Configuração Via Script

R3005G

Versão deste manual: 1.0.0

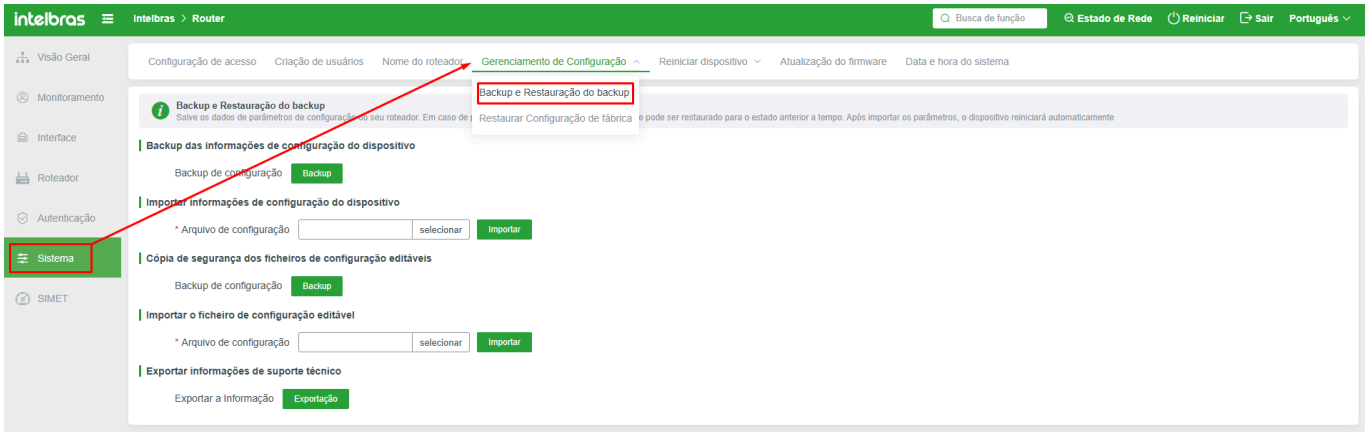
CONFIGURAÇÃO POR SCRIPT

> Todos os exemplos abaixo estão estruturados de maneira a trazer uma maior legibilidade ao usuário final, porem, na construção do script é importante que cada bloco JSON não tenha caracteres de quebra de linha (“/n”) para evitar erros de sintaxe.

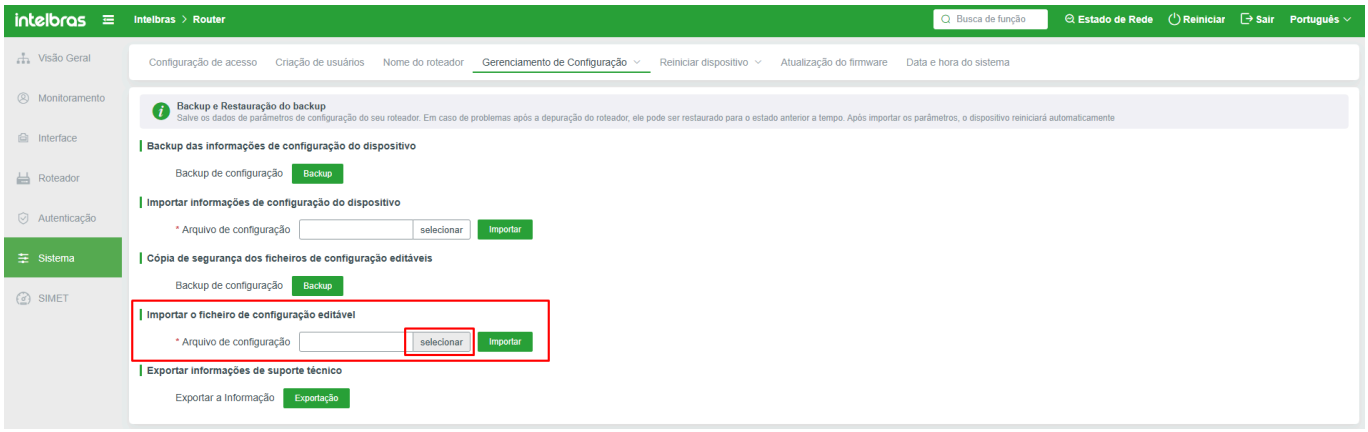
O script de configuração permite automatizar a configuração dos equipamentos de rede, facilitando a implantação de redes de grande porte. Além de agilizar o processo de manutenção e configuração, o script também garante a padronização das configurações, evitando erros humanos e garantindo a segurança da rede.

Para importar a configuração via script:

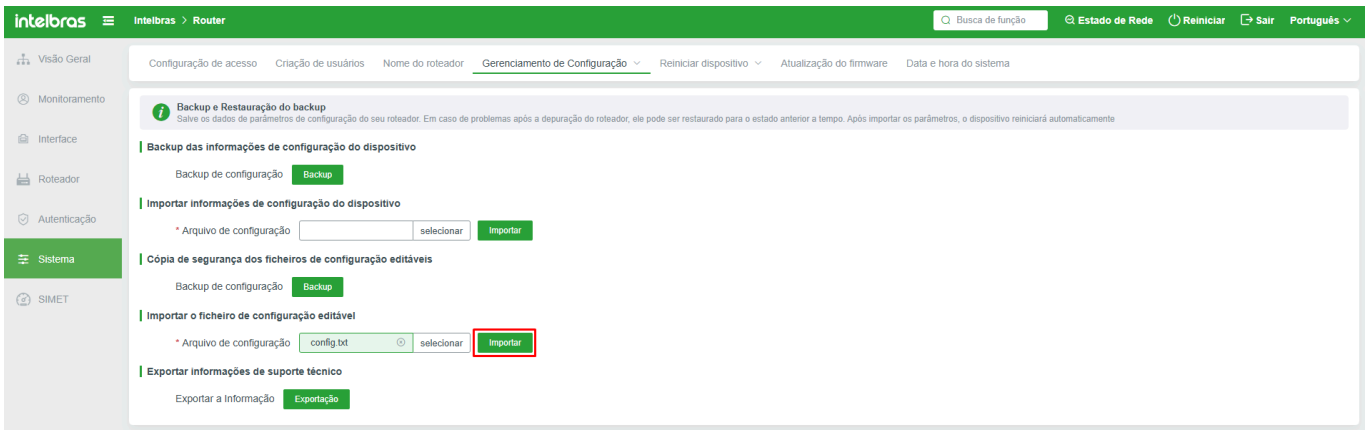
» Acesse **Sistema⇒Gerenciamento de Configuração⇒Backup e Restauração do Backup**.



