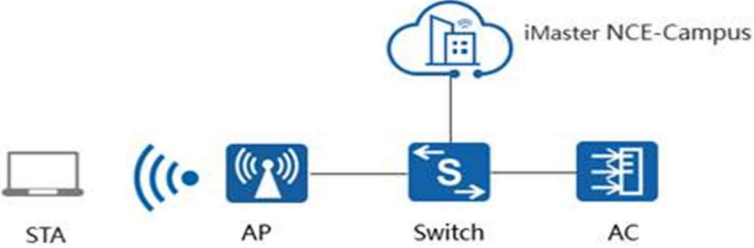
Comprovações com configurações:

### Monitoramento e geração de relatórios

5.10.4 A solução deve ser capaz de centralizar o monitoramento e relatórios de todo o parque de dispositivos, através de console única;

<b>Item de teste</b>	<b>Monitoramento e geração de relatórios (5.10.4)</b>
<b>Objetivo do teste</b>	<b>A solução deve ser capaz de centralizar o monitoramento e relatórios de todo o parque de dispositivos, através de console única.</b>
<b>Configuração de teste</b>	Topologia da rede:

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

	<div style="text-align: center;">  <p>The diagram illustrates a network topology. On the left, a laptop icon labeled 'STA' is connected to a wireless signal icon. This signal is received by an 'AP' (Access Point) icon. The AP is connected to a 'Switch' icon, which is further connected to an 'AC' (Access Controller) icon. Above the switch, a cloud icon labeled 'iMaster NCE-Campus' is connected to the switch.</p> </div> <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<p><b>Procedimento de teste</b></p>	<ol style="list-style-type: none"> <li>1) Selecione “Monitoring &gt; Monitoring &gt; Site &gt; Configuration” no menu principal. Configure a função de monitoramento de dispositivo. Resultado esperado 1 é obtido.</li> <li>2) Selecione “Monitoring &gt; Monitoring &gt; report &gt; Configuration” no menu principal. Resultado esperado 2 é obtido.</li> </ol>
<p><b>Resultado esperado</b></p>	<ol style="list-style-type: none"> <li>1) Monitorar todo o parque de dispositivos, através de console única;</li> <li>2) Gerar relatórios de todo o parque de dispositivos, através de console única;</li> </ol>
<p><b>Resultado</b></p>	
<p><b>Observação</b></p>	

**PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO**  
**PROCESSO Nº 2020.0000.604.5301**  
**INTERESSADO: GERÊNCIA DE SUPORTE DE REDES**

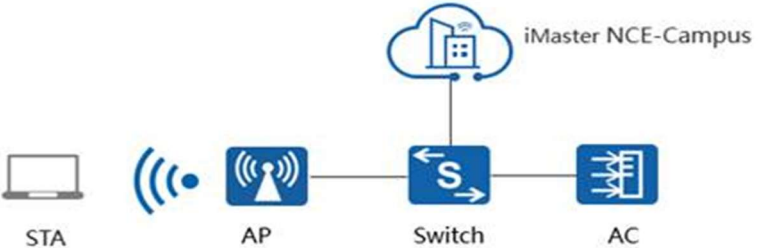
<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	
------------------------------	--	---------------------------------	--

**Gerenciamento de permissões e domínio**

5.10.15 Permitir a customização do a acesso administrativo através de atribuição de grupo de função do usuário administrador.

5.10.27 Implementar controle de a acesso de usuário administrativo por HTTPS. Deve ainda implementar perfis de a acesso diferenciados por usuário ou grupo de usuários;

5.10.28 Gerenciar de forma centralizada a autenticação de usuários;

<b>Item de teste</b>	<b>Rights and domain-based management (5.10.15)</b>
<b>Objetivo do teste</b>	Permite a administração de acessos baseado em atribuição de grupos de usuários administradores
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p>

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
PROCESSO Nº 2020.0000.604.5301  
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

	1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima		
Procedimento de teste	1) Selecione “System > User Management > User Management > Users” from the menu principal. Resultado esperado 1 é obtido.		
Resultado esperado	1) Permitir customização of administrative a access through group atribuirment of the administrator user role.		
Resultado			
Observação			
Assinatura do cliente		Assinatura do fabricante	

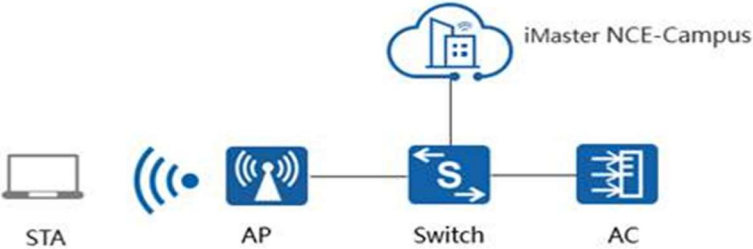
### Restauração de configurações de provisionamento

5.10.25 Deverá ser capaz de provisionar remotamente novos dispositivos em estado padrão de fábrica para estado totalmente provisionado;

<b>Item de teste</b>	<b>Restore Deployment Configurations (5.10.25)</b>
<b>Objetivo do teste</b>	Deve ser capaz de provisionar novos dispositivos em estado de padrão de fábrica para estado totalmente provisionado



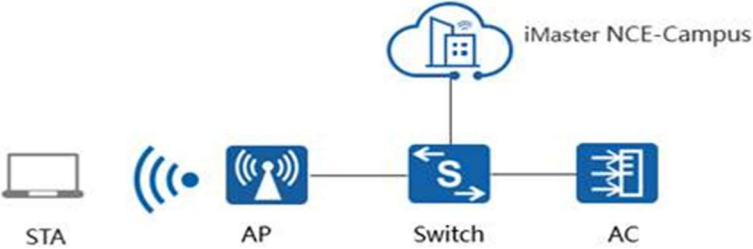
PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

