

Siemens

Industriepark Karlsruhe

Defense in Depth + Sinema Remote Connect

Labs

Unrestricted © Siemens Industry, Inc. 2017 All right

Answers for industry.



Appendix

Unrestricted © Siemens Industry, Inc. 2017 All rights



Initial Information

Unrestricted © Siemens Industry, Inc. 2017 All rights

Routing / Masquerading – Additional Information Lab

Station	Instructor	1	2	3	4	5	6	7	8
S615									
Ext	172.16.10.1/16	172.16.1.1/16	172.16.2.1/16	172.16.3.1/16	172.16.4.1/16	172.16.5.1/16	172.16.6.1/16	172.16.7.1/16	172.16.8.1/16
Int	192.168.10.1/24	192.168.1.1/24	192.168.1.1/24	192.168.1.1/24	192.168.1.1/24	192.168.1.1/24	192.168.1.1/24	192.168.1.1/24	192.168.1.1/24
VLAN3	10.0.0.1/24	10.0.0.1/24	10.0.0.1/24	10.0.0.1/24	10.0.0.1/24	10.0.0.1/24	10.0.0.1/24	10.0.0.1/24	10.0.0.1/24
HMI	192.168.10.10/24	192.168.1.10/24	192.168.1.10/24	192.168.1.10/24	192.168.1.10/24	192.168.1.10/24	192.168.1.10/24	192.168.1.10/24	192.168.1.10/24
PLC	10.0.0.10/24	10.0.0.11/24	10.0.0.12/24	10.0.0.13/24	10.0.0.14/24	10.0.0.15/24	10.0.0.16/24	10.0.0.17/24	10.0.0.18/24

Routing / Masquerading – Network Layout Lab

Instructor S615 Ext: 172.16.10.1/16 Int: 192.168.10.1/24 PC: 192.168.10.5/24 PLC: 192.168.10.10/24 **HMI**:10.0.0.10/24 hp (p) Station 2 S615 Station 3 S615 Ext: 172.16.2.1/16 GW:172.16.10.1 Ext: 172.16.3.1/16 GW:172.16.10.1 Int: 192.168.1.1/24 Int: 192.168.1.1/24 PC: 192.168.1.5/24 GW:192.168.1.1 PC: 192.168.1.5/24 GW:192.168.1.1

Station 1 S615 Ext: 172.16.1.1/16 GW:172.16.10.1 Int: 192.168.1.1/24 PC: 192.168.1.5/24 GW 192.168.1.1

> **PLC**:192.168.1.10/24 **HMI**: 10.0.0.11/24

Page 5

PLC:192.168.1.10/24 HMI: 10.0.0.12/24 PLC:192.168.1.10/24 HMI: 10.0.0.13/24



Subnetting Lab Exercises

Unrestricted © Siemens Industry, Inc. 2017 All rights

Subnetting Cheat Sheet

Quick Formulas:

- Number of subnets = 2^s (where s is the number of bits borrowed)
- Number of host addresses available per subnet = 2^h 2 (where h is the number of host bits remaining after bits are borrowed)

27	2 ⁶	2 ⁵	24	2 ³	2 ²	21	20	Power of 2
128	64	32	16	8	4	2	1	Network Increments (address multiples)
.128	.192	.224	.240	.248	.252	.254	.255	mask
2	4	8	16	32	64	128	256	# of subnetworks (2 to the power of # of borrowed bits)
/25	/26	/27	/28	/29	/30	/31	/32	CIDR C
/17	/18	/19	/20	/21	/22	/23	/24	CIDR B
/9	/10	/11	/12	/13	/14	/15	/16	CIDR A

Unrestricted © Siemens Industry, Inc. 2017 All rights reserved.

Subnetting Lab Exercise #1

Task: Given the IP host address of 192.168.3.222/27, find the following:

- Subnet Mask
- Sub-network starting address
- 1st host address
- Last host address
- Broadcast address
- Starting address of the next network

IP host address	192.168.3.222/27
Mask	
Sub-network	
1st Host	
Last Host	
Broadcast	
Next Network	

Subnetting Lab Exercise #2

Task: Given the IP host address of 172.28.114.9/21, find the following:

- Subnet Mask
- Sub-network starting address
- 1st host address
- Last host address
- Broadcast address
- Starting address of the next network

IP host address	172.28.114.9/21
Mask	
Sub-network	
1st Host	
Last Host	
Broadcast	
Next Network	

Subnetting Lab Exercise #3

Task: Given the IP host address of 192.168.247.246/30, find the following:

- Subnet Mask
- Sub-network starting address
- 1st host address
- Last host address
- Broadcast address
- Starting address of the next network

IP host address	192.168.247.246/30
Mask	
Sub-network	
1st Host	
Last Host	
Broadcast	
Next Network	

On the network 131.1.123.0/27, what is the last IP address that can be assigned to a host?

A. 131.1.123.30
B. 131.1.123.31
C. 131.1.123.32
D. 131.1.123.33

Slide Intentionally Blank



Answer Key

Lab #1 Lab #2 Lab #3

IP host address	192.168.3.222/27
Mask	255.255.255.224
Sub-network	192.168.3.192
1st Host	192.168.3.193
Last Host	192.168.3.222
Broadcast	192.168.3.223
Next Network	192.168.3.224

IP host address	172.28.114.9/21
Mask	255.255.248.0
Sub-network	172.28.112.0
1st Host	172.28.112.1
Last Host	172.28.119.254
Broadcast	172.28.119.255
Next Network	172.28.120.0

IP host address	192.168.247.246/30
Mask	255.255.255.252
Sub-network	192.168.247.244
1st Host	192.168.247.245
Last Host	192.168.247.246
Broadcast	192.168.247.247
Next Network	192.168.247.248

Bonus Question: A



Initial Configuration Lab

Unrestricted © Siemens Industry, Inc. 2017 All rights

Initial Setup – Configure PC IP Address Lab

- 1) Right Click on the Network Icon in the Notification Area
- 2) Click on Open Network and Sharing Center
- 3) Click Change adapter settings
- 4) Select the connected network and double click
- 5) Accept the Windows warning by clicking Yes



Initial Setup – Configure PC IP Address Lab

- 1) Click on Internet Protocol Version 4 (TCP/IPv4)
- 2) Click Properties
- 3) Select Use the following IP address:
- 4) Enter IP and Subnet Mask Only as shown
- 5) Click OK until all the way out of the network properties screens.
- 6) Close any remaining open screens.