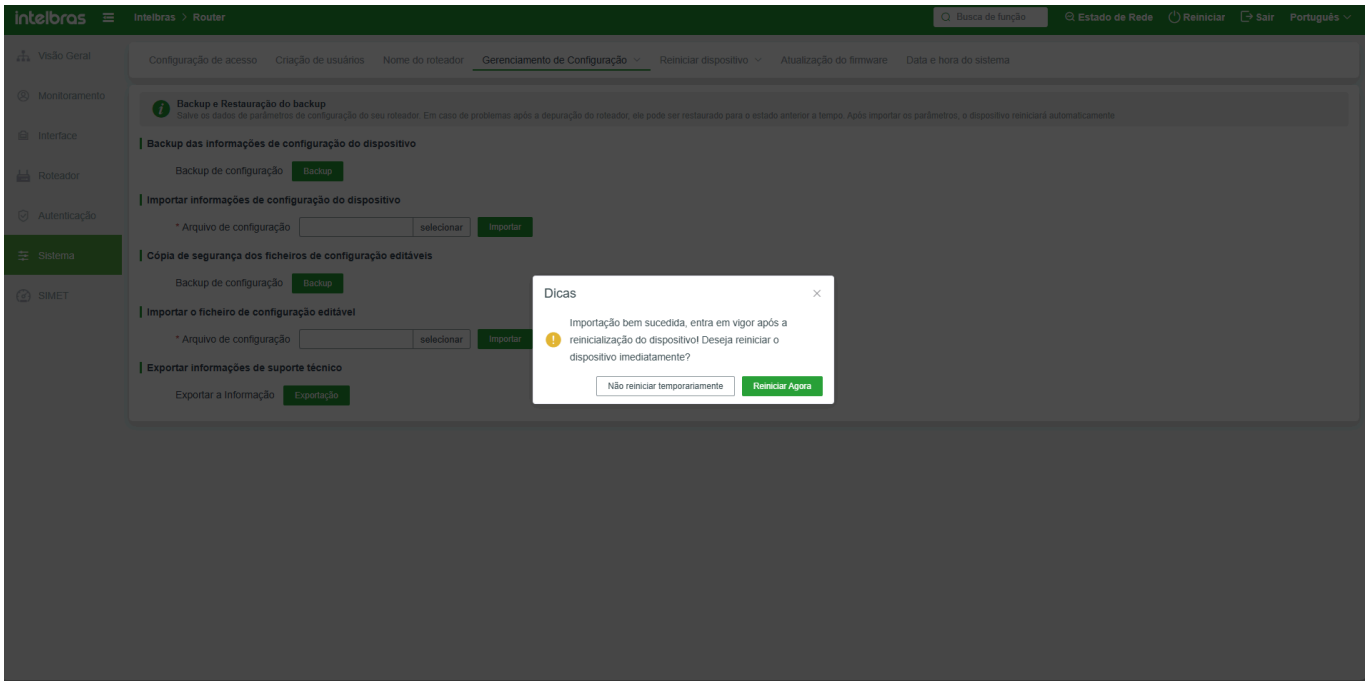
» Clique na opção ***Selecionar*** em **Importar o ficheiro de configuração editável** para abrir o gerenciador de arquivos.



» Ao selecionar o arquivo scrip, clique em **Importar**.



» Ao importar o arquivo de configuração, o dispositivo solicitará o reinício para aplicar as configurações.



Recomendações e instruções iniciais

Recomenda-se prioritizar a estruturação das configurações por meio da interface web, garantindo a adesão às melhores práticas de padronização e minimizando riscos operacionais. Esse método assegura um processo streamlined para definição de parâmetros críticos, com validação em tempo real e mitigação de inconsistências na implementação.

Para acesso preciso às funcionalidades, utilize o caminho hierárquico indicado no campo “path” para navegar até o módulo de configuração correspondente na interface administrativa. Esse caminho reflete a arquitetura lógica do sistema, permitindo:

» **Aplicação de diretivas pré-configuradas com conformidade técnica;**
» **Ajustes granulares em parâmetros específicos, alinhados aos requisitos da infraestrutura;**
» **Validação automática de sintaxe e semântica, reduzindo erros de implementação.**

A abordagem orientada por “path” não apenas otimiza a parametrização, mas também facilita a replicação de configurações em ambientes distribuídos, assegurando integridade operacional e auditabilidade.

```
1  #path=Interface - WAN settings - WAN settings
```

Ao definir a configuração padrão pela interface do dispositivo, será possível agilizar sua replicação para outros equipamentos, alterando apenas os parâmetros necessários.

Configuração de interfaces WAN

Esta configuração em JSON define os parâmetros operacionais para a interface WAN do dispositivo, estabelecendo tanto as definições básicas quanto os ajustes avançados para o gerenciamento do tráfego e a estabilidade da conexão.

Número de Interfaces WAN

O parâmetro `physics_wan_num` define que somente uma interface física WAN estará habilitada (valor “1”), o que é fundamental para manter a compatibilidade com determinadas funcionalidades, como o SIMET.

Configuração a Interface WAN1

» **Identificação e Protocolo:** A interface é identificada como ***WAN1*** e utiliza o protocolo dhcp, permitindo a obtenção dinâmica de endereço IP, gateway e demais informações de rede.

» **Desempenho e Balanceamento:** As taxas de upload e download `bandwidth_up` e `bandwidth_down` estão definidas como 0, apropriadas para cenários de WAN única. Os mecanismos de detecção de gateway e balanceamento de carga estão ativados (ambos com valor “1”), assegurando a eficiência na distribuição do tráfego.

» **Modo de Trabalho e Ajustes Avançados:** O `work_mode` está configurado como ***gateway***, onde o dispositivo realiza o NAT das conexões provenientes da LAN. O ajuste do MTU `wan_mtu` permanece em ***auto***, possibilitando a adaptação conforme as necessidades do ambiente ou orientações do ISP.

» **Parâmetros de Rede e Autenticação:** O endereço MAC está explicitamente definido como ***80:85:44:20:F8:5E***. Caso este campo estivesse vazio, o sistema utilizaria o MAC da porta WAN ou geraria um endereço aleatório. A prioridade do DNS é ajustada pelo parâmetro `dns_pri` com o valor ***low***, e o atributo dns pode ser configurado estaticamente conforme necessário.

Funções Adicionais

» **ISP:** O atributo `isp` está definido como “none”, servindo para uso futuro e devendo permanecer inalterado se não houver indicação do contrário.

» **Rediscagem Automática de WAN:** O parâmetro `time_ctrl_enable` possibilita a rediscagem automática da interface WAN, com as opções:

» 0 - Desativado;

» 3 - Rediscagem Agendada;

» 4 - Desconexão Agendada;

» 5 - Rediscagem por Intervalo.

O valor atual ***0*** indica que a rediscagem automática está desativada. O parâmetro `time_ctrl_value` define os dias da semana (de 0 para domingo a 6 para sábado) e o horário para a execução dessa rediscagem, estando configurado como `0-6;01:00`, ou seja, a rediscagem ocorrerá diariamente às 01:00, caso a função seja ativada.

» **Detecção de IPs Anormais:** O atributo `abnormal_ip_enable`, com valor ***0***, indica que a detecção de IPs anormais está desativada. Caso ativado (valor **1**), a conexão WAN será reiniciada automaticamente ao detectar um IP considerado anormal. Já o parâmetro `abnormal_ip_list` permite especificar os IPs que, quando detectados, acionariam o reinício da conexão. No exemplo, está configurado com ***0.0.0.0*** e a recomendação é deixá-lo em branco (“”), utilizando-o somente quando necessário.

Em síntese, esta configuração visa garantir uma operação robusta e eficiente da interface WAN, com um conjunto de mecanismos que permitem a adaptação automática (como a obtenção de IP via DHCP e ajuste do MTU) e o gerenciamento avançado (como rediscagem automática e detecção de anomalias), assegurando a continuidade e a estabilidade da conexão em ambientes de rede críticos.

Tabela de Parâmetros

Parâmetro	Valor	Descrição
`“physics_wan_num”`	`“1”`	Define a quantidade de WANs habilitadas. Para uso do SIMET deixe sempre a opção “1”, caso altere para outros valores o simet será desabilitado
`“wan”`	`“WAN1”`	Interface WAN a ser configurada
`“group”`	`""`	Caso haja um grupo WAN configurado, especificar qual
`"remark"`	`""`	Comentários para identificação da interface
`"proto"`	`"dhcp"`	Protocolo de conexão WAN, as opções disponíveis são: DHCP, PPPOE, I.P. estático e FECHAR. Na opção Fechar, a interface WAN é desabilitada

