

# Пример настройки аутентификации 802.1X через Web-интерфейс

Стандарт IEEE 802.1X (IEEE Std 802.1X-2010) описывает использование протокола EAP (Extensible Authentication Protocol) для поддержки аутентификации с помощью сервера аутентификации. Стандарт IEEE 802.1X осуществляет контроль доступа и не позволяет неавторизованным устройствам подключаться к локальной сети через порты коммутатора.

Сервер аутентификации **Remote Authentication in Dial-In User Service (RADIUS)** проверяет права доступа каждого клиента, подключаемого к порту коммутатора, прежде чем разрешить доступ к любому из сервисов, предоставляемых коммутатором или локальной сетью.

В стандарте IEEE 802.1X определены три роли устройств в общей схеме аутентификации:

- Клиент (Client/Supplicant);
- Аутентификатор (Authenticator);
- Сервер аутентификации (Authentication Server).

Клиент (Client/Supplicant) — это рабочая станция, которая запрашивает доступ к локальной сети и отвечает на запросы коммутатора. На рабочей станции должно быть установлено клиентское ПО для 802.1Х, например, то, которое встроено в ОС клиентского компьютера или установлено дополнительно.

Сервер аутентификации (Authentication Server) выполняет фактическую аутентификацию клиента. Он проверяет подлинность клиента и информирует коммутатор о предоставлении или отказе клиенту в доступе к локальной сети. Служба RADIUS является клиент/серверным приложением, при работе которого информация об аутентификации передается между сервером RADIUS и клиентами RADIUS.

Аутентификатор (Authenticator) управляет физическим доступом к сети, основываясь на статусе аутентификации клиента. Эту роль выполняет коммутатор. Он работает как посредник (Proxy) между клиентом и сервером аутентификации: получает запрос на проверку подлинности от клиента, проверяет данную информацию при помощи сервера аутентификации и пересылает ответ клиенту. Коммутатор реализует функциональность клиента RADIUS, который отвечает за инкапсуляцию и деинкапсуляцию кадров EAP и взаимодействие с сервером аутентификации.

Коммутаторы D-Link поддерживают две реализации аутентификации 802.1X:

- Port-Based 802.1X (802.1X на основе портов);
- MAC-Based 802.1X (802.1X на основе МАС-адресов).

При аутентификации 802.1Х на основе портов (Port-Based 802.1Х), после того как порт был авторизован, любой компьютер, подключенный к нему, может получить доступ к сети.

В отличие от аутентификации 802.1Х на основе портов, где один порт, авторизированный клиентом, остается открытым для всех клиентов, аутентификация 802.1Х на основе МАС-адресов (МАС-Based 802.1Х) — это аутентификация множества клиентов на одном физическом порте коммутатора. При аутентификации 802.1Х на основе МАС-адресов проверяются не только имя пользователя/пароль, подключенных к порту коммутатора клиентов, но и их количество. Количество подключаемых клиентов ограничено максимальным количеством МАС-адресов, которое может изучить каждый порт коммутатора. Для функции MAC-Based 802.1X количество изучаемых MAC-адресов указывается в спецификации устройство. Сервер аутентификации на проверяет имя пользователя/пароль, И, информация достоверна, аутентификатор если (коммутатор) открывает логическое соединение на основе МАС-адреса клиента. При этом, если достигнут предел изученных портом коммутатора МАС-адресов, новый клиент будет заблокирован.

Функция 802.1X Guest VLAN используется для создания гостевой VLAN с ограниченными правами для пользователей, не прошедших аутентификацию. подключается коммутатора С Когда клиент К порту активизированной аутентификацией 802.1X И функцией Guest VLAN. происходит процесс аутентификации (локально или удаленно с использованием сервера RADIUS). В случае успешной аутентификации клиент будет помещен в VLAN назначения (Target VLAN) в соответствии с предустановленным на сервере RADIUS параметром VLAN. Если этот параметр не определен, то клиент будет возвращен в первоначальную VLAN (в соответствии с настройками порта подключения).

В том случае, если клиент не прошел аутентификацию, он помещается в Guest VLAN с ограниченными правами доступа.

#### Примечание к настройке

Рассматриваемый пример настройки подходит для следующих серий коммутаторов: DGS-1100/ME, DGS-1210, DGS-1210/ME, DGS-1210/FL, DGS-3000.