<p align="center"><b>Configuração de teste</b></p>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>		
<p align="center"><b>Procedimento de teste</b></p>	<ol style="list-style-type: none"> <li>1) Selecione "Design &gt; Site Design &gt; Device Management "; select a device , clique "More &gt; Restore Deployment Configurations "</li> </ol>		
<p align="center"><b>Resultado esperado</b></p>	<ol style="list-style-type: none"> <li>1) Novos dispositivos em estado padrão de fábrica são remotamente provisionados para um estado totalmente provisionado</li> </ol>		
<p align="center"><b>Resultado</b></p>			
<p align="center"><b>Observação</b></p>			
<p align="center"><b>Assinatura do cliente</b></p>		<p align="center"><b>Assinatura do fabricante</b></p>	

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

**Radius relay**

5.10.32 Implementar Radius relay, de forma a permitir integração com servidor Radius externos;

<b>Item de teste</b>	<b>Radius relay (5.10.32)</b>
<b>Objetivo do teste</b>	Implementar Radius relay, a fim de permitir a integração com servidores RADIUS externos;
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Selecione “Designn &gt; Network Design &gt; Template Management” a partir do menu principal. Clique em criar.Resultado esperado 1 é obtido.</li> </ol>



PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
PROCESSO Nº 2020.0000.604.5301  
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

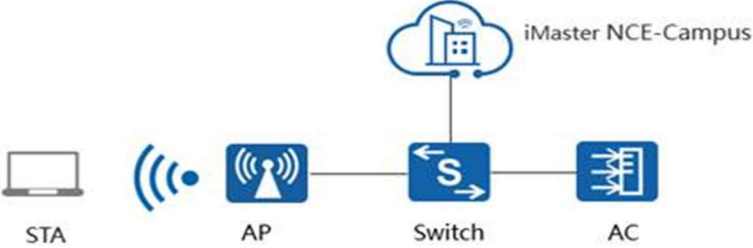
<b>Resultado esperado</b>	1) Servidor RADIUS relay created com sucesso		
<b>Resultado</b>			
<b>Observação</b>			
<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	

**Permitir autenticação de usuário em página customizada**

5.10.33 Permitir a customização de página de autenticação de usuários, com inclusão de textos e logotipo;

<b>Item de teste</b>	Permitir autenticação de usuário via portal customizado (5.10.33)
<b>Objetivo do teste</b>	Permitir a customização da página de autenticação do usuário, com inclusão de texto e logo;
<b>Configuração de teste</b>	Topologia da rede:

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

	<div style="text-align: center;">  <p>STA      AP      Switch      AC      iMaster NCE-Campus</p> </div> <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>		
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Selecione " Admission &gt; Admission Resources &gt; Page Management" from the menu principal. Resultado esperado 1 é obtido.</li> </ol>		
<b>Resultado esperado</b>	<ol style="list-style-type: none"> <li>1) <b>Permitir a customização da página de autenticação do usuário, com inclusão de texto e logo;</b></li> </ol>		
<b>Resultado</b>			
<b>Observação</b>			
<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	

**Identificar usuários conectados e informação de dispositivos**

5.10.36 Identificar usuários e dispositivo conectados e permitir a visualização de, no mínimo:



**PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO**  
**PROCESSO Nº 2020.0000.604.5301**  
**INTERESSADO: GERÊNCIA DE SUPORTE DE REDES**

---

5.10.36.1 Nome usuário conectado;

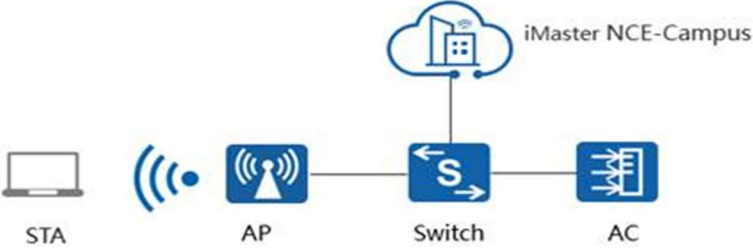
5.10.36.2 Endereço MAC;

5.10.36.3 Status da autenticação;

5.10.36.4 Horário de início da sessão ou Tempo de conexão;

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

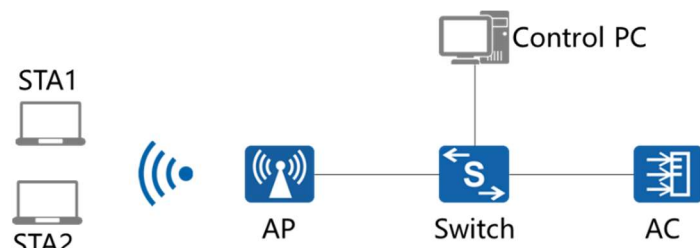
5.10.36.5 Sistema Operacional do dispositivo a qual está associado;

<b>Item de teste</b>	<b>Identificação de informações de dispositivos de usuário. (5.10.36)</b>
<b>Objetivo do teste</b>	Identificação de dispositivos de usuários conectados, com a visão de Login de usuário. MAC address; Status de Autenticação; Horário de início da sessão ou Tempo de conexão; Sistema Operacional do dispositivo a qual está associado;
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Selecione "Admission &gt; Admission Policy &gt; Online User Control &gt; Online User &gt; Site "from the menu principal. Resultado esperado 1 é obtido.</li> </ol>

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

<b>Resultado esperado</b>	1) Identificar usuários conectados e dispositivos, e visualizar login de usuário, endereço MAC, status autenticação, horário de início de sessão, ou tempo de conexão e sistema operacional.		
<b>Resultado</b>			
<b>Observação</b>			
<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	

**WLAN AC GUI**

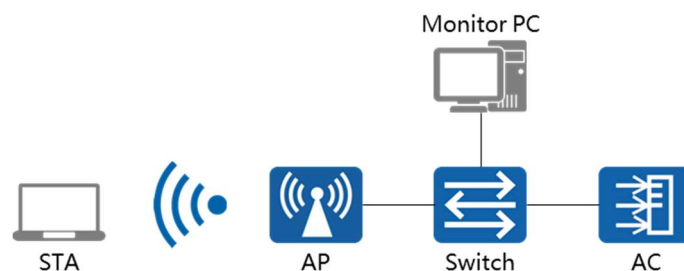
<b>Item de teste</b>	WLAN AC Web Management
<b>Objetivo do teste</b>	Validar que a WLAN AC suporta Web Management
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>

**PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO**  
**PROCESSO Nº 2020.0000.604.5301**  
**INTERESSADO: GERÊNCIA DE SUPORTE DE REDES**