`"bandwidth_up"`	`"0"`	Configure a taxa de Upload do plano em Bps para informar ao algoritmo de load balance. Em caso de WAN única, deixe o valor zerado
`"bandwidth_down"`	`"0"`	Configure a taxa de Download do plano em Bps para informar ao algoritmo de load balance. Em caso de WAN única, deixe o valor zerado
`"detection"`	`"1"`	Configura a detecção de gateway (0- Desativado, 1- Ativado)
`"balanced"`	`"1"`	Configura o Balanceamento de carga (0- Desativado, 1- Ativado)
`"work_mode"`	`"gateway"`	Configure o modo da WAN. No modo “gateway”, que é o modo padrão, o dispositivo realiza o NAT das conexões LAN para a WAN. No modo “router”, o dispositivo encaminha o tráfego sem realizar o NAT.
`"wan_mtu"`	`"auto"`	Ajusta o MTU da interface WAN. Não altere este parâmetro se não for expressamente solicitado pelo seu ISP
`"dns"`	`"1.1.1.1"`	Configura estáticamente os DNSs da interface WAN
`"mac"`	`"80:85:44:20:F8:5E"`	Configura o MAC da interface WAN. Para exportar para outros dispositivos deixe o valor em branco apenas com as aspas “”. Defina um mac no formato AA:BB:CC:DD:EE:FF apenas se houver necessidade de clonar o mac de outro dispositivo para fins de autenticação em um BRAS
`"dns_pri"`	`"low"`	Ajusta a prioridade de resolução DNS. ajuste esta opção em caso de uso de Multiplas WANs para priorizar determinada WAN
`"isp"`	`"none"`	Função para uso futuro, deixe o atributo como “none”
`"time_ctrl_enable"`	`"0"`	Habilitar rediscagem automática da interface WAN (0- Desativado, 3- Rediscagem Agendada, 4- Desconexão Agendada, 5- Rediscagem por intervalo)
`"time_ctrl_value"`	`"0-6;01:00"`	Define os dias da semana de Domingo(0) a sábado(6) e o horário para realizar a rediscagem automática
`"abnormal_ip_enable"`	`"0"`	Configurar a detecção de IPs anormais (0- Desativado, 1- Ativado). ao ser detecum IP anormal ser detectado a conexão de WAN reiniciará
`"abnormal_ip_list"`	`"0.0.0.0"`	Configurar IPs a serem detectados para disparar o reinício da WAN. **DEIXE O VALOR SEMPRE EM BRANCO “ ”** usando somente quando for necessário

Exemplo de código de configuração

```
1 ##################################################################################################################################
2
3 #
4 #function=wan
5 #path=Interface - WAN settings - WAN settings
6 #
7 # If the MAC address is empty, the MAC address corresponding to the WAN port in the current parameters will be used preferentially.
8 # If no corresponding WAN port is found, a randomly generated MAC address will be used.
9
10 physics_wan_num={"num":1}
11 wan={
12      "wan":"WAN1",
13      "group":"",
14      "remark":"",
15      "proto":"dhcp",
16      "bandwidth_up":0,
17      "bandwidth_down":0,
18      "detection":"1",
19      "balanced":"1",
20      "work_mode":"gateway",
21      "wan_mtu":"auto",
22      "dns":"",
23      "mac":"80:85:44:20:F8:5E",
24      "dns_pri":"low",
25      "isp":"none",
26      "time_ctrl_enable":"0",
27      "time_ctrl_value":"",
28      "abnormal_ip_enable":"0",
29      "abnormal_ip_list":""
30 }
```

Configuração de Interfaces LAN

Esta configuração em JSON estabelece as definições para a interface LAN do dispositivo, definindo uma estrutura hierárquica onde a interface principal (LAN1) concentra os parâmetros essenciais, enquanto as interfaces LAN2, LAN3 e LAN4 são vinculadas a ela, formando um único segmento de rede.

Configuração da LAN1

- **Endereço IP e Máscara:** A LAN1 é configurada com o endereço IP 192.168.255.1 e máscara 255.255.255.0, definindo a rede local padrão para os dispositivos conectados.
- **MAC Address:** O endereço MAC é explicitamente definido como 80:85:44:20:F8:5D. Caso este campo estivesse vazio, o sistema usaria o MAC correspondente à porta LAN ou um gerado aleatoriamente.
- **Serviço DHCP:** O DHCP está habilitado, permitindo a distribuição automática de endereços IP. O pool vai de 192.168.255.10 a 192.168.255.240, com tempo de concessão de 3600 segundos. O gateway e o DNS primário apontam para 192.168.255.1, enquanto o DNS

secundário está configurado como 0.0.0.0, indicando que não há um segundo servidor DNS definido.

» **Sub-redes:** A opção de sub-rede está desativada (subnet_enable: 0) e a lista de sub-redes encontra-se vazia, o que significa que não há segmentação adicional da LAN.

» **Configuração das Interfaces Vinculadas (LAN2, LAN3 e LAN4)** Cada uma das interfaces LAN2, LAN3 e LAN4 está associada à LAN1 por meio do parâmetro `“bind” : “LAN1”`. Isso indica que elas não possuem configurações próprias de IP ou DHCP, herdando ou compartilhando os mesmos parâmetros da interface principal. Tal abordagem é útil para agregar múltiplas portas físicas em um único domínio de broadcast, facilitando o gerenciamento e a consolidação do tráfego.

Em resumo, esta configuração visa centralizar o gerenciamento da rede local na interface LAN1, que fornece os parâmetros básicos de endereçamento e distribuição de IP via DHCP, enquanto as demais interfaces operam de forma integrada, ampliando a capacidade física do segmento sem comprometer a uniformidade das configurações.

Tabela de parâmetros

Parâmetro	Valor	Descrição
`“lan”`	`“LAN1”`	Específicando a interface física conforme descrito fisicamente no dispositivo
`“bind”`	`“off”`	Parametro para vincular com outra interface física em bridge. não modifique o “off” da LAN1, pois a LAN1 é a Lan default e ocorrerá erro ao aplicar a regra
`“lan_ipaddr”`	`“192.168.255.1”`	Ip da interface
`“lan_netmask”`	`“255.255.255.0”`	Máscara de rede da interface
`“remark”`	`“”`	Comentários para identificação
`“mac”`	`“80:85:44:20:F8:5D”`	MAC Address, em caso de exportação para outros dispositivos, deixe o valor em branco “”
`“dhcp_type”`	`“on”`	“on” Habilita o Servidor DHCP, “off” Desabilita
`“dhcp_start”`	`“192.168.255.10”`	Início do Range DHCP
`“dhcp_end”`	`“192.168.255.240”`	Final do Range DHCP
`“dhcp_lease”`	`“3600”`	tempo de lease DHCP em segundos, tempo mínimo=120 máximo=172800
`“dhcp_gateway”`	`“192.168.255.1”`	Gateway DHCP(caso o dispositivo apenas forneça o dhcp e o gateway seja outro device)
`“dhcp_mask”`	`“255.255.255.0”`	Máscara do DHCP
`“dhcp_dns0”`	`“192.168.255.1”`	IP DNS Primário
`“dhcp_dns1”`	`“0.0.0.0”`	IP DNS Secundário
`“dhcp_option”`	`“”`	utilize este campo, caso precise enviar alguma option específica aos dispositivos
`“subnet_enable”`	`“0”`	Permite adicionar subredes com endereços IPs distintos na interface “0” Desativado, “1” ativado
“subnet_list”	“[]”	Específica os blocos da subnet, utilize a notação {“ip”:“10.0.0.1”,“mask”:“255.255.255.0”} dentro de cada conjunto de [] para específicar as subredes

Exemplo de Código de Configuração

```
1 ###################################################################
2 #
3 #function=lan
4 #path=Interface - LAN settings - LAN setting
5 #
6 # If the MAC address is empty, the MAC address corresponding to the LAN port in the current parameters will be used preferentially.
7 # If no corresponding LAN port is found, a randomly generated MAC address will be used.
8
9 #LAN
10 lan={
11      "lan":"LAN1",
12      "bind":"off",
13      "lan_ipaddr":"192.168.255.1",
14      "lan_netmask":"255.255.255.0",
15      "remark":"",
16      "mac":"80:85:44:20:F8:5D",
17      "dhcp_type":"on",
18      "dhcp_start":"192.168.255.10",
19      "dhcp_end":"192.168.255.240",
20      "dhcp_lease":"3600",
21      "dhcp_gateway":"192.168.255.1",
22      "dhcp_mask":"255.255.255.0",
23      "dhcp_dns0":"192.168.255.1",
24      "dhcp_dns1":"0.0.0.0",
25      "dhcp_option":"",
26      "subnet_enable":0,
27      "subnet_list":[]}
28 lan={"lan":"LAN2","bind":"LAN1"}
29 lan={"lan":"LAN3","bind":"LAN1"}
30 lan={"lan":"LAN4","bind":"LAN1"}
```

