

Сетевой администратор попросил вас настроить новый коммутатор. В рамках этого упражнения, используя список требований, вам предстоит выполнить базовую настройку коммутатора, конфигурацию протокола SSH и параметры безопасности портов.

Требования

- Установите следующие начальные значения параметров коммутатора S1:

Имя пользователя

Баннер, который содержит слово предупреждение (warning)

Включите проверку пароля на консоли и портах cisco

Зашифрованный пароль привилегированного режима — class

Зашифруйте все незашифрованные пароли

Адресация административного интерфейса

- Установите следующие параметры протокола SSH для безопасного удаленного доступа:

Имя домена cisco.com

Параметры портовой RSA для поддержки протокола SSH версии 2

Протокол SSH версии 2

Пользователь admin с секретным паролем cisco

Используйте MDT для хранения конфигурации коммутатора SSH, а для проверки подлинности

используются только данные из локальной базы данных

© Корпорация Cisco и/или ее дочерние компании, 2016. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

Страница 1 из 2

Packet Tracer. Отработка комплексных практических навыков

- Настройте функцию безопасности портов для ограничения сетевого доступа.

Отключите все неиспользуемые порты.

Настройте режим интерфейса в режим доступа (access).

Активируйте защиту порта, позволяющую подключаться только двум пользователям одному порту.

Запишите MAC-адрес в текущей конфигурации

Убедитесь, что в случае нарушения порт будет отключен.

You did not complete the activity. Please close this window and try again.

Score : 97/100

Item Count : 45/46

Assessment Items	Status	Points	Component(s)
Network			
S1			
Banner MOTD	Correct	3	Basic Security
Console Line			
Login	Correct	3	Basic Security
Password	Correct	3	Basic Security
Enable Secret	Correct	3	Basic Security
Host Name	Incorrect	3	Hostname Cor
IP Domain Name	Correct	5	Device Harder
Ports			
FastEthernet0/1			
Port Security			
Enabled	Correct	3	Port Security (
Maximum Static MACs	Correct	3	Port Security (
Port Security Violation	Correct	4	Port Security (
Sticky Enabled	Correct	3	Port Security (
FastEthernet0/10		0	Other
Port Status	Correct	1	Port Security (
FastEthernet0/11		0	Other
Port Status	Correct	1	Port Security (
FastEthernet0/12		0	Other
Port Status	Correct	1	Port Security (
FastEthernet0/13		0	Other
Port Status	Correct	1	Port Security (
FastEthernet0/14		0	Other
Port Status	Correct	1	Port Security (
FastEthernet0/15		0	Other
Port Status	Correct	1	Port Security (
FastEthernet0/16		0	Other
Port Status	Correct	1	Port Security (
FastEthernet0/17		0	Other
Port Status	Correct	1	Port Security (
FastEthernet0/18		0	Other
Port Status	Correct	1	Port Security (
FastEthernet0/19		0	Other
Port Status	Correct	1	Port Security (
FastEthernet0/2			
Port Security			
Enabled	Correct	3	Port Security (
Maximum Static MACs	Correct	3	Port Security (
Port Security Violation	Correct	4	Port Security (
Sticky Enabled	Correct	3	Port Security (
FastEthernet0/20		0	Other
Port Status	Correct	1	Port Security (
FastEthernet0/21		0	Other
Port Status	Correct	1	Port Security (
FastEthernet0/22		0	Other
Port Status	Correct	1	Port Security (
FastEthernet0/23		0	Other
Port Status	Correct	1	Port Security (
FastEthernet0/24		0	Other
Port Status	Correct	1	Port Security (
FastEthernet0/3		0	Other

Component	Items/Total	Score
Basic Security Configuration	5/5	15/15
Device Hardening Configuration	5/5	25/25
Hostname Configuration	0/1	0/3
IPv4 Host Address Configuration	3/3	7/7
Port Security Configuration	32/32	50/50

- Убедитесь, что в случае нарушения порт будет отключен.

ems/Total	Score
5/5	15/15
5/5	25/25
0/1	0/3
3/3	7/7
32/32	50/50

Сетевой администратор попросил вас настроить новый коммутатор. В рамках этого упражнения, используя список требований, вам предстоит выполнить базовую настройку коммутатора, конфигурацию протокола SSH и параметры безопасности портов.

Требования

- Установите следующие начальные значения параметров коммутатора S1:

Имя пользователя

Баннер, который содержит слово предупреждение (warning)

Включите проверку пароля на консоли и портах vty

Зашифрованный пароль привилегированного режима — cisco

Зашифруйте все незашифрованные пароли

Адресация административного интерфейса

- Установите следующие параметры протокола SSH для безопасного удаленного доступа:

Имя домена cisco.com

Параметры портовой RSA для поддержки протокола SSH версии 2

Протокол SSH версии 2

Пользователи admin с секретным паролем cisco

Ограничьте доступ к коммутатору SSH с помощью проверки подлинности

Используйте только данные из локальной базы данных

© Корпорация Cisco и/или ее дочерние компании, 2016. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

Страница 1 из 2

Packet Tracer. Отработка комплексных практических навыков

- Настройте функцию безопасности портов для ограничения сетевого доступа.

Отключите все неиспользуемые порты.

Настройте режим интерфейса в режим доступа (access).