<b>Procedimento de teste</b>	1) Configure Switch, AC e Control PC, Control PC pode acessar a AC; 2) Login à AC GUI por meio da controladora do iMaster NCE Campus. Resultado esperado 1.		
<b>Resultado esperado</b>	1) Usuário pode logar na GUI com as credenciais de username e senha corretas. Usuário pode gerenciar a AC por meio da interface gráfica GUI.		
<b>Resultado</b>			
<b>Observação</b>			
<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	

### CAPWAP Control-link DTLS Encrypt by PSK

5.10.6 A comunicação entre a solução de Gerenciamento e os access Points/Switches deve ser criptografada; (Switches via SSH sobre Netconf)

<b>Item de teste</b>	CAPWAP Control-link DTLS Encrypt by PSK
<b>Objetivo do teste</b>	Validar que o Sistema WLAN suporta CAPWAP control-link DTLS encrypt via PSK
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos are funcionando normalmente.</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima.</li> </ol>



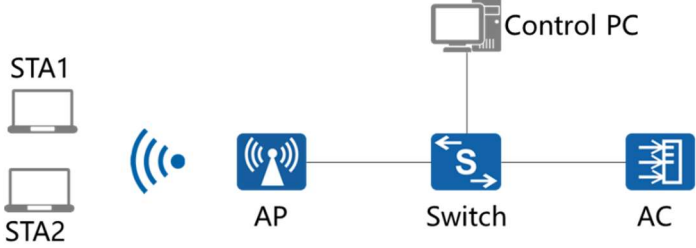
PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Configure os dispositivos de rede para que o AP possa comunicar com o AC.</li> <li>2) Configure port mirroring no switch para que PC de monitoramento possa capturar a comunicação de pacotes entre o AP e a AC.</li> <li>3) Habilite autenticação CAPWAP DTLS no AP, e configure PSK como DTLS encryption.</li> <li>4) Configure AP login parameters no AC, Habilite a função DTLS encryption para o túnel de controle CAPWAP, e configure PSK para encriptação DTLS para que o túnel de controle seja o mesmo que do AP.</li> <li>5) Aguarde um tempo e verifique o AP status na AC. Resultado esperado 1.</li> <li>6) Verifique que os pacotes trocados entre o AP e a AC no monitor PC quando o AP ficar online. Resultado esperado 2.</li> </ol>		
<b>Resultado esperado</b>	<ol style="list-style-type: none"> <li>1) The AP goes online on the a ac.</li> <li>2) Pacotes trocados entre o AP e a AC mostram que o método de encriptação DTLS é PSK.</li> </ol>		
<b>Resultado</b>			
<b>Observação</b>			
<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	

### AP Group

5.10.12 Deve permitir que as configurações sejam aplicadas em vários pontos de a acesso selecionados simultaneamente, isto é, não será permitido soluções que necessitem configurar os pontos de a acesso individualmente.

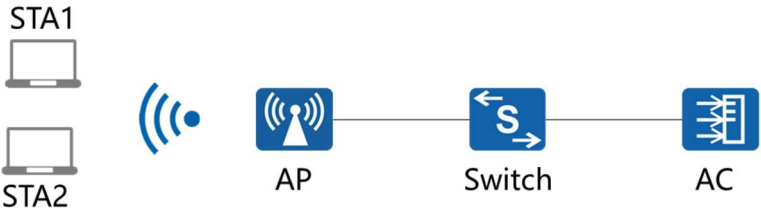
PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

<b>Item de teste</b>	WLAN AC Web Management		
<b>Objetivo do teste</b>	Validar que a WLAN AC suporta gerenciamento via Web e é possível realizar configurações em grupos de AP		
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>		
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Login to the a ac GUI through NCE controller. Resultado esperado 1.</li> <li>2) Selecione "Configuration"- "AP Configuration"- "AP group"</li> </ol>		
<b>Resultado esperado</b>	<ol style="list-style-type: none"> <li>1) User can login to GUI with the correct username e senha. User can also manage the a ac using GUI.</li> <li>2) AP can be managed as groups</li> </ol>		
<b>Resultado</b>			
<b>Observação</b>			
<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	

**Auto-off radio**

<b>Item de teste</b>	Auto-off radio
<b>Objetivo do teste</b>	Validar que o Sistema WLAN suporta shutdown em radios individuais de

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

	forma imediata ou agendada
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Configure a ac corretamente, AP delivers SSID: "SSID-Temp";</li> <li>2) o dispositivo cliente (STA) connet to "SSID-Temp". Resultado esperado 1;</li> <li>3) Habilite Auto-off radio function nac, set from time AAA to time BBB to turn off the radio; ou certain day of the week/time;</li> <li>4) After time AAA/day, o dispositivo cliente (STA) conecte to SSID. Resultado esperado 2;</li> <li>5) After time BBB/day, o dispositivo cliente (STA) conecte to SSID. Resultado esperado 3.</li> </ol>
<b>Resultado esperado</b>	<ol style="list-style-type: none"> <li>1) o dispositivo cliente (STA) can scan "SSID-Temp" on both 2.4G e 5G radio ;</li> <li>2) o dispositivo cliente (STA) can scan "SSID-Temp" only on 5G radio;</li> <li>3) o dispositivo cliente (STA) can scan "SSID-Temp" on both 2.4G e 5G radio.</li> </ol>
<b>Resultado</b>	
<b>Observação</b>	


PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	
------------------------------	--	---------------------------------	--

### Rogue AP Detection

5.10.13 Permitir a configuração total dos pontos de a acesso, assim como os aspectos de segurança da rede sem fio (WLAN) e Rádio Frequência (RF).