Configuração de VLAN e DHCP

Esta configuração em JSON define três VLANs distintas para segmentar o tráfego da rede em ambientes separados, cada uma com suas próprias definições de IP e parâmetros de servidor DHCP. De forma resumida:

- **VLAN 10 - Administrativo:**
  - **IP/Máscara:** 192.168.10.1 / 255.255.255.0
  - **DHCP:** Ativado com faixa de endereços de 192.168.10.100 a 192.168.10.200, lease de 3600 segundos, e gateway e DNS apontando para 192.168.10.1
- **VLAN 20 - Acadêmico:**
  - **IP/Máscara:** 192.168.20.1 / 255.255.255.0
  - **DHCP:** Ativado com faixa de endereços de 192.168.20.100 a 192.168.20.200, lease de 3600 segundos, e gateway e DNS apontando para 192.168.20.1
- **VLAN 30 - Visitantes:**
  - **IP/Máscara:** 192.168.30.1 / 255.255.255.0

» **DHCP:** Ativado com faixa de endereços de 192.168.30.100 a 192.168.30.200, lease de 3600 segundos, e gateway e DNS apontando para 192.168.30.1

Cada bloco configura um segmento de rede com endereçamento exclusivo, garantindo que dispositivos conectados recebam IPs dentro do respectivo escopo e mantendo a separação do tráfego conforme o perfil (Administrativo, Acadêmico e Visitantes). A diretiva de MAC, que utiliza o endereço definido ou, se vazio, o da porta LAN (ou um gerado aleatoriamente), reforça a integridade da identificação física da interface. Por fim, todas as VLANs estão vinculadas à interface “LAN1”, sugerindo que a segregação lógica será aplicada sobre uma mesma porta física, geralmente acompanhada de configurações de tagging em um switch gerenciável.

Esta abordagem permite um controle refinado do tráfego, segurança e eficiência na gestão dos recursos de rede, aspectos essenciais para ambientes corporativos e institucionais.

Tabela de parâmetros

Parâmetro	Valor	Descrição
“vlanid”	“10”	VLAN ID
“lan_ipaddr”	“192.168.10.1”	IP Gateway da interface
“lan_netmask”	“255.255.255.0”	Máscara de rede
“dhcp_type”	“on”	“on” Ativa o serviço DHCP “off” Desativa
“dhcp_lease”	“3600”	Tempo de Lease DHCP
“dhcp_start”	“192.168.10.100”	Primeiro IP do Range DHCP
“dhcp_end”	“192.168.10.200”	Ultimo IP do Range DHCP
“dhcp_gateway”	“192.168.10.1”	Gateway DHCP (caso o dispositivo apenas forneça o dhcp e o gateway seja outro device)
“dhcp_dns0”	“192.168.10.1”	IP do DNs Primário
“dhcp_dns1”	“8.8.8.8”	IP do DNS Secundário
“dhcp_mask”	“255.255.255.0”	Mascara do DHCP
“mac”	“00:0E:01:57:AF:CB”	MAC da interface, em caso de exportação de um dispositivo a outro verifique a real necessidade de exportar esta informação
“remark”	“Administrativo”	Comentário para identificação do serviço utilizado na vlan, para melhor organização
“dhcp_option”	“”	Utilize este campo, caso precise enviar alguma option específica para os dispositivos
“untag_port”	“LAN2”	utilize para colocar portas físicas específicas em modo untag na vlan específica
“bind”	“LAN1”	selecione em quais portas a VLAN estará configurada

Exemplo de Código de Configuração

```
#function=lan
#path=Interface - LAN settings - LAN setting
#
# If the MAC address is empty, the MAC address corresponding to the LAN port in the current parameters will be used preferentially.
# If no corresponding LAN port is found, a randomly generated MAC address will be used.


vlan={
     "vlanid":"10",
      "lan_ipaddr":"192.168.10.1",
      "lan_netmask":"255.255.255.0",
      "dhcp_type":"on",
      "dhcp_lease":3600,
      "dhcp_start":"192.168.10.100",
      "dhcp_end":"192.168.10.200",
      "dhcp_gateway":"192.168.10.1",
      "dhcp_dns0":"192.168.10.1",
      "dhcp_dns1":"8.8.8.8",
      "dhcp_mask":"255.255.255.0",
      "mac":"00:0E:01:57:AF:CB",
      "remark":"Administrativo",
      "dhcp_option":"",
      "untag_port":"",
      "bind":"LAN1"}
vlan={
      "vlanid":"20",
      "lan_ipaddr":"192.168.20.1",
      "lan_netmask":"255.255.255.0",
      "dhcp_type":"on",
      "dhcp_lease":3600,
      "dhcp_start":"192.168.20.100",
      "dhcp_end":"192.168.20.200",
      "dhcp_gateway":"192.168.20.1",
      "dhcp_dns0":"192.168.20.1",
      "dhcp_dns1":"8.8.8.8",
      "dhcp_mask":"255.255.255.0",
      "mac":"00:82:42:DA:89:BD",
      "remark":"Academico",
      "dhcp_option":"",
      "untag_port":"",
      "bind":"LAN1"}
vlan={
      "vlanid":"30",
      "lan_ipaddr":"192.168.30.1",
      "lan_netmask":"255.255.255.0",
      "dhcp_type":"on",
      "dhcp_lease":3600,
```

```
48      "dhcp_start":"192.168.30.100",
49      "dhcp_end":"192.168.30.200",
50      "dhcp_gateway":"192.168.30.1",
51      "dhcp_dns0":"192.168.30.1",
52      "dhcp_dns1":"8.8.8.8",
53      "dhcp_mask":"255.255.255.0",
54      "mac":"00:A8:43:80:37:86",
55      "remark":"Visitantes",
56      "dhcp_option":"",
57      "untag_port":"",
58      "bind":"LAN1"}
```

Configuração de Grupo de IP

Esta configuração em JSON estabelece os grupos de endereçamento IP que serão referenciados pelas regras de ACL, permitindo que o administrador de rede segmente e controle o tráfego de forma precisa e segura. Cada grupo representa um intervalo específico de endereços IP, facilitando a definição de políticas de acesso baseadas em categorias, como Administrativo, Acadêmico, Visitantes e um grupo padrão.

- **Administrativo:** Define o intervalo de IPs de 192.168.10.1 a 192.168.10.254 e possui o identificador `“1”`. Este grupo é destinado aos dispositivos e usuários com perfil administrativo, permitindo a aplicação de regras específicas para ambientes críticos.
- **Acadêmico:** Abrange o intervalo de 192.168.20.1 a 192.168.20.254, identificado pelo valor `“2”`. Este grupo segmenta os usuários acadêmicos, possibilitando políticas diferenciadas que atendam às necessidades desse ambiente.
- **Visitantes:** Configurado com o range de 192.168.30.1 a 192.168.30.254 e identificado como `“3”`, este grupo é utilizado para isolar o tráfego dos dispositivos de visitantes, contribuindo para a segurança e a organização da rede.
- **defalt:** Engloba o intervalo de 192.168.255.1 a 192.168.255.254, com o identificador `“4”`. Este grupo serve como padrão ou fallback, para dispositivos que não se enquadrem nos demais grupos definidos.

Ao definir esses grupos com os respectivos intervalos e identificadores, a configuração possibilita a referência clara e consistente nas regras de ACL, assegurando que a máscara de sub-rede e os intervalos de endereçamento sejam aplicados corretamente. Dessa forma, é possível implementar controles de acesso refinados, promovendo uma rede mais segura e bem gerenciada.

Tabela de parâmetros

Parâmetro	Valor	Descrição
`“name”`	`“Academico”`	Nome do grupo
`“ips”`	`“192.168.20.1-192.168.20.254”`	Range de endereçamento
`“id”`	`“1”`	index de sequenciamento

Exemplo de código de configuração

```
1 #
2 #function=ip_group
3 #path=Router - Behavior - IP address group
4
5
6 group={
7      "name":"Academico",
8      "ips":"192.168.20.1-192.168.20.254",
9      "id":"2"}
10 group={
11      "name":"Visitantes",
12      "ips":"192.168.30.1-192.168.30.254",
13      "id":"3"}
14 group={
15      "name":"Administrativo",
16      "ips":"192.168.10.1-192.168.10.254",
17      "id":"1"}
18 group={
19      "name":"default",
20      "ips":"192.168.255.1-192.168.255.254",
21      "id":"4"}
```

Configuração de ACL

Esta configuração em JSON estabelece as regras do firewall por meio de ACL (Access Control List) para bloquear o tráfego de pacotes entre diferentes VLANs, garantindo que usuários conectados a uma VLAN não tenham acesso a outras. Em outras palavras, o objetivo é evitar a comunicação direta LAN-to-LAN pelo roteador, promovendo uma segregação efetiva dos ambientes.