🖞 eth0 Properties	×									
Networking Authentication Sharing										
Connect using:										
Intel(R) PRO/1000 MT Desktop Adapter										
Configure)									
This connection uses the following items:	.									
Client for Microsoft Networks										
QoS Packet Scheduler Ele and Printer Sharing for Microsoft Networks										
 Internet Protocol Version 6 (TCP/IPv6) 										
Internet Protocol Version 4 (TCP/IPv4)										
Link-Layer Topology Discovery Mapper I/O Driver										
Ink-Layer Topology Discovery Responder										
Install Uninstall Properties										
Transmission Control Protocol/Internet Protocol. The default										
across diverse interconnected networks.										
OK Cano	el									

Internet Protocol Version 4 (TCP/IPv4)	Properties
General	
You can get IP settings assigned autom this capability. Otherwise, you need to for the appropriate IP settings.	natically if your network supports ask your network administrator
Obtain an IP address automaticall	y
• Use the following IP address:	
IP address:	192.168.1.5
Subnet mask:	255.255.255.0
Default gateway:	
Obtain DNS server address autom	natically
• Use the following DNS server add	resses:
Preferred DNS server:	
Alternate DNS server:	· · ·
Validate settings upon exit	Advanced
	OK Cancel

SIEMENS

Unrestricted © Siemens Industry, Inc. 2017 All rights reserved.

Initial Setup - Login Lab

- 1) In web browser type http://192.168.1.1
- 2) Login with admin for the username and password
- 3) Click the Login button



Initial Setup - Login Lab

 Click OK to acknowledge that the password must be changed



SIEMENS

Unrestricted © Siemens Industry, Inc. 2017 All

Initial Setup - Login Lab

- 1) Enter the Current User Password for admin: admin
- In New Password box type: Admin!123
- In Password Confirmation box type: Admin!123
- 4) Click Set Values



SIEMENS



Unrestricted © Siemens Industry, Inc. 2017 All rights

Initial Setup - Wizard Lab

- 1) The Basic Wizard automatically launches
- 2) Find External (vlan2)
- In the IP Address type in 172.16.X.1 where the X is replaced by the Station Number you were assigned
- 4) In the Subnet Mask box type in 255.255.0.0
- 5) In the Gateway box type 172.16.10.1
- 6) Click Next





Initial Setup - Wizard Lab

- 1) Click Next on the Device tab (we aren't naming the device)
- 2) Click Use PC Time
- 3) Click Next

C 192.1	68.1.1					
🎍 Most Visited 🧧	🌶 Getting Started	b Slice Gallery				
SIEMENS						English 💌 Go
SIEMENS 192.168.1.1/SCALANCE S615 01012000 0017 Wetcome admin WAN Basic Wizard: Time Settings 1 Location Image: DDNS_SINEMA RC_Summary 1 Here you set the date and time to check the validity (time) of certificates and for the time stamps of log entries. You can set the system time yourself manually or have it synchronized automatically with a time server. There are a number of time servers on the line server. If you want to use another method, configure these method after completing the WAN Basic Wizard. Image: Time Manually Time Manually System Time: 03/21/2017 09:52:12 Image: Dot time Image: Dot timage: Dot timage: Dot timage: Dot time						
Welcome admin	WAN Basic Wiz	ard: Time Settir	ngs			
Lopout						= ? =
10000	IP Device Time DDN	S SINEMA RC Sumr	mary			
	com	leting the WAN Basic	: Wizard.			
		ma Manually				
	System Time: 03/2	1/2017 09:52:12				
		PC Time				
	Use	ro mile				
	Use	P Client				
	Use N Time Zone: +00	P Client				
	Use N Time Zone: +00:	IP Client	NTD Server Address	NTD Sonor Dot	Poll Istand	

Initial Setup - Wizard Lab

- 1) Click Next to bypass DDNS
- 2) Click Next to bypass Sinema RC
- 3) Verify Settings
- 4) Click Set Values

€ 0 🖌	192.168.1.1							67%	C	Q Search	☆自	+	A S	9
🙆 Most Visi	ed 🥑 Getting	Started 🚺	Web Slice	Gallery										
SIEMENS													English	<u> 00</u>
	192.168.1	.1/SCAL	ANCE S	615									03/21/2017	10:27:22
Welcome admin	WAN Basic Wiz	ard: Summa	ry											. 2 .
Logout	IP Device Time DDN	SINEMA RC S	ummary											
Wizaros														
· Labor Villard	inte	nnal (vlan1)												
Information	IP Address: 192	168.1.1												
System	Subtret Middle, 200	235.235.0												
Interfaces	Exte	ernal (vlan2)												
encenduce	IP Address: 172	.16.1.1												
Layer 2	Subnet Mask: 255	255.0.0												
Layer 3	DHCP: disa	sbled												
Constanting .	Gateway: 172	16.10.1												
Security														
	System Name: syst	Name Not Set												
	System Contact: syst	Contact Not Set												
	Time Manually ena	hleri												
	System Time. 03/2	21/2017 10:26:32												
	NTP Cilent: disa	abled												
	Time Zone: +00	:00												
	NT	P Server Index	NTP Server A	ddress	NTP Server Port	Poll Interval								
	1		0.0.0.0		123	64								
	Ser	vice	Enabled	Host		Username	- 1							
	No	-IP	disabled											
	Dv	nDNS	disabled											
	CIVENUA DO MA	hind												
	SINEMA RC. URS	suleu												

Unrestricted © Siemens Industry, Inc. 20'1 Air rights reserved.