5.10.21 Detectar interferência e ajustar parâmetros de RF, evitando problemas de cobertura de RF de forma automática; (Complementado por Automatic radio calibration case 5.10.20)

<b>Item de teste</b>	Rogue AP Detection
<b>Objetivo do teste</b>	Validar que o Sistema WLAN suporta Rogue AP Detection
<b>Configuração de teste</b>	<p>Topologia da rede:</p> <div style="text-align: center;">  <p>Rogue AP      AP      Switch      AC</p> </div> <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Configure Rogue AP to deliver SSID: "SSID-Temp";</li> <li>2) Configure a ac corretamente, AP deliver SSID: "SSID-Temp";</li> <li>1) Habilite Rogue AP detection function na AC. Resultado esperado 1.</li> </ol>
<b>Resultado esperado</b>	<ol style="list-style-type: none"> <li>1) Rogue AP será detectado pelo sistema WLAN.</li> </ol>
<b>Resultado</b>	

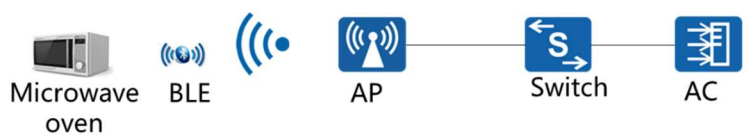
PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

<b>Observação</b>			
<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	

### Non-Wi-Fi Device Detect e Spectrum Analysis

5.10.13 Permitir a configuração total dos pontos de acesso, assim como os aspectos de segurança da rede sem fio (WLAN) e Rádio Frequência (RF).

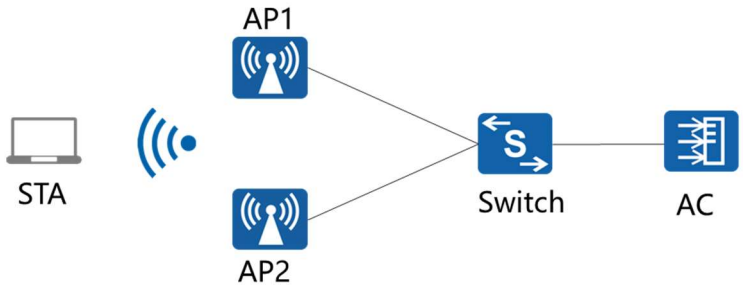
5.10.21 Detectar interferência e ajustar parâmetros de RF, evitando problemas de cobertura de RF de forma automática; (Complementado por Automatic radio calibration case 5.10.20)

<b>Item de teste</b>	Non-Wi-Fi Device Detect e Spectrum Analysis
<b>Objetivo do teste</b>	Validar que o Sistema WLAN suporta detecção de fontes de RF Non-Wi-Fi função de análise de espectro.
<b>Configuração de teste</b>	<p>Topologia da rede:</p> <div style="text-align: center;">  <p>Microwave oven   BLE   AP   Switch   AC</p> </div> <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Configure a ac corretamente, AP deliver SSID: "SSID-Temp";</li> <li>2) Habilite spectrum analysis function na AC;</li> <li>3) Dispositivos de RF Non-Wi-Fi como bluebooth, microondas duncionando próximo ao AP. Resultado esperado 1.</li> </ol>

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

<b>Resultado esperado</b>	1) Dispositivos Non-Wi-Fi podem ser detectados na AC, e a informação sobre os dispositivos é mostrada na GUI da AC.		
<b>Resultado</b>			
<b>Observação</b>			
<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	

### Session-based Dynamic Load Balancing

<b>Item de teste</b>	Session-based Dynamic Load Balancing
<b>Objetivo do teste</b>	Validar que o Sistema WLAN suporta session based dynamic load balancing – Balanceamento de carga dinâmico por sessão.
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> <li>3) There é overlap area between AP1 e AP2</li> </ol>
<b>Procedimento de teste</b>	1) Configure a ac corretamente, AP deliver SSID: "SSID-Temp";

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

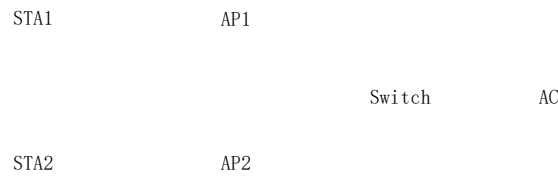
	2) Habilite Dynamic load balancing function nac, set the load balancing parameters: session based load balance, start threshold e balance gap;  3) o dispositivo cliente (STA1) ~ o dispositivo cliente (STAn) conecte to “SSID-Temp”, e verifique the information of o dispositivo cliente (STA)s na AC. Resultado esperado 1.		
<b>Resultado esperado</b>	1) o dispositivo cliente (STA1) ~ o dispositivo cliente (STAn) conecte com sucesso to “SSID-Temp”, e Ping gateway com sucesso. The gap of o dispositivo cliente (STA)s between AP1 e AP2 é smaller than the session gap.		
<b>Resultado</b>			
<b>Observação</b>			
<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	

**AP service disable**

5.10.24 Permitir que o serviço sem fio seja desabilitado de determinado ponto de a acesso;

<b>Item de teste</b>	AP service disable
<b>Objetivo do teste</b>	Validar que o sistema suporta shutdown do serviço Wireless em um ou mais AP's
<b>Configuração de teste</b>	Topologia da rede:

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

	<div style="text-align: center;">  </div> <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>		
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Configure a AC corretamente, AP1 e AP2 entregam a SSID: "SSID-Temp";</li> <li>2) Verifique radio status. Resultado esperado 1;</li> <li>3) Desabilitar todos os radios do AP1 na AC. Resultado esperado 2;</li> </ol>		
<b>Resultado esperado</b>	<ol style="list-style-type: none"> <li>1) WLAN service é normal on both AP1 e AP2</li> <li>2) O serviço WLAN do AP1 é desabilitado, e o AP2 funciona normalmente.</li> </ol>		
<b>Resultado</b>			
<b>Observação</b>			
<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	

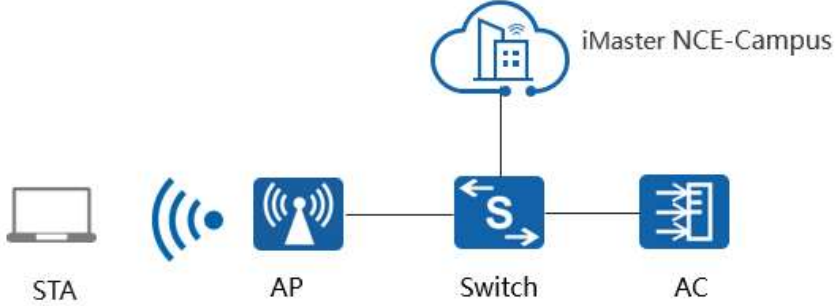
### Autenticação MAC

5.10.26 Implantar autenticação de dispositivos e usuários via 802.1x, Web Portal e endereço MAC na rede sem fio;

<b>Item de teste</b>	Autenticação via MAC
----------------------	----------------------



PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

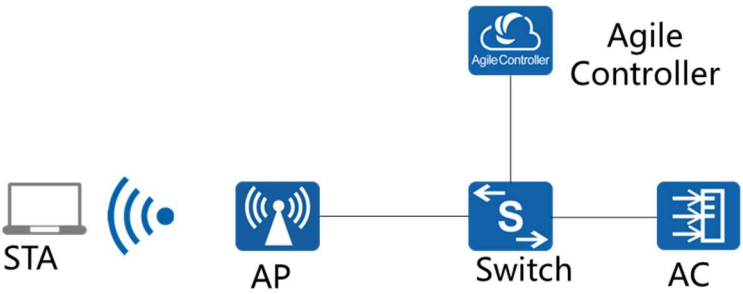
<b>Objetivo do teste</b>	Validar que o Sistema WLAN suporta Autenticação via MAC
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Configure MAC Autenticação WLAN service on WLAN:SSID é "SSID-MAC", MAC Authentication, use external Radius servidor: iMaster NCE-Campus. AP deploys it;</li> <li>2) Configure MAC Authentication no Authentication Server ( iMaster NCE-Campus), o dispositivo cliente (STA)1 MAC é configurado como uma cont authentication account;</li> <li>3) o dispositivo cliente (STA1) e o dispositivo cliente (STA2) conectam ao "SSID-MAC". Resultado esperado 1.</li> </ol>
<b>Resultado esperado</b>	<ol style="list-style-type: none"> <li>1) O dispositivo cliente (STA1) se conecta ao "SSID-MAC" e realiza Ping no gateway com sucesso; porem o dispositivo cliente (STA2) não se conecta ao "SSID-MAC".</li> </ol>
<b>Resultado</b>	
<b>Observação</b>	

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	
------------------------------	--	---------------------------------	--

**Autenticação via Portal (iMaster NCE-Campus como servidor de Portal)**

5.10.26 Implantar autenticação de dispositivos e usuários via 802.1x, **Web Portal** e endereço MAC na rede sem fio;

<b>Item de teste</b>	<b>Portal Autenticação</b>
<b>Objetivo do teste</b>	Validar que o Sistema WLAN suporta Portal Autenticação
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Configure web autenticação WLAN service nac: SSID é "SSID-Portal", web autenticação, use external Portal servidor: iMaster NCE-Campus. AP deploys it;</li> <li>2) Configure Portal functions on Portal servidor( iMaster NCE-Campus), autenticação function on radius servidor ( iMaster NCE-Campus);</li> </ol>

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

	3) o dispositivo cliente (STA) connet to “SSID-Temp”. Resultado esperado 1; 4) o dispositivo cliente (STA) visit a website. Resultado esperado 2.		
<b>Resultado esperado</b>	1) o dispositivo cliente (STA) conecte to “SSID-Portal” e get IP endereço com sucesso, but Ping gateway uncom sucesso; 2) An autenticação page é forced to push when o dispositivo cliente (STA) visit a website, after input right username e senha, o dispositivo cliente (STA) passes autenticação com sucesso, then o dispositivo cliente (STA) Ping gateway e visit the website com sucesso.		
<b>Resultado</b>			
<b>Observação</b>			
<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	

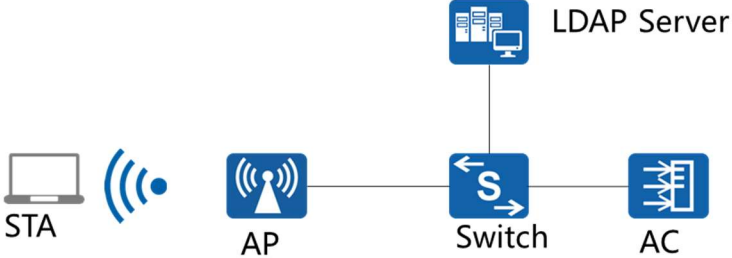
### Autenticação de usuários em redes sem fio

#### Built-in Portal-Authentication (Identity source LDAP)

5.10.26 Implantar autenticação de dispositivos e usuários via 802.1x, Web Portal e endereço MAC na rede sem fio;

<b>Item de teste</b>	Built-in Portal Authentication
<b>Objetivo do teste</b>	Validar que o Sistema WLAN suporta Autenticação e autorização via LDAP

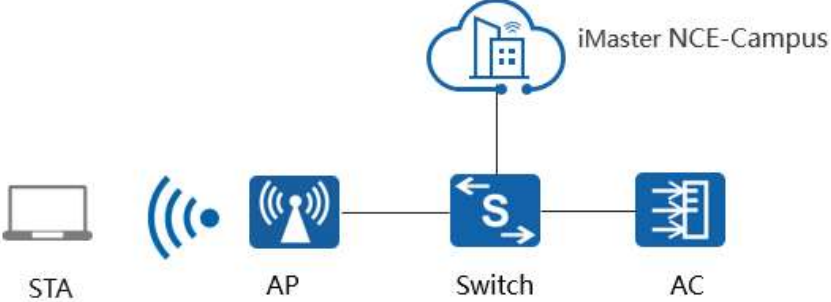
PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>		
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Configure web autenticação WLAN service nac: SSID é “SSID-Portal”, web autenticação, use built-in Portal servidor, identity source é LDAP user. AP deploys it;</li> <li>2) Configure authenticatinac account no servidor LDAP (Lightweight Directory A access Protocol);</li> <li>3) o dispositivo cliente (STA) conecte to “SSID-Portal”, visit a website. Resultado esperado 1;</li> <li>4) o dispositivo cliente (STA) input username e senhacreated by Step 2, Ping PC de Teste. Resultado esperado 2;</li> </ol>		
<b>Resultado esperado</b>	<ol style="list-style-type: none"> <li>1) o dispositivo cliente (STA) é forçosamente redirecionado à página de autenticação do Portal;</li> <li>2) o dispositivo cliente (STA) passa na autenticação e realiza um ping de Teste com sucesso;</li> </ol>		
<b>Resultado</b>			
<b>Observação</b>			
<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