# Задача №1

В локальной сети необходимо обеспечить аутентификацию пользователей при подключении их к сети.

Задача решается настройкой Port-Based 802.1Х на портах коммутатора.

Помимо коммутатора, необходимо настроить RADIUS-сервер и 802.1Х-клиент на рабочей станции. В качестве RADIUS-сервера можно использовать пакет freeradius для OC Linux.





### Настройка коммутатора SW 1

 В меню слева выберите Management → IP Interface → System IP Address Settings и измените IP-адрес интерфейса управления коммутатора (в примере – 192.168.0.10/24).

System Configuration System Information Settings Fort Configuration System Log Configuration System Log Configuration System Log Configuration Time Range Settings Super Accounts Settings Reboot Schedule Settings Atto Backup Settings Atto B	• Static Interface Name Management VLAN Name Interface Admin State IP Address Subnet Mask Gateway	O DHCP System default Enabled ✓ 192 . 168 . 0 10 255 . 255 . 255 . 0 0 . 0 . 0 . 0	ОВООТР	Apply

- 2. Выберите пункт меню Security → 802.1X → 802.1X Global Settings и активируйте функцию 802.1X, выполнив следующие настройки:
  - -в поле Authentication Mode выберите Port-based;
  - -в поле RADIUS Authorization выберите Enabled;
  - -в поле Authentication Protocol выберите RADIUS EAP.

Нажмите **Apply**.

System Configuration     Management     L2 Features     Solution     GoS     GoS     GoS     GoS	Authentication Mode Forward EAPOL PDU RADIUS Authorization	Port-based     v       Disabled     v       Enabled     v	Authentication Protocol Max User (1-448)	RADIUS EAP ✓ ✓
				Appiy

3. Выберите пункт меню 802.1X Port Settings и укажите порт или диапазон портов, к которым будут подключены клиенты, выбрав соответствующие значения в полях From Port и To Port (в примере порты 2 – 10). В поле Capability выберите Authenticator и нажмите Apply.

Ter															
System Configuration	002 1	V Dort /	Access Cont	trol											
🗄 👘 Management	602.1	IN POIL /	ACCESS COM							_					
🗄 🃁 L2 Features	From	Port		02		×	ļ	To Port		1	10		<b>~</b>		
E Seatures	Quiet	Period (	0-65535)	60			sec	SuppTin	neout (1-658	535) 3	0		sec		
🗄 📁 🖉 QoS	Serve	erTimeou	it (1-65535)	30			sec	MaxReg	(1-10)	2			times		
III MACL	TYD	oriod (1	CEEDEN	20				DoAuth	Doriod (1 65	E0E) 0	600				
E Security	IAP	enou (1-	00000)	30			Sec	ReAuun	-enou (1-05	555) <u></u>	000		sec		
🖻 🎾 802.1X	ReAu	thentica	tion	Disabl	ed	~		Port Cor	ntrol	1	Auto		<b>v</b>		
802.1X Global Settings	Capa	bility		Auther	nticator	~	)	Direction	ı	E	Both		~		Refresh
802.1X User Settings	Forwa	ard EAP	OL PDU	Disabl	ed	×	)	Max Use	er (1-448)	1	6			lo Limit	Apply
Guest VLAN Settings															
🕀 🃁 RADIUS				Port	TX	Ouiet	S	Supp-	Server-		ReAuth			Forward	
	Port	AdmDir	OpenCriDir	Control	Period	Period	Ti	meout	Timeout	махкео	Period	ReAuth	Capability	EAPOL PDU	Max User
MAC-based Access Control (MAC)	1	Both	Both	Auto	30	60		30	30	2	3600	Disabled	None	Disabled	16
Web-based Access Control (WAC)	2	Both	Both	Auto	30	60		30	30	2	3600	Disabled	None	Disabled	16
E Compound Authentication	3	Both	Both	Auto	30	60		30	30	2	3600	Disabled	None	Disabled	16
IGMP Access Control Settings	4	Both	Both	Auto	30	60		30	30	2	3600	Disabled	None	Disabled	16
Port Security	5	Both	Both	Auto	30	60		30	30	2	3600	Disabled	None	Disabled	16
ARP Spoofing Prevention Settings	6	Both	Both	Auto	30	60		30	30	2	3600	Disabled	None	Disabled	16
BPDU Attack Protection	7	Both	Both	Auto	30	60		30	30	2	3600	Disabled	None	Disabled	16
	8	Both	Both	Auto	30	60		30	30	2	3600	Disabled	None	Disabled	16
RPC PortMapper Filter Settings	9	Both	Both	Auto	30	60		30	30	2	3600	Disabled	None	Disabled	16
NetBIOS Filtering Settings	10	Both	Both	Auto	30	60		30	30	2	3600	Disabled	None	Disabled	16