Initial Setup – Disable Automatic Save Lab

- 1) Navigate to and click on System
- 2) Navigate to and click on Configuration
- 3) Change "Configuration Mode" from "Automatic Save" to "Trial"
- 4) Click Set Values

Page 23



Initial Setup – Write Startup Config Lab

- 1) Navigate to and click on System
- 2) Navigate to and click on Configuration
 - A. Alternatively, note the hot link at the top of the screen will go to the correct screen
- 3) Click Write Startup Config button
- 4) Acknowledge the Success Popup



Unrestricted @	Siemens	Industry,	Inc.	2017	All	rights	reserved.
----------------	---------	-----------	------	------	-----	--------	-----------

	Welcome admin	System Configuration
		Trial Mode Active - Press 'Write Startup Config' button to make your settings persistent
	Logout	
	▶Wizards	✓ Teinet Server
	▶Information	✓ SSH Server
	Finioritation	HTTPS Server only
e	▼System	SMTP Client
	► Configuration	Syslog Client
	▶General	DCP Server: Read/Write
	▶Restart	
	▶Load&Save	Time: Manual
	▶Events	SNMP: SNMPv1/v2c/v3 V
	▶ SMTP Client	SNMPv1/v2 Read-Only
	▶ SNMP	SNMPv1 Traps
	▶System Time	Configuration Mode: Trial
	►Auto Logout	Write Startup Config
	▶Syslog Client	Definition Definition
	Fault	Set values Refresh
	Monitoring	
	▶PLUG	
	▶ Ping	
	▶ DNS	
	▶ DHCP	
	▶cRSP / SRS	
	Proxy Server	
	▶ SINEMA RC	
	►Interfaces	
	▶Layer 2	
	▶Layer 3	
	▶ Security	



Routing / Masquerading Lab

Unrestricted © Siemens Industry, Inc. 2017 All rights

Routing / Masquerading – Disable Firewall Lab

- 1) Navigate to and click on Security
- 2) Navigate to and click on Firewall
- Uncheck the Activate Firewall box
- 4) Click Set Values

	SCALANCE S615 WEB Management (192.168.1.1) - Google Chrome	- + 2
SCALANCE S61	5 WEB // ×	Patr
← → C 🕕 1	92.168.1.1	ବ ମ 🛧 🔓 🚺 🕪 🐥
		English 🔻 🖸
SIEMENS		
	192.168.1.1/SCALANCE S615	03/22/2017 07:13:52
Welcome admin	Firewall General	
		• ? •
Logout	General Predefined IPv4 IP Services ICMP Services IP Protocols IP Rules	
Wizards		
Information	Activate Firewall	
D	TCP Idle Timeout [s]: 86400	
system	UDP Idle Timeout [s]: 300	
terfaces	rower rate intrieoux (s); sou	
ayer 2	Set Values Refresh	
aver 3		
ayero		
ecurity		
Users		
Passwords		
Certificates		
Client		

SIEMENS

Unrestricted © Siemens Industry, Inc. 2017

Routing / Masquerading – Enable Masquerading Lab

- 1) Navigate to and click on Layer 3
- 2) Navigate to and click on NAT
- 3) Check the Enable Masquerading for vlan2 (EXT)
- 4) Click Set Values

SIEMENS

Interface

ppp2

vlan1 (INT)

vlan2 (EXT)

192.168.1.1/SCALANCE S615 Internet Protocol (IP) Masquerading

Enable Masquerading

Image: A transmission
 Ima

SIEMENS

▶Wizards

Welcome admin

Masquerading NAPT Source NAT NETMAP

► Information

▶System

Interfaces

Layer 2

Static Routes

▶ Subnets

◄Layer 3

▶Security

Set Values	Refresh
------------	---------

Routing / Masquerading – Examine Routing Table Lab

- 1) Navigate to Information
- 2) Navigate to Routing

				SCALANCE S61	5 WEB Management (192.1	l68.1.1) - Google Chrome	- +
SCALANCE S615 WEB N	×						Pre
\rightarrow C $(192.168.7)$	1.1						ର୍ମନ 🔊 🚱 📲 🚺 👻 🐥 ଓ ୮
							English 🔻 Go
SIEMENS							
	192.168.	1.1/SCALA	ANCE S6	15			04/11/2017 12:28:27
Welcome admin	Layer 3: IPv4	Routing Table					
							· ? -
Logout	Routing Table						
Wizards	j						
Information	Destination	Subnet Mask	Gateway	Interface	Metric	Routing Protocol	
▶ Start Page	Network 0.0.0.0	0.0.0	172.16.10.1	vlan2	not used	static	
Versions	172.16.0.0	255.255.0.0	0.0.0.0	vlan2	0	connected	
ARP Table	192.168.1.0	255.255.255.0	0.0.0	vlan1	0	connected	
Log Tables	3 entries.						
▶ Faults	Defeash						
DHCP Server	Reiresh						
LLDP							
Routing							
▶IPsec VPN							
▶SINEMA RC							
OpenVPN Client							
System							
nterfaces							
ayer 2							
ayer 3							
Security							

SIEMENS

Unrestricted © Siemens Industry, Inc. 2017 All rights reserved.

Routing / Masquerading – Ping Test Lab

- 1) Ping S615 Internal Address
- 2) Ping S615 External Address (172.16.X.1 where X is the station number assigned to you)



Routing / Masquerading – Configure PC Gateway Address Lab

- 1) Right Click on the Network Icon in the Notification Area
- 2) Click on Open Network and Sharing Center
- 3) Click Change adapter settings
- 4) Select the connected network and double click
- 5) Accept the Windows warning by clicking Yes



Routing / Masquerading – Configure PC Gateway Address Lab

- 1) Click on Internet Protocol Version 4 (TCP/IPv4)
- 2) Click Properties
- 3) Enter Default Gateway
- 4) Click OK until all the way out of the network properties screens.
- 5) Close any remaining open screens.

eth0 Properties	— ×
Networking Authentication Sharing	
Connect using:	
Intel(R) PRO/1000 MT Desktop Adapter	
Configur	e
This connection uses the following items:	
Client for Microsoft Networks	
Internet Protocol Version 6 (TCP/IPv6)	
✓ → Internet Protocol Version 4 (TCP/IPv4)	
🗹 🔟 Link-Layer Topology Discovery Mapper I/O Driver	
🗹 🛶 Link-Layer Topology Discovery Responder	
Install Uninstall Propertie	s
Description	
Transmission Control Protocol/Internet Protocol. The defau	ult
wide area network protocol that provides communication across diverse interconnected networks.	
	Cancel

Internet Protocol Version 4 (TCP/IPv4)	Properties										
General											
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.											
Obtain an IP address automatical	ly										
O Use the following IP address:											
IP address:	192.168.1.5										
Subnet mask:	255.255.255.0										
Default gateway:	192.168.1.1										
Obtain DNS server address auton	natically										
Ose the following DNS server add	resses:										
Preferred DNS server:											
Alternate DNS server:	· · ·										
Validate settings upon exit	Advanced										
	OK Cancel										

Routing / Masquerading – Ping Test Lab

1. Ping S615 External Address (172.16.X.1 where X is the station number assigned to you)

1. Ping Instructor S615 External Address



SIEMENS

Unrestricted © Siemens Industry, Inc. 2017 All rights reserved.