**802.1x Authentication Escape (AAA is Down, Escape Policy: Backup Service VAP)**

5.10.18 A falha de comunicação entre o sistema de Gerenciamento e os Pontos de Acesso não devem interferir na operação dos Pontos de Acesso;

<b>Item de teste</b>	802.1x Authentication Escape
<b>Objetivo do teste</b>	Valida que o sistema WLAN suporta a função de Radius server backup
<b>Configuração de teste</b>	<p>Topologia da Rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Configure o serviço WLAN 802.1x no SSID "SSID-Dot1x", 802.1x authentication, local forwarding. AP deploys it;</li> <li>2) Configure autenticação 802.1x no servidor de autenticação ( iMaster NCE-Campus);</li> <li>3) STA se conecta ao "SSID-Dot1x", utilizando o correto login de usuário e senha. Resultado esperado 1.</li> <li>4) Desconecte o iMaster NCE-Campus do Switch, e o STA vai tentar se conectar ao "SSID-Dot1x", Resultado esperado 2.</li> </ol>

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

	5) Recupere a conexão entre o iMaster NCE-Campus e o Switch, Habilite a função Radius server backup na AC, utilize serviço de backup VAP;  6) Disconecte novamente o iMaster NCE-Campus do Switch, STA vai tentar se conectar ao “SSID-Dot1x” novamente, Resultado esperado 3.		
<b>Resultado esperado</b>	1) STA Se conecta ao “SSID-Dot1x” e consegue da um Ping no gateway com sucesso.  2) STA falha em se conectar ao “SSID-Dot1x”;  3) STA se conecta com sucesso ao “SSID-Dot1x” e da um Ping no gateway com sucesso.		
<b>Resultado</b>			
<b>Observação</b>			
<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	

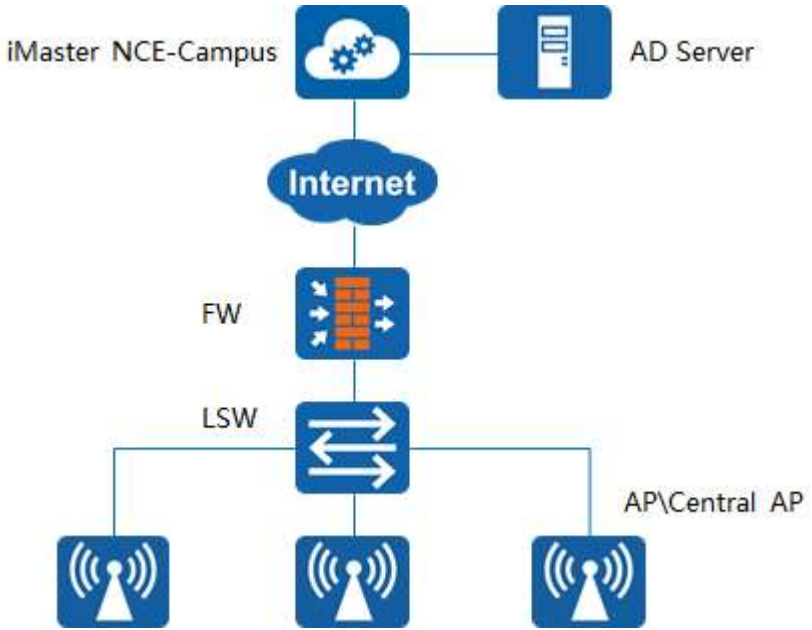
**Integrated with AD/LDAP Domain for Authentication**

5.10.30 Implantar autenticação de usuários nas redes wireless por:

5.10.30.2 LDAP;

<b>Item de teste</b>	Integração com domínio AD/LDAP para Autenticação
<b>Objetivo do teste</b>	Verificar que o CloudCampus da Huawei oferece suporte à integração com o domínio AD/LDAP para autenticação
<b>Configuração de teste</b>	Topologia da Rede:

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

	 <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> <li>3) Tenant logado na plataforma CloudCampus.</li> </ol>
<p><b>Procedimento de teste</b></p>	<ol style="list-style-type: none"> <li>1) Selecionar "Admission &gt; Admission Resources &gt; External Data Source &gt; AD/LDAP Synchronization", clicar no botão "Create", selecionar tipo de servidor como "Active Directory", detalhar Data source name/IP address/port/Ad domain/Base DN/Synchronize account/password, etc., clique "Connection test", Resultado esperado 1;</li> <li>2) Clique em "Next", Selecione o modo de sincronização, Synchronize users/Fast synchronization;</li> <li>3) Clique em "Next", configure os atributos de usuário e user group, insira user group name/user name/account;</li> <li>4) Clique "Next" button, e configure o escopo de sincronização, clique em "Create", configure name/target user group/Location of the OU/Root node/Location of the user;</li> <li>5) Clique em "Next", defina os role mapping rules e selecione o matching rule;</li> <li>6) Clique "Next", e configure Account Filtering Conditions, selecione Server type, configure Authentication source name, selecione filter criteria, adicione OU list e clique em "OK";</li> </ol>

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

	<p>7) Selecione o data source record criado, clique no botão "Synchronize", com resultado esperado 2;</p> <p>8) Selecione "Design &gt; Basic Network Design &gt; Template Management", click "Policy Template", e clique RADIUS Server, depois clique em "Create", insira o nome, e habilite o Built-in Server, insira a chave, e clique em "OK";</p> <p>9) Selecione "Provision &gt; Physical Network &gt; Site Configuration", selecione o site na lista, clique "Switch &gt; Authentication &gt; Wired Authentication", depois clique em "Create", insira o nome, selecione Authentication mode como "Secure network", selecione a escape policy, depois selecione RADIUS server como o servidor criado na etapa 8, adicione a interface do switch e clique "OK", resultado esperado 3;</p> <p>10) Selecione "Admission &gt; Admission Policy &gt; Authentication And Authorization &gt; Authentication Rules", Clique em "Create", insira o nome, selecione o modo de autenticação como User Access Authentication, selecione Access mode as Wired, selecione o Data sources como AD/LDAP, selecione o protocolo de autenticação, e clique "OK";</p> <p>11) Selecione "Admission &gt; Admission Policy &gt; Authentication And Authorization &gt; Authorization Rules", clique em "Create", insira o nome, selecione o modo de autenticação como User Access Authentication, Selecione Access mode como Wired, depois selecione Authentication and Authorization Result como Permit Access e clique "OK";</p> <p>12) STA conecta-se com a porta do switch configurada na etapa 9, com resultado esperado 4.</p>		
<p style="text-align: center;"><b>Resultado esperado</b></p>	<p>1) O servidor AD/LDAP é connectado com sucesso;</p> <p>2) O data source AD/LDAP é configurado para sincronizar com sucesso;</p> <p>3) A regra de autenticação é implementada com sucesso;</p> <p>4) Insira o username/password suportado pelo servidor AD/LDAP, e a autenticação é realizada com sucesso.</p>		
<p style="text-align: center;"><b>Resultado</b></p>			
<p style="text-align: center;"><b>Observação</b></p>			
<p style="text-align: center;"><b>Assinatura do cliente</b></p>		<p style="text-align: center;"><b>Assinatura do fabricante</b></p>	