 Выберите пункт меню RADIUS → Authentication RADIUS Server Settings. В поле IPv4 Address укажите адрес своего сервера (в примере 192.168.0.2). Введите и подтвердите пароль в полях Key/Confirm Key. Нажмите Apply.

System Configuration     Management     L2 Features     QoS     QoS     ACL     Security     B02.1X Global Settings     B02.1X Port Setting     B02.1X Port Setting	Index Index IPv4 Address IPv6 Address Authentication Port (1-65535) Accounting Port (1-65535) Timeout (1-255) Retransmit (1-20)	1           192.168.0.2		e.g.: 10.90.90 e.g.: 56FF::2) Default Default ec Defau pefau	0.90) ) It				
B02.1X User Settings     Guest VLAN Settings     Authentication RADIUS Server Settings     RADIUS Authentication     RADIUS Account Client     PMAC-Port Binding (IMPB)     MaC-based Access Control (MAC)     Web-based Access Control (WAC)     Given Section Settings	Retransmit (1-20) Key (Max: 32 characters) Confirm Key RADIUS Server List Index IP Address 1 192.168.0.2	Auth-Port Acc 1812 181	ct-Port	mes ♥ Defa Timeout 5	Retransmit 2	Key	Edit	Apply Delete	

5. Чтобы сохранить выполненные настройки, в левом верхнем углу нажмите **Save**, выберите **Save Configuration** и нажмите **Apply**.

🖺 Save 🛛 🏹 Tools 👅 English 🗸 🗸		
DGS-3000-28X	Save	O Safeguard
System Configuration	Save Configuration / Log	
	Type All V	
E L3 Features		
		Apply

# Задача № 2

В локальной сети необходимо обеспечить аутентификацию пользователей при их подключении к сети через неуправляемый коммутатор. Задача решается настройкой MAC-Based 802.1X на портах управляемого коммутатора.



Рис. 2 Схема подключения

#### Настройка коммутатора SW 1

- 1. Выберите пункт меню Security → 802.1X → 802.1X Global Settings и выполните следующие настройки:
  - -в поле Authentication Mode выберите MAC-based;
  - -в поле RADIUS Authorization выберите Enabled;
  - -в поле Authentication Protocol выберите RADIUS EAP.

Нажмите **Apply**.

System Configuration     Management     L2 Features     L3 Features     QoS     Soc.     L4 Features     Soc.     L5 Features     Soc.     L5 Features     Soc.     Soc.	Authentication Mode Forward EAPOL PDU RADIUS Authorization	MAC-based Disabled Enabled	> > >	Authentication Protocol Max User (1-448)	RADIUS EAP v	No Limit
Government						Apply

2. Выберите пункт меню 802.1X Port Settings и укажите порт, к которому будет подключен неуправляемый коммутатор, выбрав соответствующее значение в полях From Port и To Port (в примере – порт 2). В поле Capability выберите Authenticator и нажмите Apply.