Configuração Geral

» **Modo Básico:** Define o modo padrão do sistema como “accept”, ou seja, na ausência de regras específicas, o tráfego seria aceito. Contudo, as regras ACL possuem prioridade e, quando acionadas, realizam a ação de “drop” para descartar os pacotes indesejados.

Detalhamento das Regras ACL

» **AdministrativoBlock:**

» **Origem:** 192.168.10.1-192.168.10.254 (VLAN Administrativo)

» **Destino:** 192.168.20.1-192.168.20.254 e 192.168.30.1-192.168.30.254 (VLAN Acadêmico e Visitantes)

» **Ação:** drop

» **Prioridade:** 30000

» **Logs:** Ativados

» **Aplicação Temporal:** Configurada para `“all”`, ou pode ser personalizada com um intervalo específico, conforme a necessidade.

» **AcademicoBlock:**

» **Origem:** 192.168.20.1-192.168.20.254 (VLAN Acadêmico)

» **Destino:** 192.168.10.1-192.168.10.254 e 192.168.30.1-192.168.30.254 (VLAN Administrativo e Visitantes)

» **Ação:** drop

» **Prioridade:** 30000

» **Logs:** Ativados

» **Aplicação Temporal:** `"all"`

» **VisitantesBlock:**

» **Origem:** 192.168.30.1-192.168.30.254 (VLAN Visitantes)

» **Destino:** 192.168.10.1-192.168.10.254 e 192.168.20.1-192.168.20.254 (VLAN Administrativo e Acadêmico)

» **Ação:** drop

» **Prioridade:** 30000

» **Logs:** Ativados

» **Aplicação Temporal:** `"all"`

» **defaltBlock:**

» **Origem:** 192.168.255.1-192.168.255.254 (VLAN Default)

» **Destino:** 192.168.10.1-192.168.10.254 e 192.168.20.1-192.168.20.254 (VLAN Administrativo e Acadêmico)

» **Ação:** drop

» **Prioridade:** 30000

» **Logs:** Ativados

» **Aplicação Temporal:** `"all"`

Com essa abordagem, o firewall atua de forma preventiva, bloqueando tentativas de comunicação entre as VLANs e, assim, mantendo a integridade e a segurança do ambiente. Essa segmentação é fundamental para evitar que tráfegos indesejados ou não autorizados transitem entre áreas distintas, protegendo os dados e isolando os diferentes perfis de usuários dentro da rede.

Tabela de parâmetros

Parâmetro	Valor	Descrição
`“basic_mode”`	`“accept”`	Modo padrão do sistema (accept/drop)
`“acl_description”`	`“AdministrativoBlock”`	Nome da regra de controle de acesso
`“acl_enable”`	`“1”`	Habilita regra (1- ativo, 0- inativo)
`“log_enable”`	`“1”`	Registro em log (1- ativo, 0- inativo)
`“priority”`	`“30000”`	Prioridade de processamento da regra
`“acl_mode”`	`“drop”`	Ação executada (drop/permit)
`“source_ip”`	`“192.168.10.1-192.168.10.254”`	Faixa de IPs locais
`“remote_ip”`	`“192.168.20.1-192.168.20.254, 192.168.30.1-192.168.30.254”`	Faixa de IPs remoto
`“time_policy”`	`“0-6;09:00:00-18:00:00”`	horários para a regra ser aplicada “0-6” dias da semana, “09:00:00” hora de início, “18:00:00” hora de encerramento da vigencia. para que a regra sempre esteja aplicada utilize “all” Lembre-se de usar exatamente a formatação que está dentro do campo valor

Exemplo de código de configuração

```
basics={"mode":"accept"}
acl={
"describe":"AdministrativoBlock",
"enable":1,"log":"1",
"priority":"30000",
"mode":"drop",
"source":{"type":"ip", "value":"192.168.10.1-192.168.10.254"},
"remote":{
"ip_range":"",
"ip_range_not":0,
"ip":"192.168.20.1-192.168.20.254,192.168.30.1-192.168.30.254",
"port":"",
"dns":"0"},
"time":{"type":"all"}
}
acl={
     "describe":"AcademicoBlock",
     "enable":1,"log":"1",
     "priority":"30000",
     "mode":"drop",
     "source":{"type":"ip", "value":"192.168.20.1-192.168.20.254"},
     "remote":{
       "ip_range":"",
       "ip_range_not":0,
       "ip":"192.168.10.1-192.168.10.254,192.168.30.1-192.168.30.254",
       "port":"",
       "dns":"0"},
   "time":{"type":"all"}
   }
acl={
     "describe":"VisitantesBlock",
     "enable":1,"log":"1",
     "priority":"30000",
     "mode":"drop",
     "source":{"type":"ip","value":"192.168.30.1-192.168.30.254"},
     "remote":{
       "ip_range":"",
       "ip_range_not":0,
       "ip":"192.168.10.1-192.168.10.254,192.168.20.1-192.168.20.254",
       "port":"",
       "dns":"0"},
   "time":{"type":"all"}
   }
acl={
     "describe":"defaultBlock",
     "enable":1,"log":"1",
     "priority":"30000",
     "mode":"drop",
```

```
49      "source":{"type":"ip","value":"192.168.255.1-192.168.255.254"},
50      "remote":{
51        "ip_range":"",
52        "ip_range_not":0,
53        "ip":"192.168.10.1-192.168.10.254,192.168.20.1-192.168.20.254",
54        "port":"",
55        "dns":"0"},
56    "time":{"type":"all"}
57    }
```

Bloqueio de Dominio

Para restringir o acesso a sites específicos dentro da rede, é necessário configurar a lista de domínios bloqueados. Esse mecanismo permite que o administrador de rede impeça conexões para serviços não autorizados, garantindo maior controle sobre o tráfego de saída.

No exemplo abaixo, Esta configuração em JSON mostra como configurar domínios relacionados a jogos online, redes sociais, serviços de streaming e compartilhamento de arquivos. O bloqueio pode ser implementado diretamente no firewall ou em um sistema de filtragem de DNS, impedindo a resolução desses endereços e, consequentemente, o acesso aos sites especificados.

Código de exemplo

```
1 dns=[
2      "intl.garena.com",
3      "discord.com",
4      "tv.apple.com",
5      "hola.org",
6      "www.garena.sg",
7      "www.garena.vn",
8      "www.garena.co.th",
9      "www.garena.ph",
10      "www.garena.my",
11      "www.garena.co.id",
12      "www.paramountplus.com.br",
13      "www.starplus.com.br",
14      "www.starplus.com",
15      "www.kwai.com.br",
16      "www.kwai.com",
17      "www.lionsgateplus.com.br",
18      "www.lionsgateplus.com",
19      "www.primevideo.com",
20      "www.disneyplus.com",
21      "www.tiktok.com",
22      "www.hbomax.com",
23      "www.icloud.com",
24      "www.bittorrent.com",
25      "www.4shared.com"
26 ]
```

Configuração de Acesso Remoto

A configuração de acesso remoto permite que administradores gerenciem o dispositivo de maneira segura através da rede local (LAN) ou de redes externas (WAN). Esse tipo de configuração é essencial para a administração remota de equipamentos de rede, possibilitando ajustes e monitoramento sem a necessidade de acesso físico ao dispositivo.

No entanto, o acesso remoto via WAN deve ser configurado com cautela, garantindo que apenas IPs autorizados possam estabelecer conexão, evitando exposições desnecessárias e riscos de segurança.