Активируйте функцию порта, позволяющую подключаться только двум пользователям к одному порту.

Задайте MAC-адрес в следующей конфигурации

Убедитесь, что в случае нарушения порт будет отключен.

You did not complete the activity. Please close this window and try again.

04 5.3.1.2 Packet Tracer - Skills Integration Challenge.pdf - Adobe Acrobat Pro (32-bit)

Файл Редактирование Просмотр Электронное подписание Окно Справка

Главная Инструменты 04 5.3.1.2 Packet Tr... Войти

Заполнить и подписать IAb X ✓ O — • ● ... Далее Закреть

Сетевой администратор попросил вас настроить новый коммутатор. В рамках этого упражнения, используя список требований, вам предстоит выполнить базовую настройку коммутатора, конфигурацию протокола SSH и параметры безопасности портов.

Требования

- Установите следующие начальные значения параметров коммутатора **S1**:
 - Имя узла
 - Баннер, который содержит слово предупреждение (warning)
 - Включить проверку пароля на консоли и портах
 - Зашифрованный пароль привилегированного режима — class
 - Зашифруйте все неиспользуемые порты
 - Адресация административного интерфейса
- Установите следующие параметры протокола SSH для безопасного удаленного доступа:
 - Имя домена cisco.com
 - Параметры версии SSH для поддержки протокола SSH версии 2
 - Протокол SSH версии 2
 - Пользователь admin с секретным паролем cisco
 - Имя VTY-линии, которая поддерживает протокол SSH, а для проверки работоспособности
 - Используйте только данные из локальной базы данных

© Корпорация Cisco и/или ее дочерние компании, 2016. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

Страница 1 из 2

Packet Tracer. Отработка комплексных практических навыков

- Настройте функцию безопасности портов для ограничения сетевого доступа.
 - Отключите все неиспользуемые порты.
 - Настройте режим интерфейса в режиме доступа (access).
 - Активируйте сокет портов, позволяющие подключаться только двум узлам к одному порту.
 - Запишите MAC-адрес в текущей конфигурации
- Убедитесь, что в случае нарушения порт будет отключен.

Cisco Packet Tracer - D:\Education\Education3\net\4\04 5.3.1.2 Packet Tracer - Skills Integration Challenge.pka

File Edit Options View Tools Extensions Help

Activity Results Time Elapsed: 00:24:14

You did not complete the activity. Please close this window and try again.

Overall Feedback Assessment Item

Expand/Collapse All Show Incorrect

Assessment Items

Network

- S1
 - ✓ Banner MOTD
 - Console Line
 - ✓ Login
 - ✓ Password
 - ✓ Enable Secret
 - ✗ Host Name
 - ✓ IP Domain Name
 - Ports
 - FastEthernet0/1
 - Port Security
 - ✓ Enabled
 - ✓ Maximum
 - ✓ Port Secu
 - ✓ Sticky En
 - FastEthernet0/10
 - ✓ Port Status
 - FastEthernet0/11
 - ✓ Port Status
 - FastEthernet0/12
 - ✓ Port Status
 - FastEthernet0/13
 - ✓ Port Status
 - FastEthernet0/14
 - ✓ Port Status
 - FastEthernet0/15
 - ✓ Port Status
 - FastEthernet0/16
 - ✓ Port Status
 - FastEthernet0/17
 - ✓ Port Status
 - FastEthernet0/18
 - ✓ Port Status
 - FastEthernet0/19
 - ✓ Port Status
 - FastEthernet0/2
 - Port Security
 - ✓ Enabled
 - ✓ Maximum Static MACs
 - ✓ Port Security Violation
 - ✓ Sticky Enabled
 - FastEthernet0/20
 - ✓ Port Status
 - FastEthernet0/21
 - ✓ Port Status
 - FastEthernet0/22
 - ✓ Port Status
 - FastEthernet0/23
 - ✓ Port Status
 - FastEthernet0/24
 - ✓ Port Status
 - FastEthernet0/25
 - ✓ Port Status

S1

Physical Config CLI Attributes

IOS Command Line Interface

Medvedev(config-line)#transport input ssh
Medvedev(config-line)#exit
Medvedev(config)#username admin secret ccns
Medvedev(config)#username admin secret ccna
Medvedev(config)#in
Medvedev(config)#interface fa
Medvedev(config)#interface fastEthernet 0/1 -2
Medvedev(config)#
% Invalid input detected at '^' marker.

Medvedev(config)#interface range fastEthernet 0/1 -2
Medvedev(config-if-range)#sw
Medvedev(config-if-range)#switchport por
Medvedev(config-if-range)#switchport port-security
Medvedev(config-if-range)#exit
Medvedev(config)#interface v
Medvedev(config)#interface vlan 1
Medvedev(config-if)#no shut
Medvedev(config-if)#no shutdown

Medvedev(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Medvedev(config-if)#exit
Medvedev(config)#

Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top

Correct	1	Port Security (
Correct	3	Port Security (
Correct	3	Port Security (
Correct	4	Port Security (
Correct	3	Port Security (
	0	Other
Correct	1	Port Security (
	0	Other
Correct	1	Port Security (
	0	Other
Correct	1	Port Security (
	0	Other
Correct	1	Port Security (
	0	Other
Correct	1	Port Security (
	0	Other

Close

23:59 21.09.2023

Close