∃-	802.1)	(Port A	ccess Con	trol	_											
. ■ E2 Features	From F	Port			0	2	~	]	To Port				02	<b>v</b> ]		
E E3 Features	QuietP	Period (C	)-65535)		60	)		s	ec SuppTimed	out (1-655	535)		30		sec	
∃-	Server	Timeou	t (1-65535)		30	)		s	ec MaxReq (1	-10)			2		times	
Security	TX Pe	riod (1-6	65535)		30	)		S	ec ReAuthPer	iod (1-65	535)		3600		sec	
E 602.1X	ReAut	henticat	ion			isabled	~		Port Contro	ol			Auto	~		
802.1X Global Settings	Capab	ility			Ā	uthenticat	or v	Ĵ	Direction				Both	<b>v</b>		
802.1X User Settings	Forwa	rd EAPO	OL PDU			isabled	~	]	Max User (	1-448)			16			No Limit
Guest VLAN Settings											Re	fresh	Apply			
🗈 📁 RADIUS																
IP-MAC-Port Binding (IMPB)     MAC-based Access Control (MAC)     MAC-based Access Control (MAC)	Port /	AdmDir	OpenCrlDir	Port Control	TX Period	Quiet Period	Supp- Timeou	ut	Server- Timeout	MaxReq	ReAuth Period	ReAuth	Capability	Forwar EAPOL P		Max User
web-based Access Control (WAC)	1	Both	Both	Auto	30	60	30		30	2	3600	Disabled	None	Disable	d	16
Port Security	2	Both	Both	Auto	30	60	30		30	2	3600	Disabled	Authenticator	Disable	d	16
ARP Spoofing Prevention Settings	3	Both	Both	Auto	30	60	30		30	2	3600	Disabled	None	Disable	d	16

3. Выберите пункт меню RADIUS → Authentication RADIUS Server Settings. В поле IPv4 Address укажите адрес своего сервера (в примере 192.168.0.2). Введите и подтвердите пароль в полях Key/Confirm Key. Нажмите Apply.

System Configuration		(		1				
Management	Index	1	~	ļ				
E E L2 Features	IPv4 Address	192.168.0.2		(e.q.: 10.90.9	0.90)			
	0							
	O IPv6 Address			(e.g.: 56FF::2	-)			
🗄 📁 📁 ACL	Authentication Port (1-65535)			🗹 Default				
E Security	Association Dort (1 (SEE))							
🖻 🌈 802.1X	Accounting Port (1-65535)			Default				
	Timeout (1-255)			sec 🔽 Defa	ult			
	Determine (1.00)							
	Retransmit (1-20)			times 🔽 De	lault			
Guest VLAN Settings	Key (Max: 32 characters)	•••••						
🖻 🌈 RADIUS	Confirm Kou							A
Authentication RADIUS Server Settings	Committeey							Арріу
RADIUS Authentication								
RADIUS Account Client								
庄 🧊 IP-MAC-Port Binding (IMPB)	RADIUS Server List							
MAC-based Access Control (MAC)	Index IP Address	Auth-Port	Acct-Port	Timeout	Retransmit	Kev		
🕀 🃁 Web-based Access Control (WAC)	1 192,168,0,2	1812	1813	5	2	*****	Edit	Delete
E Compound Authentication	2	1011	1010		-		- Dair	J Denote
IGMP Access Control Settings	2							
i Port Security	5							

- 4. Установите максимальное количество изучаемых MAC-адресов равным 1. Для этого в меню слева выберите Port Security → Port Security Settings и задайте следующие настройки:
  - выберите порт, к которому подключен неуправляемый коммутатор (в примере – порт 2);
  - в поле Admin State выберите Enabled;
  - в поле Action выберите Drop;
  - в поле Max Learning Address(0-3328) укажите 1 и нажмите Apply.

System Configuration     Management     L2 Features	Port Security	Trap/Log Settin	i <b>gs</b> O Ena	abled 💿	Disabled		Apply
	Port Security System Maxim	System Setting	<b>s</b> 3328)		No Limit		Apply
602.1X     602.1X Global Settings     602.1X Port Settings     602.1X Port Settings     602.1X Viser Settings     602.1X User Settings     602.1X User Settings     602.1X User Settings     602.1X User Settings	From Port To	Port Admin 2 v Enabl	State Action ed v Drop	Lock A	ddress Mode Max Learn	ning Address(0-3328)	Apply
MAC-based Access Control (MAC)	Port	Admin State	Lock Address Mode	Max Learning Address	Action		
Web-based Access Control (WAC)	1	Disabled	DeleteOnReset	32	Drop	Edit	View Details
Port Security	2	Enabled	DeleteOnReset	1	Drop	Edit	View Details
Port Security Settings	3	Disabled	DeleteOnReset	32	Drop	Edit	View Details
Port Security VLAN Settings	4	Disabled	DeleteOnReset	32	Drop	Edit	View Details
Port Security Entries	5	Disabled	DeleteOnReset	32	Drop	Edit	View Details

5. Чтобы сохранить выполненные настройки, в левом верхнем углу нажмите Save, выберите Save Configuration и нажмите Apply.