Routing / Masquerading – Write Startup Config Lab

- 1) Navigate to and click on System
- 2) Navigate to and click on Configuration
 - A. Alternatively, note the hot link at the top of the screen will go to the correct screen
- 3) Click Write Startup Config button
- 4) Acknowledge the Success Popup



Unrestricted © Siem	ens Industry, Inc.	2017 All rights	reserved.
---------------------	--------------------	-----------------	-----------

	Welcome admin	System Configuration
	Logout	Trial Mode Active - Press 'Write Startup Config' button to make your settings persistent
	Logour	
	▶Wizards	Telnet Server
	►Information	SSH Server
าย	▼System	SMTP Client
	Configuration	Syslog Client
	▶ General	DCP Server: Read/Write
	▶Restart	
	▶Load&Save	Time: Manual
	► Events	SNMP: SNMPv1/v2c/v3 V
	▶ SMTP Client	SNMPv1/v2 Read-Only
	▶SNMP	SNMPv1 Traps
	▶System Time	Configuration Mode: Trial
	►Auto Logout	Write Startup Config
	►Syslog Client	Cat Valuas Defrach
	►Fault Monitoring	Set values Reliesi
	▶PLUG	
	▶ Ping	
	▶ DNS	
	▶ DHCP	
	▶cRSP / SRS	
	Proxy Server	
	▶SINEMA RC	
	►Interfaces	
	▶Layer 2	
	►Layer 3	
	▶ Security	



VLAN Lab

Unrestricted © Siemens Industry, Inc. 2017 All rights

VLAN – Default Configuration Lab

- 1) Navigate to and click on Layer 2
- 2) Navigate to and click on VLAN

J SCALANCE SOLD W														x
€ 🛈 🔏 192.168.1.1	1					C	Q. Search	ŝ		☆ 🖻	•	⋒		≡
🙆 Most Visited 🥑 Get	tting Started 🚺 Wel	o Slice Gallery												
SIEMENS 1	92.168.1.	1/SCALA	NCES	6615							03/2	Engli	sh 💌 9 08:37:1	<u>30</u> 18
Welcome admin Vi	irtual Local Are	ea Network (VL	AN) Gen	eral									? :	÷
► Wizards	neral Port Based VL	AN												
 Information System Interfaces ✓Layer 2 ✓UAN Dynamic MAC Aging LLDP Layer 3 Security 	Base Bridge Mode: VLAN ID:	802.1Q VLAN Bridge Select VLAN ID 1 2 2 entries. et Values Refresh	Name INT EXT	Status Static Static	P1 U -	P2 U -	P3 U -	P4 U -	P5 - U					

VLAN – Ping Test Lab

1) Ping the PLC


VLAN – VLAN ID Creation Lab

- 1) In the VLAN ID box, type 3
- 2) Click on the Create button

SCALANCE SE	515 WEB Man × +	F						_							x
€ 🛈 🔏 192.16	58.1.1					C (🔍 Search			☆	ê	+	⋒		≡
🙆 Most Visited 🧕	Getting Started 🚺 W	eb Slice Gallery													
SIEMENS	192.168.1	.1/SCALA	NCE	S615								03/22/	English	n ▼ <u>Go</u>)8:47:36	
Welcome admin	Virtual Local A	rea Network (VL	AN) Gen	eral									t	? :	
Wizards	General Port Based \	/LAN													
 Information System Interfaces Layer 2 VLAN Dynamic MAC Aging LLDP Layer 3 Security 	Base Bridge Mode. VLAN ID	802.1Q VLAN Bridg	e v	Status Static Static	P1 U -	P2 U -	P3 U -	P4 U -	P5 - U						

VLAN – VLAN ID Creation Lab

- 1) The new VLAN is created
- 2) Click in the box under Name and next to the VLAN ID 3 and type in Controls

SCALANCE S615 WEB N	× /											
- → C (i) 192.168.1	l.1											ବ ମ 🏠 🖓 🦉 🚺
												E
SIEMENS	102 168 1	1 1/9		NCE	S615							04/11/20/
	192.100.1	1.1/0			3013							
Welcome admin	Virtual Local A	rea Ne	etwork (V	LAN) Ge	neral							
Logout												
Wizards	General Port Based	VLAN										
	Raso Bridgo Modo	002.10										
Information	VLAN ID):		e v								
System		Select	VLAN ID	Name	Status	P1	P2	P3	P4	P5		
Interfaces			1	INT	Static	U	U	U	U	-		
Laver 2			3	LXI	Static	-	-	-	-	-		
► VLAN		3 entrie	es.									
▶ Dynamic MAC	Create Delete	Set Value	Refresh									
Aging												
Layer 3												
Security												

SCALANCE S615 WEB Management (192.168.1.1) - Google Chrome



- + ×

VLAN – VLAN Renaming Lab

- 1) Select the box under Name and next to VLAN ID 1 and change it to Engineering
- 2) Select the box under Name and next to VLAN ID 2 and change it to Corporate
- 3) Click Set Values