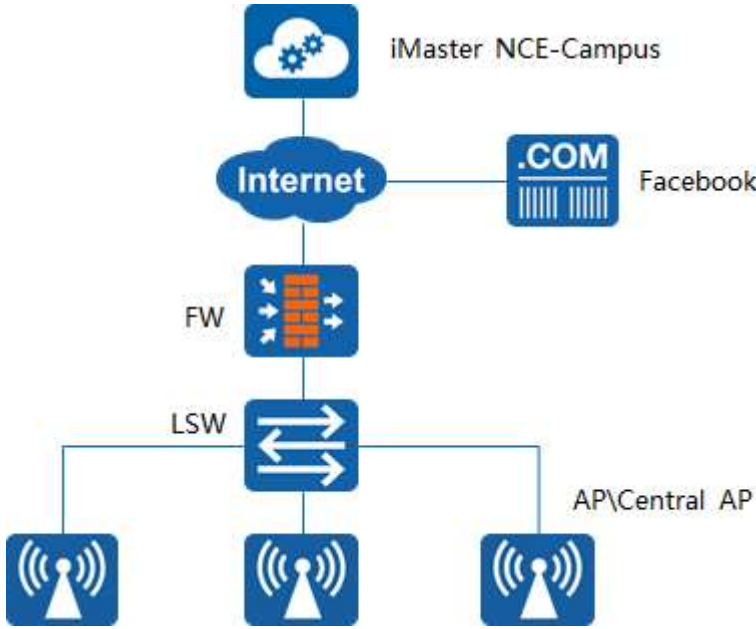


PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

### Facebook Authentication

5.10.30 Implantar autenticação de usuários nas redes wireless por:

5.10.30.3 Implementar pelo menos duas formas de autenticação que permita que o usuário obtenha acesso a rede sem a necessidade de usuário ou senha previamente cadastrados. Exemplo: Google, Office365, Facebook, Instagram, Linkedin, Twitter;

<b>Item de teste</b>	Autenticação via Facebook
<b>Objetivo do teste</b>	Verificar se o CloudCampus da Huawei suporta funcionar como servidor de portal para fornecer autenticação do Facebook para usuários Guest
<b>Configuração de teste</b>	<p>Topologia da Rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> <li>3) Tenant logado na plataforma CloudCampus.</li> <li>4) Os parâmetros da conta facebook estão configurados corretamente.</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Selecione "Admission &gt; Admission Policy &gt; Admission Settings/ Social Media Parameters", habilite "Facebook", configure "APP ID" e "APP Secret", com resultado esperado 1;</li> </ol>

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

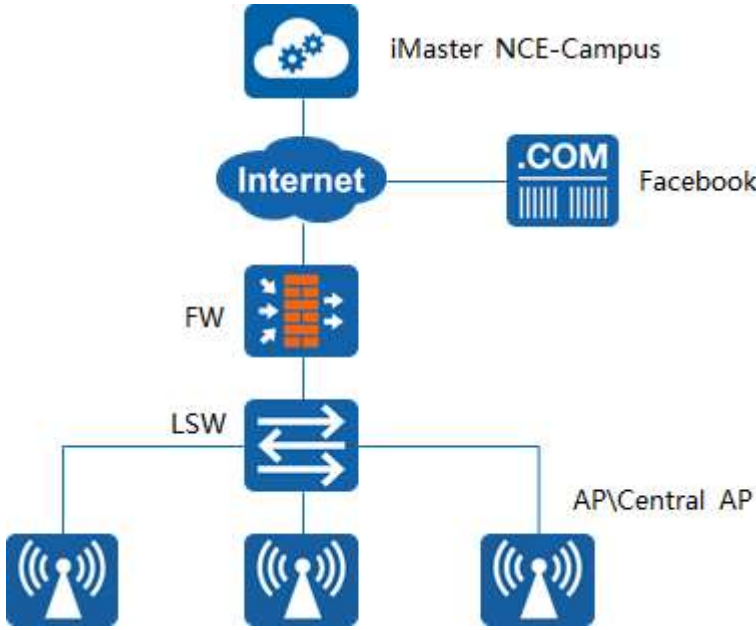
	2) Selecione "Admission > Admission Resources > Page Management" para adicionar uma página de portal customizada e confirmar a página preferida "Social Media Template" e configure outros parâmetros relacionados, com resultado esperado 2; 3) Configure o portal SSID na controladora e selecione o "Login mode" como "Facebook authentication", com resultado esperado 3; 4) Configure o Portal page push policy na controladora, vinculando o SSID e AP, selecione "Login mode" como Facebook authentication, cheque o push page e clique em "Confirm", com resultado esperado 4; 5) Após o terminal ser associado com o SSID, a autenticação Facebook pode ser engatilhada para realizar a autenticação via Portal, com resultado esperado 5; 6) O usuário acessa recursos da Internet, com resultado esperado 6.		
<b>Resultado esperado</b>	1) A configuração de parâmetros de mídia social está completa; 2) Criação com sucesso de um template customizado de push page em page customization; 3) SSID com autenticação Facebook criada com sucesso; 4) Estratégia de portal page push completa; 5) O terminal móvel pode acessar a autenticação Facebook; 6) Clicando em "Facebook Authentication", o usuário complete a autenticação via facebook e acessa a internet.		
<b>Resultado</b>			
<b>Observação</b>			
<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	