Considerações Técnicas

» **Segurança:** O acesso remoto via WAN pode representar um risco significativo caso seja configurado de forma indiscriminada. Recomenda-se restringir o acesso a IPs específicos, evitando exposições desnecessárias.
» **Uso de portas seguras:** A escolha da porta de acesso remoto (remote_port) deve evitar portas comumente utilizadas (ex: 22, 23, 80, 443, 3389), pois essas portas são frequentemente alvos de ataques automatizados.
» **Filtragem de IPs:** O parâmetro source_restrictions permite definir quais IPs ou blocos de IPs podem acessar remotamente o dispositivo. Recomenda-se evitar valores como 0.0.0.0/0, pois isso libera o acesso para qualquer origem.
» **Monitoramento de Logs:** Caso o acesso remoto esteja ativado, é essencial monitorar os logs do sistema para identificar tentativas de acesso não autorizadas e possíveis tentativas de ataque.
» **Firewall e NAT:** Em redes protegidas por firewall, é necessário garantir que a porta especificada em remote_port esteja aberta e devidamente encaminhada para o dispositivo de destino.

Essa configuração permite um gerenciamento remoto eficiente do equipamento, garantindo flexibilidade na administração, mas requer atenção redobrada quanto à segurança para evitar acessos indevidos e vulnerabilidades na rede.

Para a configuração do acesso ao dispositivo, tanto local quanto remoto, deve ser seguido o padrão abaixo:

Estrutura de Configuração

A configuração é composta por quatro parâmetros fundamentais que controlam o comportamento do acesso remoto, tanto via LAN quanto via WAN.

Tabela de parâmetros

Parâmetro	Valor	Descrição
`“lan_port”`	`“80”`	Porta de acesso via LAN
`“remote_enable”`	`“1”`	Ativa o acesso remoto (1 para ativar, 0 para desativar)
`“remote_port”`	`“15555”`	Porta de acesso externo via WAN
`“source_restrictions”`	`“0.0.0.0/0,200.200.200.0/24”`	Blocos de IP liberados para acesso via WAN

Exeplo de Código de Configuração

```
1 basics={
2      "lan_port":80,
3      "remote_enable":1,
4      "remote_port":15555,
5      "source_restrictions":"0.0.0.0/0,200.200.200.0/24"
6      }
```

Habilitar a Autenticação Via Radius

Para configurar a autenticação via Radius, utilize o parâmetro abaixo dentro do código de configuração.

Tabela de parâmetros

Parâmetro	Valor	Descrição
`“radius”`	`“0”`	Habilitar a autenticação via Radius (0- Desativado, 1- Ativado)

Exemplo de código de configuração

```
1 basics={
2      "radius":0
3      }
```

Configuração Radius

A configuração apresentada refere-se à implementação de um servidor RADIUS (Remote Authentication Dial-In User Service) para gerenciar autenticação, autorização e contabilização de usuários em uma rede. O RADIUS é amplamente utilizado para reforçar a segurança em redes sem fio, garantindo que apenas usuários autorizados tenham acesso aos recursos da rede.

No contexto desta configuração, diversos parâmetros críticos são definidos para assegurar o funcionamento adequado do servidor RADIUS. O parâmetro state indica o estado operacional do servidor, onde 0 representa inativo e 1 ativo. Os campos `auth_addr`, `web_auth_addr` e `billing_addr` especificam os endereços IP e portas dos servidores responsáveis pela autenticação, autenticação via web e contabilização, respectivamente, seguindo o formato IP:porta. A `offline_port` designa a porta utilizada para comunicação offline, enquanto `communication_key` estabelece a chave secreta compartilhada entre o cliente RADIUS e o servidor para criptografar as mensagens transmitidas, reforçando a segurança da comunicação.

`nas_identity` identifica de forma única o NAS (Network Access Server) na infraestrutura RADIUS, sendo essencial para a distinção entre diferentes dispositivos de acesso na rede. O parâmetro `interface` determina qual interface de rede, como WAN1, será utilizada para o tráfego RADIUS. A opção `get_user` define se a lista de usuários será obtida diretamente do servidor RADIUS (1 para sim, 0 para não), enquanto `auth_mode` especifica o método de autenticação adotado: 0 para certificado, 1 para RADIUS e 2 para autenticação local precedendo o RADIUS.

A correta configuração desses parâmetros é vital para garantir que o servidor RADIUS opere de maneira eficiente e segura, proporcionando um controle rigoroso sobre o acesso à rede e monitoramento adequado das atividades dos usuários.

Tabela de parâmetros

Parâmetro	Valor	Descrição
“state”	“0”	Estado (0- inativo, 1- ativo)
“auth_addr”	“xxx.xxx.xxx.xxx:1812”	Endereço de autenticação
“web_auth_addr”	“xxx.xxx.xxx.xxx:1812”	Endereço para autenticação via web
“billing_addr”	“xxx.xxx.xxx.xxx:1813”	Endereço para faturamento
“offline_port”	“3799”	Porta offline
“communication_key”	“123456”	Chave de comunicação
“nas_identity”	“Intelbras”	Identidade do NAS
“interface”	“WAN1”	Interface de rede utilizada
“get_user”	“0”	Obter lista de usuários do Servidor (0- não, 1- sim)
“auth_mode”	“1”	Modo de autenticação: (0- certificado, 1- Radius, 2- Local antes do Radius)

Exemplo de Código de Configuração

```
radius={
    "state":1,
    "auth_addr":"10.10.10.100:1812",
    "web_auth_addr":"10.10.10.100:1812",
    "billing_addr":"10.10.10.100:1813",
    "offline_port":3799,
    "communication_key":"chavecomplexa",
    "nas_identity":"SOO-12345678",
    "interface":"WAN1",
     "get_user":0,
     "auth_mode":1
     }
```

Configuração de Usuários Locais

A configuração apresentada abaixo refere-se à criação e gerenciamento de usuários locais no dispositivo, garantindo controle de acesso e permissões específicas para cada perfil. Essa configuração permite tanto a definição de credenciais em texto plano quanto a utilização de chaves encriptadas, fornecendo uma abordagem flexível e segura para administração de usuários.

No contexto desta implementação, os parâmetros `encrypt_user` e `encrypt_passwd` armazenam as credenciais do usuário de forma encriptada, sendo exportadas diretamente pelo dispositivo. Essa prática reforça a segurança, impedindo que credenciais sejam expostas em texto claro. Caso o usuário opte por definir manualmente o nome e a senha, os campos encriptados devem ser deixados em branco. Essa abordagem garante compatibilidade com diferentes cenários de configuração, evitando conflitos ao importar dados para outro dispositivo

> Ao exportar a configuração de outro roteador não modifique sob nenhuma hipótese, nenhum parâmetro dos campos `encrypt_user` e `encrypt_passwd` pois poderá inutilizar o acesso ao dispositivo, sendo necessário redefiní-lo as configurações de fábrica

Os parâmetros `user` e `passwd` permitem a inserção das credenciais em texto plano, sendo recomendados apenas para a configuração inicial de usuários. Uma vez que as credenciais são configuradas, o ideal é utilizar os valores encriptados gerados pelo próprio sistema. Essa prática minimiza riscos de exposição e garante maior segurança ao gerenciamento de acessos.

O parâmetro `role` define o nível de permissão do usuário no sistema. O valor `Administrators` concede acesso total às configurações do dispositivo, permitindo modificações e ajustes avançados. Já a opção `guest` restringe as permissões, permitindo apenas a visualização de configurações sem possibilidade de alteração. Essa diferenciação de privilégios assegura que somente usuários autorizados possam realizar mudanças críticas na infraestrutura do sistema.

A correta configuração desses parâmetros é essencial para garantir um ambiente seguro e bem administrado, permitindo um controle granular sobre os acessos ao dispositivo e prevenindo modificações indevidas por usuários não autorizados.