📄 Save 🗂 👗 Tools 🕇 English 🗸 🗸		
DGS-3000-28X	Save	O Safeguard
System Configuration     Management     Galagement	Save Configuration / Log	
B- CI		Apply

# Задача № З

В локальной сети необходимо обеспечить аутентификацию пользователей при их подключении к сети. До прохождения успешной аутентификации, или в случае её неуспеха, пользователь должен получать доступ в «гостевую» VLAN.

Задача решается настройкой 802.1Х Guest VLAN на коммутаторе. Неаутентифицированным пользователям, находящимся в VLAN 10, разрешен доступ в Интернет. После успешной аутентификации пользователей, порты к которым они подключены, будут добавлены в VLAN 20.



Рис. 3 Схема подключения

#### Настройка коммутатора SW 1

- 1. Выберите пункт меню L2 Features  $\rightarrow$  VLAN  $\rightarrow$  802.1Q VLAN Settings, откройте вкладку Add/Edit VLAN и создайте необходимые VLAN (в примере VLAN v10 и v20):
  - в поле VID укажите номер VLAN;
  - в поле VLAN Name введите название VLAN;
  - отметьте порты, которые будут являться немаркированными членами VLAN, как Untagged (в примере: порты 13 – 24 для VLAN v10 и 1 – 12 для VLAN v20)
  - нажмите **Apply**.

DGS-3000-28X	802.1Q VLAN Settings
System Configuration	
Management	VI ANU List Add/Edit//I ANU Find//I ANU VI ANI Datab Cattings Total Entries: 1
EL2 Features	VEAN LIST AUG/EDIT VEAN PIND VEAN VEAN BAICH Settings Total Entries: 1
CONTRACT OF CONTRACT.	VID 10 VLAN Name 10 (Max: 32 characters) Apply Advertisement Disabled V
MAC-based VLAN Settings	Port Select All 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28
Private VLAN Settings	
PVID Auto Assign Settings	
Brause VI AN	
Browse VLAN     Browse VLAN     Show VLAN Ports     T    OinO	
Layer 2 Protocol Tunneling Settings	Tagged Ports
🗄 🃁 Spanning Tree	Untagged Ports 13-24
<ul> <li>Link Aggregation</li> <li>FDB</li> </ul>	Forbidden Ports

P DGS-3000-28X	802.1Q VLAN Settings	O Safeg
System Configuration     Management     L2 Features	VLAN List Add/Edit VLAN Find VLAN VLAN Batch Settings Total Entries: 1	
VLAN     VLAN Settings     802.1v Protocol VLAN     SVEP     GVRP	VID 20 VLAN Name 20 (Max: 32 characters) Apply Advertisement Disabled v	]
AC-based VLAN Settings      Private VLAN Settings      Private VLAN Settings      Settings      Vice VLAN Settings      Settings	Port         Select Al 01         02         03         04         05         06         07         08         09         10         11         12         13         14         15         16         17         18         19         20         21         22         23         24         25         26           Tagged         All         O	27 28
VLAN Trunk Settings Browse VLAN Show VLAN Ports	Onlagge         All         O	00
CinQ     Spanning Tree     Link Aggregation     FDB	Tagged Ports Untagged Ports 1-12 Forbidden Ports	

 Создайте IP-интерфейс для VLAN 10. Для этого в меню слева выберите Management → IP Interface → System IP Address Settings. В поле Management VLAN Name укажите название соответствующей VLAN и нажмите Apply.

System Configuration     Management	<ul> <li>Static</li> </ul>	O DHCP	ОВООТР	
Herrie ARP     Gratuitous ARP     For Gratuitous ARP     For IP Interface     System IP Address Settings     Management Settings     Management Settings     Session Table     Session Table	Interface Name Management VLAN Name Interface Admin State IP Address Subnet Mask Gateway	System           10           Enabled         V           192         , 168         0         , 1           255         , 255         , 0         0         , 0		
Single IP Management     Single SNMP Settings				Apply

- 3. Выберите пункт меню Security → 802.1X → 802.1X Global Settings и активируйте функцию 802.1X, выполнив следующие настройки:
- в поле RADIUS Authorization выберите Enabled;
- в поле Authentication Protocol выберите RADIUS EAP.