192.16	1.1.8						01	0 6 1						
							G	⊶ Searci	16		1	*	n (-
🕙 Most Visited 🥑	Getting Started 🚺 W	eb Slice (Gallery									 		
													English	🖌 <u>Go</u>
SIEIAIEIAS	192 168 1	1/9		NCES	615							03/22	2/2017 08	3:49:26
	152.100.1	. 1/0	OALA		1015									
Welcome admin	VIITUAI LOCAI AI	rea Ne	twork (V	LAN) Gene	rai								500	~
Logout	0													
Wizards	General Port Based V	/LAN												
Information	Base Bridge Mode:	802.10	VLAN Bridg	je 💌										
Quetam	VLAN ID:	1												
oystern		Select	VLAN ID	Name	Status	P1	P2	P3	P4	P5				
Interfaces			1	Corporate	Static	-	-	-	-	U				
Layer 2			3	Controls	Static			-						
► VLAN		3 entrie	s.											
Aging	Create Delete :	Set Value	es Refrest	1										
▶LLDP			3	-										
Layer 3														
Security														

VLAN – Port Settings Lab

- Click on the U under P3 in the VLAN ID
 1 row and change it to the "-"
- Click on the U under P4 in the VLAN ID 1 row and change it to the "-"
- 3) Click Set Values



VLAN – Port Settings Lab

- Click on the "-" under P3 in the VLAN ID 3 row and change it to "u"
- Click on the "-" under P4 in the VLAN ID 3 row and change it to "u"
- 3) Click Set Values

	515 WEB Man ×	÷												٥	x
€ 0 🔏 192.10	58.1.1						C	Q Search	1		☆自	+	俞		≡
🙆 Most Visited 🧕	Getting Started 🚺 W	eb Slice (Gallery												
CIEMENIC													Englis	h 💌 🤄	<u>io</u>
SIEIMIEINS	192.168.1	. <mark>1/</mark> S	CALA	NCE S	615							03/2	2/2017	08:53:5	9
Welcome admin	Virtual Local A	rea Ne	twork (VI	LAN) Gene	ral										
Logout														?	5
₩izards	General Port Based	VLAN													
▶ Information	Base Bridge Mode VLAN ID	802.1C	Q VLAN Bridg	e 💌											
▶System		Select	VLAN ID	Name	Status	P1	P2	P3	P4	P5					
►Interfaces			1	Engineering	Static	U	U	1	2						
→Layer 2			2	Corporate	Static		575 1 1 1 1 1	- u	u	-					
► VLAN		3 entrie	S.												
► Dynamic MAC															
►LLDP	Create Delete	Set Value	es Refresh	1											
▶Layer 3			-0												
▶Security															

Unrestricted © Siemens Industry, Inc. 2017 All rights reserved.

VLAN – Port Settings Lab

- 1) Click on the Port Based VLAN tab
- Click on the dropdown under Port VID in the P3 row and change it from VLAN1 to VLAN3
- Click on the dropdown under Port VID in the P4 row and change it from VLAN1 to VLAN3

4) Click Set Values

€ 🛈 🔏 192.16	8.1.1				C' (Search	☆自	+		Ξ
a Most Visited 🥹	Getting Started	l 🚺 Web Slice G	iallery							
SIEMENS	192.16	68.1.1/S	CALANC	CE S615				03/22	English 💌 💁	1
Welcome admin	Port Base	ed Virtual Lo	cal Area Net	work (VLAN) Co	nfiguration				?	
<u>Logout</u> Wizards	General Port	Based VLAN	_	_	-	_	-			
Information System	All ports	Priority No Change	Port VID No Change 🖵	Acceptable Frames No Change	Ingress Filtering • No Change	Copy to Table Copy to Table				
Interfaces Layer 2 VLAN Dynamic MAC Aging LLDP Layer 3 Security	Port P1 P2 P3 P4 P5	Priority 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Port VID VLAN1 VLAN1 VLAN1 VLAN1 VLAN2 VLAN1 VLAN2	Acceptable Frames AII AII AII AII AII AII	Ingress Filtering	2				

VLAN – Port Settings Lab

1) The Port Based VLAN screen should look like these settings

🗲 🛈 🎽 192.16	8.1.1						C Q	Search	☆	Ê	÷	A		=
🦲 Most Visited 🧕	Getting Started	Web Slice	Gallery											
SIEMENS	192.16	68.1.1/S	CALAN		E S615						03/22	English /2017 0	<mark>ب</mark> و	<u>30</u> 49
Welcome admin	Port Base	ed Virtual Lo	ocal Area N	letwo	ork (VLAN) Co	nfiç	juration					E	? ,	-
►Wizards	General Port	Based VLAN								-	-			
▶ Information		Priority	Port VID	A	Acceptable Frames		Ingress Filtering	Copy to Table						
▶ System	All ports	No Change	No Change	•	No Change	-	No Change	Copy to Table						
▶ Interfaces	Port	Priority	Port VID	A	Acceptable Frames		Ingress Filtering	i -						
-Lavor 9	P1	0	VLAN1	-	All	-								
*Layer 2	P2	0	VLAN1	-	All	-	V							
N Dunamic MAC	P3 P4	0	VLAN3											
Aging	P5	0	VLAN2		All									
 ►LLDP ►Layer 3 ►Security 	Set Values	Refresh												

VLAN – Port Settings Lab

- 1) Click on the General tab
- 2) The u under P3 and P4 in the VLAN ID3 row should now be a capital "U"

SCALANCE SE	615 WEB Man ×	F													X
€ 🛈 🔏 192.16	68.1.1						C	🔍 Search	1		☆自	4	⋒		≡
🦲 Most Visited 🧕	Getting Started 🚺 W	eb Slice (Gallery												
SIEMENS													Englis	h 💌 🧕	òo
SIEMIENS	192.168.1	. <mark>1/</mark> S	CALA	NCE S	615							03/22	2/2017	09:00:5	i8
Welcome admin	Virtual Local A	rea Ne	twork (VI	AN) Gene	ral										
Logout														? ?	3
►Wizards	General Port Based	/LAN													
▶Information	Base Bridge Mode	802.10	VLAN Brida	e 🔽											
> Milorinidadori	VLAN ID	5													
▶System		Select	VLAN ID	Name	Status	P1	P2	P3	P4	P5					
▶Interfaces			1	Engineering	Static	U	U	-	-	-					
→Layer 2			3	Controls	Static		1 0.00	U	U	-					
► VLAN		3 entrie	s.												
► Dynamic MAC				-											
►LLDP	Create	Set Value	Refresh												
N aver 2															
F Layer 5															
▶ Security															