Tabela de parâmetros

Parâmetro	Valor	Descrição
`"encrypt_user"`	`“DS93rp5htvmcSw==”`	Chave encriptada do usuário, exportada pelo dispositivo. Não Modifique este parâmetro se for exportar para outro device. Caso coloque o usuário em texto plano, por favor deixe o campo em branco “”
`"encrypt_passwd"`	`"QVRUvV8oyU="`	Chave encriptada da senha, exportada pelo dispositivo. Não Modifique este parâmetro se for exportar para outro device. Caso coloque o usuário em texto plano, por favor deixe o campo em branco “”
`"user"`	`“usuario”`	Nome de usuário em texto plano, use caso queira configurar um usuário pela primeira vez. Prefira usar o parâmetro encriptado exportado pelo dispositivo. Caso tenha um usuário encriptado configurado, deixe o campo em branco“”
`"passwd"`	`“senhacomplexa”`	Senha do usuário em texto plano, use caso queira configurar uma senha pela primeira vez. Prefira usar o parâmetro encriptado exportado pelo dispositivo. Caso tenha um senha encriptada configurada, deixe o campo em branco“”
`"role"`	`“Administrators”`	Função do usuário (Administrators- Permissão total para alteração de configurações; guest- usuário com permissões apenas de visualização)

Exeplo de Código de Configuração

```
user={
     "encrypt_user":"",
     "encrypt_passwd":"",
     "user":"usuario",
     "passwd":"senhacomplexa",
     "role":"Administrators"
     }
user={
     "encrypt_user":"uyIz21VtF3N7CErRtY8Ssg==",
      "encrypt_passwd":"t/ffuYNFBY6oyeG2R3WwsA==",
      "user":"",
      "passwd":"",
      "role":"Administrators"
      }
user={
      "encrypt_user":"SIM3gJ3ZoLYS5L7wlFCaaA==",
      "encrypt_passwd":"t/ffuYNFBY6oyeG2R3WwsA==",
      "user":"",
      "passwd":"",
      "role":"guest"
      }
```

Exemplo de Configuração Completa Via Script

A seguir, apresenta-se um exemplo de configuração completa do dispositivo, estruturado em um script padrão adaptado ao cenário proposto. Esse script integra de forma otimizada todas as definições discutidas anteriormente, garantindo um ambiente seguro, gerenciável e alinhado às melhores práticas de configuração. Cada parâmetro foi cuidadosamente ajustado para assegurar compatibilidade, eficiência operacional e reforço dos mecanismos de controle e segurança do sistema.

> A configuração abaixo está estruturada de maneira a trazer maior legibilidade do documento, porém na execução final deve-se atentar para que não haja caracteres de quebra de linha (/n)(/t) para evitar erros de sintaxe
> Recomenda-se que as configurações sejam geradas nos respectivos menus web para melhor assertividade do padrão e apenas proceder as alterações dos campos que forem necessários.