### Google Authentication

5.10.30 Implantar autenticação de usuários nas redes wireless por:

5.10.30.3 Implementar pelo menos duas formas de autenticação que permita que o usuário obtenha acesso a rede sem a necessidade de usuário ou senha previamente cadastrados. Exemplo: Google, Office365, Facebook, Instagram, LinkedIn, Twitter;

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

<b>Item de teste</b>	Google Authentication
<b>Objetivo do teste</b>	Verifique se o CloudCampus da Huawei oferece suporte para funcionar como servidor de portal para fornecer autenticação do Google para guests
<b>Configuração de teste</b>	<p>Topologia da Rede:</p>  <p>Prerequisites:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> <li>3) Tenant logado na plataforma CloudCampus.</li> <li>4) Os parâmetros da conta google estão configurados corretamente.</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Selecione "Admission &gt; Admission Policy &gt; Admission Settings/ Social Media Parameters", habilite " Google", configure "APP ID" e "APP Secret", com resultado esperado 1;</li> <li>2) Selecione "Admission &gt; Admission Resources &gt; Page Management" para adicionar a customização de página de portal e setar o tipo de página para "Social Media Template" e configure outros parâmetros relacionados, com resultado esperado 2;</li> <li>3) Configure o SSID do portal na controladora e selecione o "Login mode" como " Google authentication", com resultado esperado 3;</li> <li>4) Configure a política de push de Portal page na controladora, vinculando o SSID ao AP, selecione "Login mode" como Google authentication, cheque a página e clique em "Confirm", com resultado esperado 4;</li> </ol>

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

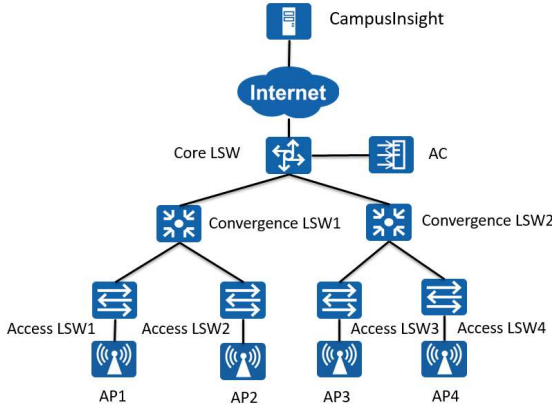
	5) Após o terminal ser associado ao SSID, a autenticação Google pode ser engatilhada para realizar a autenticação via portal, com resultado esperado 5; 6) Usuários acessam recursos da Internet, com resultado esperado 6.		
<b>Resultado esperado</b>	1) A configuração de parâmetros de mídia social está completa; 2) Criação com sucesso de um template customizado de push page em page customization; 3) SSID com autenticação Google criado; 4) Estratégia de portal page push completa; 5) O terminal móvel pode acessar a autenticação Google; 6) Clicando em " Google Authentication", o usuário complete a autenticação google e acessa a internet.		
<b>Resultado</b>			
<b>Observação</b>			
<b>Assinatura do cliente</b>		<b>Assinatura do fabricante</b>	

### Wireless Location and Heatmap

5.10.22 Deve permitir ao administrador visualizar e monitorar o mapa de cobertura da rede sem fio;

<b>Item de teste</b>	Wireless Location and Heatmap
<b>Objetivo do teste</b>	Para verificar a função de localizar terminais sem fio na topologia WLAN..

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

<p><b>Topologia da Rede:</b></p>	 <p>Prerequisites:</p> <ol style="list-style-type: none"> <li>1. O CampusInsight e o pacote de patch de localização sem fio foram instalados e o sistema está funcionando corretamente.</li> <li>2. A AC e os APs foram configurados para relatar métricas e pacotes Syslog e tem a função de localização sem fio ativada.</li> <li>3. A licença do pacote de software para localização sem fio foi configurada na página de gerenciamento de recursos para APs.</li> <li>4. O arquivo de plano de rede foi importado com sucesso e a imagem de fundo, a escala e o obstáculo foram definidos.</li> <li>5. O caminho percorrido foi planejado .</li> </ol>
<p><b>Procedimento de teste</b></p>	<ol style="list-style-type: none"> <li>1. Realizar login no CampusInsight e selecionar <b>Inventory &gt; Service Topology</b> do menu principal. Clique no ícone <b>Enter WLAN Topology</b> na esquerda. Na página de topologia de WLAN exibida, selecione um piso planejado no painel de navegação e clique <b>Wireless Location</b> no canto superior direito. Resultado esperado 1.</li> <li>2. Selecione o <b>Walkable Path</b> e clique <b>OK</b>. Resultado esperado 2.</li> <li>3. Selecione o <b>Heat Map of Pedestrian Flow</b> e clique <b>OK</b>. Resultado esperado 3.</li> <li>4. Selecionar <b>Wi-Fi Interference</b> e clique <b>OK</b>. Resultado esperado 4.</li> </ol>
<p><b>Resultado esperado</b></p>	<ol style="list-style-type: none"> <li>1. O menu <b>Configurações</b> é exibido à direita da página, no qual você pode clicar em vários botões de função para visualizar diferentes efeitos de localização.</li> <li>2. Os caminhos disponíveis em diferentes cenários são exibidos na visualização de topologia.</li> </ol>

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
PROCESSO Nº 2020.0000.604.5301  
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

	<p>3. Na topologia, um mapa de calor baseado no tráfego do cliente detectado é exibido no caminho percorrido, e o tráfego do cliente pode ser distinguido por cores diferentes.</p> <p>4. Todas as fontes e locais de interferência Wi-Fi detectados são exibidos na topologia, como Rogue APs, dispositivos ad-hoc, dispositivos de bridge e terminais sem fio.</p>	
<b>Resultado</b>		
<b>Observação</b>	Apenas alguns modelos de dispositivos WLAN suportam a função de localização sem fios. Para obter detalhes, consulte a lista de especificações.	
<b>Assinatura do cliente</b>	<b>Assinatura do fabricante</b>	