VLAN – Ping Test Lab

SIEMENS

1) Ping the PLC



VLAN – Write Startup Config Lab

- 1) Navigate to and click on System
- 2) Navigate to and click on Configuration
 - A. Alternatively, note the hot link at the top of the screen will go to the correct screen
- 3) Click Write Startup Config button
- 4) Acknowledge the Success Popup



Unrestricted ©	Siemens	Industry,	Inc. 2017	' All	rights	reserved.
----------------	---------	-----------	-----------	-------	--------	-----------

	Welcome admin	System Configuration
		Trial Mode Active - Press 'Write Startup Config' button to make your settings persistent
	Logout	
	▶Wizards	✓ Telnet Server
	▶Information	SSH Server
~	, mondation	HTTPS Server only
e	▼System	SMTP Client
	► Configuration	Syslog Client
	General	DCP Server: Read/Write
	▶Restart	
	▶Load&Save	Time: Manual
	▶Events	SNMP: SNMPv1/v2c/v3 V
	▶SMTP Client	SNMPv1/v2 Read-Only
	▶ SNMP	SNMPv1 Traps
	▶System Time	Configuration Mode: Trial
	► Auto Logout	Write Startup Config
	Syslog Client	Cot Voluce Defreeh
	Fault Monitoring	Set values Reliesi
	▶ PLUG	
	▶Ping	
	▶ DNS	
	▶ DHCP	
	▶cRSP / SRS	
	Proxy Server	
	▶ SINEMA RC	
	▶ Interfaces	
	▶Layer 2	
	▶Layer 3	
	▶ Security	



VLAN Routing Lab

Unrestricted © Siemens Industry, Inc. 2017 All rights

VLAN Routing – Initial Screen Lab

- 1) Navigate to and click on Layer 3
- 2) Navigate to and click on Subnets



VLAN Routing – Initial Screen Lab

1) Ping the HMI at IP Address 10.0.0.1X where X is the station number assigned to you



- 1) Navigate to and click on Layer 3
- 2) Navigate to and click on Subnets
- 3) In the Interface dropdown, select VLAN3
- 4) Click Create



- 1) Note the new vlan3 interface
- 2) Either the Configuration tab can be clicked or the vlan3 that is underlined can be clicked to go to the configuration of the interface

								1	_
SIEMENS								English	
	192.168.	1.1/SCA	LANCE S	615			(03/22/2017 0	9:59
Welcome admin	Connected Su	bnets Overv	view						
1								Ē	3?
Logour	Overview Configura	ition							
Wizards									
Information	Interface: VLAN1	•							
▶Svstem									
	Select	Interface	TIA Interface	Interface Name	MAC Address	IP Address	Subnet Mask	Address	Туре
Interfaces		vlan1	yes	INT	20-87-56-15-c1-30	192.168.1.1	255.255.255.0	Primary	
Layer 2		vlan2	1	EXT	20-87-56-15-c1-34	172.16.1.1	255.255.0.0	Primary	
		vlan3	-	vlan3	20-87-56-15-c1-32	0.0.0.0	0.0.0.0	Primary	
▼Layer 3		ppp2	-	ppp2	00-00-00-00-00	0.0.0.0	0.0.0	Primary	
 Static Routes 		loopback0		loopback0	00-00-00-00-00-00	127.0.0.1	255.0.0.0	Primary	
▶ Subnets	•			III					
▶NAT	5 entrie	S.							
Security									
Geounty									
	Oraște Delate	Defrech							
	Create Delete	Retresh							

- 1) Click on the Configuration tab
- 2) Click in the box next to Interface Name: and change it from INT to Engineering
- 3) Click Set Values



SIEMENS

Page 52

 Click the dropdown next to Interface (Name): and select vlan2 (EXT)



- 1) Click in the box next to Interface Name: and change the name from EXT to Corporate
- 2) Click Set Values



 Click on the dropdown next to Interface (Name): and select vlan3



- 1) Click in the box next to Interface Name: and change it from vlan3 to Controls
- 2) Click in the box next to IP Address: and enter 10.0.0.1
- 3) Click in the box next to Subnet Mask and enter in 255.255.255.0
- 4) Click Set Values



Routing / Masquerading – Enable Masquerading Lab

- 1) Navigate to and click on Layer 3
- 2) Navigate to and click on NAT
- 3) Check the Enable Masquerading for vlan3 (Controls)
- 4) Click Set Values

Welcome admin	Internet Pr	rotoco	ol (IP) Mas	squerad	ing
Logout					
▶Wizards	Masquerading	NAPT	Source NAT	NETMAP	
►Information	Interface		Enable Maso	querading	
▶System	vlan1 (Engine vlan2 (Corpo	eering) orate))	
►Interfaces	vlan3 (Contro	ols)	 ✓ ✓)	
▶Layer 2	Set Values	Refresh		,	
■Layer 3	Oct Values	Rencon			
Static Routes					
▶Subnets					
▶ NAT					
▶Security					

1) Ping the PLC at IP Address 10.0.0.1X where X is the station number assigned to you



VLAN Routing – Write Startup Config Lab

- 1) Navigate to and click on System
- 2) Navigate to and click on Configuration
 - A. Alternatively, note the hot link at the top of the screen will go to the correct screen
- 3) Click Write Startup Config button
- 4) Acknowledge the Success Popup



Unrestricted ©) Siemens	Industry,	Inc. 2017	All rights	reserved.
----------------	-----------	-----------	-----------	-------------------	-----------

	Welcome admin	System Configuration
		Trial Mode Active - Press 'Write Startup Config' button to make your settings persistent
	Logout	
	▶Wizards	
	▶ Information	SSH Server
e	▼System	SMTP Client
	► Configuration	Syslog Client
	▶General	DCP Server: Read/Write
	▶Restart	
	▶Load&Save	Time: Manual
	▶Events	SNMP: SNMPv1/v2c/v3 V
	▶ SMTP Client	SNMPv1/v2 Read-Only
	▶SNMP	SNMPv1 Traps
	▶System Time	Configuration Mode: Trial
	►Auto Logout	Write Startup Config
	▶Syslog Client	Sat Values Patrosh
	Fault Monitoring	oer values Reliesi
	▶ PLUG	
	▶ Ping	
	▶ DNS	
	▶ DHCP	
	▶cRSP / SRS	
	Proxy Server	
	▶SINEMA RC	
	►Interfaces	
	Layer 2	
	►Layer 3	
	h Coourity	