#### Нажмите **Apply**.

System Configuration     Management     L2 Features     QoS     QoS     CL	Authentication Mode Forward EAPOL PDU RADIUS Authorization	Disabled Disabled Enabled	> > >	Authentication Protocol Max User (1-448)	RADIUS EAP V	✔ No Limit
						Apply

4. В разделе Guest VLAN Settings настройте VLAN v10 в качестве гостевой VLAN. Для этого в поле VLAN Name укажите 10, отметьте порты, принадлежащие данной VLAN, и нажмите Apply.

DGS-3000-28X	Guest VLAN Settings	O Safeguard
System Configuration     Management	Add Guest VLAN	
E → E2 Features     E → E2 Features     A → E2 Features     A → E     C → C	VLAN Name 10 Apply	Delete
	Port         01         02         03         04         05         06         07         08         09         10         11         12         13         14         15         16         17         18         19         20         21         22         23           All	24 25 26 27 28
Guest VLAN Settings	Current Guest VLAN Ports:	

 Выберите пункт меню 802.1X Port Settings и настройте порты, принадлежащие гостевой VLAN, в качестве аутентификатора. Для этого в полях From Port и To Port укажите порты 13 – 24, в поле Capability выберите Authenticator и нажмите Apply.

⊕-	802.1X Port Access Control	<u></u>			
E C Features	From Port	13 v	To Port	24 ~	J
E → C Features	QuietPeriod (0-65535)	60	sec SuppTimeout (1-65535)	30	sec
terre and the second s	ServerTimeout (1-65535)	30	sec MaxReq (1-10)	2	times
	TX Period (1-65535)	30	sec ReAuthPeriod (1-65535)	3600	sec
⊡- 🌈 802.1X	ReAuthentication	Disabled v	Port Control	Auto 🗸	]
802.1X Global Settings	Capability	Authenticator v	Direction	Both v	J
	Forward EAPOL PDU	Disabled v	Max User (1-448)	16	No Limit
Guest VLAN Settings			Refresh	Apply	

6. Выберите пункт меню RADIUS → Authentication RADIUS Server Settings. В поле IPv4 Address укажите адрес своего сервера (в примере 192.168.0.10). Введите и подтвердите пароль в полях Key/Confirm Key. Нажмите Apply.

Tot				
System Configuration			_	
🗈 🃁 Management	Index	1 v	]	
🗄 📁 L2 Features	IPv4 Address	192.168.0.10	(e.g.: 10.90.90.90)	
🗄 📁 🎾 QoS	<ul> <li>IPv6 Address</li> </ul>		(e.g.: 56FF::2)	
🗄 📁 ACL	Authentication Port (1-65535)		🔽 Default	
E Security				
🖻 🎾 802.1X	Accounting Port (1-65535)		🛛 🗹 Default	
	Timeout (1-255)		sec 🔽 Default	
802.1X User Settings	Retransmit (1-20)		times 🗹 Default	
Guest VLAN Settings	Key (Max: 32 characters)	•••••	7	
🖻 🎾 RADIUS	0		7	
Authentication RADIUS Server Settings	Confirm Key	•••••		Apply
RADIUS Authentication				
RADIUS Account Client	RADIUS Server List			
IP-MAC-Port Binding (IMPB)	Index IP Address Au	uth-Port Acct-Port T	ïmeout Retransmit Key	
MAC-based Access Control (MAC)	1 192,168,0,10 18	12 1813 5	2 ******	Edit Delete
Web-based Access Control (WAC)	2		-	Delete
Compound Authentication	2			

7. Чтобы сохранить выполненные настройки, в левом верхнем углу нажмите **Save**, выберите **Save Configuration** и нажмите **Apply**.

🗄 Save 🕇 👗 Tools 🎽 English 🛛 🗸 🗸		
DGS-3000-28X	Save	O Safeguard
System Configuration     Management	Save Configuration / Log	
	Type All v	
E © QoS	ſ	Apply