Exemplo de Código de Configuração Completa

```
#
# Export Date : 2025-02-28 14:19:27
# Model       : R3005G
# SN          : MWDM08003883A
# SVN         : 89555
# Version     : 25.02.20V
# Build Time  : 2025-02-19 17:59:57
#####################################################################

#
#function=time_group
#path=Router - Behavior - Time group

#####################################################################

#
#function=ip_group
#path=Router - Behavior - IP address group

group={
      "name":"Academico",
      "ips":"192.168.20.1-192.168.20.254",
      "id":"2"
      }
group={
      "name":"Visitantes",
      "ips":"192.168.30.1-192.168.30.254",
      "id":"3"
      }
group={
      "name":"Administrativo",
      "ips":"192.168.10.1-192.168.10.254",
      "id":"1"
      }
group={
      "name":"default",
      "ips":"192.168.255.1-192.168.255.254",
      "id":"4"
      }
#####################################################################

#
#function=dns_group
#path=Router - Advanced - DNS policy - DNS group

basics={
      "update":0
      }
```

```
49 ####################################################################
50
51 #
52 #function=addr_range
53 #path=Interface - Policy routing - Address range
54
55 range={
56       "Custom1_enable":0,
57       "Custom1":[]
58       }
59 range={
60       "Custom2_enable":0,
61       "Custom2":[]
62       }
63 ####################################################################
64
65 #
66 #function=wan_extend
67 #path=Interface - WAN settings - WAN extend
68
69 basics={
70       "enable":0,
71       "native":1
72       }
73 ####################################################################
74
75 #
76 #function=multi_dial
77 #path=Interface - WAN settings - MultiDial
78
79 basics={"enable":0}
80 ####################################################################
81
82 #
83 #function=wan
84 #path=Interface - WAN settings - WAN settings
85 #
86 # If the MAC address is empty, the MAC address corresponding to the WAN port in the current parameters will be
used preferentially.
87 # If no corresponding WAN port is found, a randomly generated MAC address will be used.
88
89 physics_wan_num={"num":2}
90 wan={
91       "wan":"WAN1",
92       "group":"",
93       "remark":"",
94       "proto":"dhcp",
95       "bandwidth_up":0,
96       "bandwidth_down":0,
```

```
97       "detection":"1",
98       "balanced":"1",
99       "work_mode":"gateway",
100       "wan_mtu":"auto",
101       "dns":"",
102       "mac":"80:85:44:20:F8:5E",
103       "dns_pri":"low",
104       "isp":"none",
105       "time_ctrl_enable":"0",
106       "time_ctrl_value":"",
107       "abnormal_ip_enable":"0",
108       "abnormal_ip_list":""
109       }
110 ###################################################################
111
112 #
113 #function=lan
114 #path=Interface - LAN settings - LAN setting
115 #
116 # If the MAC address is empty, the MAC address corresponding to the LAN port in the current parameters will be
used preferentially.
117 # If no corresponding LAN port is found, a randomly generated MAC address will be used.
118
AN1",
122       "bind":"off",
123       "lan_ipaddr":"192.168.255.1",
124       "lan_netmask":"255.255.255.0",
125       "remark":"",
126       "mac":"80:85:44:20:F8:5D",
127       "dhcp_type":"on",
128       "dhcp_start":"192.168.255.10",
129       "dhcp_end":"192.168.255.240",
130       "dhcp_lease":"3600",
131       "dhcp_gateway":"192.168.255.1",
132       "dhcp_mask":"255.255.255.0",
133       "dhcp_dns0":"192.168.255.1",
134       "dhcp_dns1":"0.0.0.0",
135       "dhcp_option":"",
136       "subnet_enable":0,
137       "subnet_list":[]
138       }
139 lan={
140       "lan":"LAN2",
141       "bind":"LAN1"
142       }
143 lan={
144       "lan":"LAN3"
```

```
144       "lan":"LAN3",
145       "bind":"LAN1"
146       }
147 lan={
148       "lan":"LAN4",
149       "bind":"LAN1"
150       }
151
152 #VLAN
153 vlan={
154       "vlanid":"10",
155       "lan_ipaddr":"192.168.10.1",
156       "lan_netmask":"255.255.255.0",
157       "dhcp_type":"on",
158       "dhcp_lease":3600,
159       "dhcp_start":"192.168.10.100",
160       "dhcp_end":"192.168.10.200",
161       "dhcp_gateway":"192.168.10.1",
162       "dhcp_dns0":"192.168.10.1",
163       "dhcp_dns1":"8.8.8.8",
164       "dhcp_mask":"255.255.255.0",
165       "mac":"00:0E:01:57:AF:CB",
166       "remark":"Administrativo",
167       "dhcp_option":"",
168       "untag_port":"",
169       "bind":"LAN1,LAN2,LAN3,LAN4"
170       }
171 vlan={
172       "vlanid":"20",
173       "lan_ipaddr":"192.168.20.1",
174       "lan_netmask":"255.255.255.0",
175       "dhcp_type":"on",
176       "dhcp_lease":3600,
177       "dhcp_start":"192.168.20.100",
178       "dhcp_end":"192.168.20.200",
179       "dhcp_gateway":"192.168.20.1",
180       "dhcp_dns0":"192.168.20.1",
181       "dhcp_dns1":"8.8.8.8",
182       "dhcp_mask":"255.255.255.0",
183       "mac":"00:82:42:DA:89:BD",
184       "remark":"Academico",
185       "dhcp_option":"",
186       "untag_port":"",
187       "bind":"LAN1,LAN2,LAN3,LAN4"
188       }
189 vlan={
190       "vlanid":"30",
191       "lan_ipaddr":"192.168.30.1",
192       "lan_netmask":"255.255.255.0",
```

```
193       "dhcp_type":"on",
194       "dhcp_lease":3600,
195       "dhcp_start":"192.168.30.100",
196       "dhcp_end":"192.168.30.200",
197       "dhcp_gateway":"192.168.30.1",
198       "dhcp_dns0":"192.168.30.1",
199       "dhcp_dns1":"8.8.8.8",
200       "dhcp_mask":"255.255.255.0",
201       "mac":"00:A8:43:80:37:86",
202       "remark":"Visitantes",
203       "dhcp_option":"",
204       "untag_port":"",
205       "bind":"LAN1,LAN2,LAN3,LAN4"
206       }
207 ###################################################################
208
209 #utilize caso precise fixar um IP em algum device específico internamente, necessário obter o mac previamente
210 #function=arp_bind
211 #path=Router - Security - ARP list
212
213 arp={
214       "describe":"DESKTOP-9A68P67",
215       "ip":"192.168.255.11",
216       "mac":"C0:25:A5:5A:5D:7D",
217       "interface":"LAN",
218       "type":"dynamic"
219       }
220
221 ###################################################################
222
223 #
224 #function=nat
225 #path=Router - Advanced - Port mapping
226
227 basics={
228       "loopback":1,
229       "fullcone":0}
230 ###################################################################
231
232 #
233 #function=ovpn
234 #path=Router - VPN - OVPN
235
236 ovpn={
237       "mode":"client",
238       "proto":"tcp",
239       "keepalive":60,
240       "tls":0,
241       "tls_auth":"",
```

```
242       "cipher":"BF-CBC",
243       "auth":"SHA1",
244       "mtu":1400,
245       "client_mode":"rt",
246       "private_key_passwd":"",
247       "username":"",
248       "password":"",
249       "server_addr":""
250       }
251
252 #user
253
254 #certificate base encode
255 cert={"ca_crt":""}
256 cert={"dh1024_pem":""}
257 cert={"server_crt":""}
258 cert={"server_key":""}
259 cert={"client_crt":""}
260 cert={"client_key":""}
261 ####################################################################
262
263 #
264 #function=acl
265 #path=Router - Security - Access control
266
267 basics={"mode":"accept"}
268 acl={
269       "describe":"AdministrativoBlock",
270       "enable":1,"log":"1",
271       "priority":"30000",
272       "mode":"drop",
273       "source":{"type":"ip", "value":"192.168.10.1-192.168.10.254"},
274       "remote":{
275         "ip_range":"",
276         "ip_range_not":0,
277         "ip":"192.168.20.1-192.168.20.254,192.168.30.1-192.168.30.254",
278         "port":"",
279         "dns":"0"},
280       "time":{"type":"all"}
281       }
282 acl={
283       "describe":"AcademicoBlock",
284       "enable":1,"log":"1",
285       "priority":"30000",
286       "mode":"drop",
287       "source":{"type":"ip", "value":"192.168.20.1-192.168.20.254"},
288       "remote":{
289         "ip_range":"",
290         "ip_range_not":0
```

```
290          "ip_range_not":0,
291          "ip":"192.168.10.1-192.168.10.254,192.168.30.1-192.168.30.254",
292          "port":"",
293          "dns":"0"},
294        "time":{"type":"all"}
295        }
296 acl={
297        "describe":"VisitantesBlock",
298        "enable":1,"log":"1",
299        "priority":"30000",
300        "mode":"drop",
301        "source":{"type":"ip","value":"192.168.30.1-192.168.30.254"},
302        "remote":{
303          "ip_range":"",
304          "ip_range_not":0,
305          "ip":"192.168.10.1-192.168.10.254,192.168.20.1-192.168.20.254",
306          "port":"",
307          "dns":"0"},
308        "time":{"type":"all"}
309        }
310 acl={
311        "describe":"defaultBlock",
312        "enable":1,"log":"1",
313        "priority":"30000",
314        "mode":"drop",
315        "source":{"type":"ip","value":"192.168.255.1-192.168.255.254"},
316        "remote":{
317          "ip_range":"",
318          "ip_range_not":0,
319          "ip":"192.168.10.1-192.168.10.254,192.168.20.1-192.168.20.254",
320          "port":"",
321          "dns":"0"},
322        "time":{"type":"all"}
323        }
324 ##################################################################
325
326 #
327 #function=policy
328 #path=Interface - Policy routing
329
330 ##################################################################
331
332 #
333 #function=nat_one_by_one
334 #path=Router - Advanced - NAT conversion - NAT one to one
335
336 ##################################################################
337
338 #
```

```
#function=dns_acc
#path=Router - Behavior - Domain name - Domain name filtering

basics={"mode":"accept"}
dns=[
      "intl.garena.com",
      "discord.com",
      "tv.apple.com",
      "hola.org",
      "www.garena.sg",
      "www.garena.vn",
      "www.garena.co.th",
      "www.garena.ph",
      "www.garena.my",
      "www.garena.co.id",
      "www.paramountplus.com.br",
      "www.starplus.com.br",
      "www.starplus.com",
      "www.kwai.com.br",
      "www.kwai.com",
      "www.lionsgateplus.com.br",
      "www.lionsgateplus.com",
      "www.primevideo.com",
      "www.disneyplus.com",
      "www.tiktok.com",
      "www.hbomax.com",
      "www.icloud.com",
      "www.bittorrent.com",
      "www.4shared.com"
      ]

######################################################################

#
#function=web_access
#path=System - Access setting
#
# source_restrictions: Access source restrictions, multiple ips are separated by commas
# Format: ip,ip-ip,ip/mask,domain
# e.g: 0.0.0.0/0,192.168.2.2,192.168.1.1-192.168.1.254,www.google.com

basics={
      "lan_port":80,
      "remote_enable":1,
      "remote_port":8080,
      "source_restrictions":"0.0.0.0/0"
      }
######################################################################

```

```
388 #
389 #function=radius
390 #path=Auth - Radius setting
391
392 radius={
393       "state":0,
394       "auth_addr":"",
395       "web_auth_addr":"",
396       "billing_addr":"",
397       "offline_port":3799,
398       "communication_key":"123456",
399       "nas_identity":"Intelbras",
400       "interface":"WAN1",
401       "get_user":0,"auth_mode":1
402       }
403 ###################################################################
404
405 #
406 #function=multi_user
407 #path=System - Access setting
408 #
409 # Please do not modify the ``encrypt_user` and `encrypt_passwd` fields as they are encrypted. However, you can import them as-is to other devices.
410 # If you need to modify or add a new user, please use the `user` and `passwd` fields, which are in plain text and not encrypted.
411 # The `user` and `passwd` fields need to meet certain complexity requirements to ensure security. For more information, please refer to the product manual.
412 # user: Please do not use common accounts. (such as `admin`,`root`,`guest`,`abc123`,`1q2w3e4r`...)
413 # passwd: The password must contain the following content:
414 #     At least 10 characters
415 #     At least 2 uppercase letters
416 #     At least 1 lowercase letter
417 #     At least 2 digits
418 #     At least 2 special characters
419 #     Cannot use continuous sequences (such as AbCd, 123)
420 #     Continuous identical characters cannot exceed two times (such as 000, aaa)
421 #     Cannot use prohibited password
422
423 basics={"radius":0}
424 user={
425       "encrypt_user":"",
426       "encrypt_passwd":"",
427       "user":"usuario",
428       "passwd":"senhacomplexa",
429       "role":"Administrators"
430       }
431 user={
432       "encrypt_user":"uyIz21VtF3N7CErRtY8Ssg==",
```

```
433       "encrypt_passwd":"t/ffuYNFBY6oyeG2R3WwsA==",
434       "user":"",
435       "passwd":"",
436       "role":"Administrators"
437       }
438 user={
439       "encrypt_user":"SIM3gJ3ZoLYS5L7wlFCaaA==",
440       "encrypt_passwd":"t/ffuYNFBY6oyeG2R3WwsA==",
441       "user":"",
442       "passwd":"",
443       "role":"guest"
444       }
445
446
447 ###################################################################
```