1:1 NAT Lab – DNAT

Unrestricted © Siemens Industry, Inc. 2017 All right

- 1) Navigate to and click on Layer 3
- 2) Navigate to and click on NAT
- 3) Click on the NETMAP tab

SCALANCE SE	515 WEB Man × +									-	Ø	83
€ 🛈 🔏 192.16	58.1.1				C	Q Search	☆	Ê	4	俞		≡
🙆 Most Visited 🧕	Getting Started 🚺 Web Slice Gallery						11. 222.02					
SIEMENS	192.168.1.1/SCA	LAN		615					03/22	Englis	h 💽 ⊆ 12:58:1	<u>io</u> 18
Welcome admin	NETMAP										- ? ,	1
Wizards	Masquerading NAPT Source NAT	IETMAP	i									
Information System Interfaces Layer 2 Layer 3 Static Routes Subnets NAT Security	Type: Source Interface: Destination Interface: Source IP Subnet: Translated Source IP Subnet: Destination IP Subnet: Translated Destination IP Subnet:	Source vlan1 (I vlan1 (I Select < 0 entrie	Engineering) Engineering) Type	Source Interface	_	Destination Interface	Source	P Sul	bnet		Fransla Subnet ⊁	þ

1) Click the dropdown next to Type: and select Destination



 Click the dropdown next to Source Interface: and select vlan2 (Corporate)



1:1 NAT – Destination NAT Lab

1) Click the dropdown next to Destination Interface: and select vlan3 (Controls)



1) Click the box next to Source IP Subnet: and type in 172.16.10.1/32

SCALANCE 56	i15 WEB Man × +										٥	x
€ 🛈 🔏 192.16	8.1.1				C	Q Search	☆	Ê	+	Â		≡
🙆 Most Visited 🧕	Getting Started 🚺 Web Slice Gallery											
SIEMENS	192 168 1 1/SCA		ICF S	615					03/2	Engli 2/2017	sh 💽 9	<u>30</u> 07
Welcome admin	NETMAP			010							?	-
▶Wizards	Masquerading NAPT Source NAT N	IETMAP										
 ► Information ► System ► Interfaces ► Layer 2 ► Layer 3 	Type: Source Interface: Destination Interface: Source IP Subnet: Translated Source IP Subnet Destination IP Subnet Translated Destination IP Subnet	Destina vlan2 (C vlan3 (C 172.16.	ation Corporate) Controls) 10.1/32				10					
Subnets		Select	Туре	Source Interface		Destination Interface	Source	IP Su	bnet		Transla Subnet	ati :
► Security	Create Delete Refresh	• Contries	3.	m							,	

1:1 NAT – Destination NAT Lab

1) Click the box next to Destination IP Subnet: and type in 172.16.X.50/32 where X is the number of the station assigned to you



1:1 NAT – Destination NAT Lab

- Click the box next to Translated Destination IP Subnet: and type in 10.0.0.1X/32 where X is the number of the station assigned to you
- 2) Click Create

	615 WEB Man × +										Ø	23
< () ≤ 192.10	68.1.1				C	Q Search	☆	Ê		俞		≡
🙆 Most Visited 🧕	Getting Started 🚺 Web Slice Gallery											
SIEMENS	192.168.1.1/SCA	LAN	CE S	615					03/22	Englis	in 💌 9 13:36:2	<u>30</u> 26
Welcome admin	NETMAP										? ,	i.
▶ Wizards	Masquerading NAPT Source NAT	NETMAP										
Information System Interfaces Layer 2 Layer 3	Type: Source Interface: Destination Interface: Source IP Subnet: Translated Source IP Subnet: Destination IP Subnet: Translated Destination IP Subnet:	Destination vlan2 (Co vlan3 (Con 172.16.10 172.16.1.5 10.0.0.10/	on rporate) ntrols)).1/32 50/32 /32	•								
 Static Routes Subnets NAT Security 	Create Delete Refresh	Select	Туре	Source Interface		Destination Interface	Sourc	e IP Su	bnet		Fransla Subnet ♪	D



- 1) Note the entry for Destination NAT
- 2) The instructor will perform a ping test

C © 192.168.1.1 SIEMENS 192.168.1.1/SCALANCE S615 Welcome admin NETMAP Logoat Wasquerading NAPT Source NAT NETMAP VWzards Information Source Interface: vian3 (Controls) Source Interface: vian3 (Controls) Source Interface: vian3 (Controls) Layer 2 Layer 3 Static Routes Submets Submets Submets Layer 4 Layer 4 Layer 4 Layer 5 Layer 6 Layer 7	역 가 쇼 등 가 가 다 다 다 다 다 다 다 다 다 다 다 다 다 다 다 다 다
SIEMENS Bug2.168.1.1/SCALANCE S615 Welcome adm NETMAP Logon Masquerading NAPT Source NAT NETMAP Witards Information Source Interface Van2 (Corporate) V System Source Interface Van2 (Corporate) V Source Interface Van2 (Corporate) V Destination Interface Van2 (Corporate) V System Source IP Subnet: IT2:16.1.50/32 Translated Destination IP Subnet: Translated Source IP Destination IP Subnet: Destination IP Subnet: Translated Source IP Destination IP Subnet: Static Routes Select Type Source Interface Van3 Translated Source IP Destination IP Subnet: Static Routes Subnets Unit Select Type Source Interface Vial Translated Source IP Destination IP Subnet Static Routes Subnets Unit Subnet Translated Source IP Destination IP Subnet NAT Select Type Source Interface Vian3 Type Translated Source IP Destination IP Subnet NAT Item Itenty. Vian3 Type </th <th>English 04/11/2017 14</th>	English 04/11/2017 14
Since information Vitrands	04/11/2017 14
Wetcome admin NETMAP Logout Masquerading NAPT Source NAT NETMAP Wizards Masquerading NAPT Source NAT NETMAP Wizards Type: Destination Varia (Corporate) Source Interface: Varia (Corporate) Viards Varia (Corporate) Source IP Subnet: 172.16.1.0.1/32 Translated Source IP Subnet: 172.16.1.0.1/32 Translated Source IP Subnet: 172.16.1.0.1/32 Translated Destination IP Subnet: 172.16.1.0.1/32 Translated Destination IP Subnet: 172.16.1.0.1/32 Static Routes Source IP Subnet: Static Routes Source Interface: Static Routes Destination IP Subnet: Static Routes Type: Static Routes Destination Van2 Static Routes Destination Van2 Static Routes Type: Static Routes T	
Logod Masquerading NAPT Source NAT NETMAP Wizards	
Logoti Wizards Masquerading NAPT Source NAT NETMAP Information Type: Destination Type: Destination <	per
Wizards Masquerading NAP1 Source NAI NEt MAP Information Type: Destination Viazards Source Interface: Vian3 (Controls) Vian4 Vian3 (Controls) Vian4 Vian4 (Controls) Vian	
Information System Information System Interfaces Source IP Subnet: It2.16.10.1/32 Translated Source IP Subnet: It2.16.10.1/32 Translated Source IP Subnet: It2.16.10.1/32 Translated Destination IP Subnet: It2.16.10.1/32 It2.16.10.1	
Information Inferface: Usesination Interface: Van2 (Corporate) System Destination Interface: Van3 (Controls) Destination Interface: Van3 (Controls) Interfaces Source IP Subnet: 172.16.10.1/32 Translated Source IP Subnet: 172.16.10.1/32 Translated Destination IP Subnet: 172.16.10.1/32 Translated Destination IP Subnet: 172.16.10.1/32 Layer 2 Destination IP Subnet: 172.16.10.1/32 Translated Destination IP Subnet: 172.16.10.1/32 Layer 3 Static Routes Subnets Subnets Layer 3 I entry.	
System Destination Interface: Variat (Colorate) Destination Interface: Variat (Controls) Interfaces Source IP Subnet: Translated Source IP Subnet: Translated Source IP Subnet: Translated Source IP Subnet: Translated Source IP Subnet: Translated Destination IP Subnet: Static Routes Static Routes Subnets NAT	
Interfaces Source IP Subnet 172.16.10.1/32 Interfaces Source IP Subnet 172.16.10.1/32 Image: Application IP Subnet 172.16.1.50/32 Translated Destination IP Subnet 172.16.1.50/32 Static Routes Select Type Subnets Select Type Image: Application Interface Source IP Subnet Image: Application Interface Source IP Subnet Image: Application IP Subnet Image: Application Translated Destination IP Subnet Image: Application IP Subnet Image: Application IP Subnet Image: Application Select Type Source Interface Source IP Subnet Image: Application IP Subnet Image: Application Image: Application Image: Application Image: Application Image: Application Image: Application Image: Application Image: Application Image: Application Image: Application Image: Application Image: Application Image: Application Image: Application Image: Application Image: Application Image: Application Image: Application Image: Application Image: Application Image: Application Image: App	
Auge 2 Source IP Subnet: Translated Source IP Subnet: T72.16.1.50/32 Layer 3 Translated Destination IP Subnet: 10.0.0.10/32 Static Routes Select Type Source Interface Source IP Subnet: Translated Source IP Static Routes Select Type Source Interface Destination Interface Source IP Subnet: Destination IP Subnet: NAT Interface Interface Source IP Subnet: Translated Source IP Destination IP Subnet:	
Layer 2 Destination IP Subnet 172.16.1.50/32 Layer 3 Translated Destination IP Subnet 10.0.01/32 Static Routes Select Type Source Interface Destination Interface Source IP Subnet Subnet Destination IP Subnet NAT Interface	
Static Routes Select Type Source Interface Destination Interface Source IP Subnet Translated Source IP Destination IP Subnet > Static Routes > Select Type Source Interface Destination Interface Source IP Subnet Destination IP Subnet > NAT Interface Interface Interface Source IP Subnet Translated Source IP Destination IP Subnet	
Select Type Source Interface Destination Interface Source IP Subnet Translated Source IP Destination IP Subnet > Subnets Destination vlan2 vlan3 172.16.10.1/32 - 172.16.1.50/32	
Static Routes Destination vlan2 vlan3 172.16.10.1/32 - 172.16.1.50/32	Translated Destination IP
► NAT 1 entry.	10.0.0.10/32
Security Create Delete Refresh	

Unrestricted © Siemens Industry, I....

- 1) Click the check box next to the NAT rule in the Select column
- 2) Click Delete





1:1 NAT Lab – NAPT

Unrestricted © Siemens Industry, Inc. 2017 All rights

1:1 NAT – NAPT Lab

1) Click the NAPT Tab



1:1 NAT – NAPT Lab

1) Click the dropdown next to the Source Interface: and select vlan2 (Corporate)


SIEMENS

1:1 NAT – NAPT Lab

- 1) Make sure there is a check in the box next to User Interface IP from Source Interface
- 2) In the box next to Destination Port: enter the value 4443
- 3) In the box next to Translated Destination IP Address: enter the IP Address 10.0.0.1X where X is the number of the station assigned to you
- 4) In the box next to Translated Destination Port: enter the value 443
- 5) Click Create

SCALANCE S6	i15 WEB Man × +											X
€ 🛈 🔏 192.16	8.1.1				C	Q Search		☆∎	a 🔸	A		≡
🙆 Most Visited 🧕	Getting Started 🚺 Web Slice Gallery											
SIEMENS	192.168.1.1/SCAL	AN	CE S615						03/2	Englis	h 💌 🤄 15:22:3	io 4
Welcome admin <u>Logout</u>	IP Network Address Port Tr	ranslat	tion (NAPT) (F	Port Forwa	rding)						- ? ;	ŝ
Wizards	Masquerading NAPT Source NAT N	TMAP										
 Information System Interfaces Layer 2 Layer 3 Static Routes Subnets NAT Security 	Source Interface: Traffic Type: Destination IP Address: Destination Port: Translated Destination IP Address: Translated Destination Port:	Vlan2 (C TCP - Use I 172.16. 4443 10.0.0.1 443 Select • 0 entries	Corporate) Interface IP from Sc I.1 Source Interface S.	Traffic Type	Interface IP	9 Destination IP	Destinati	on Port	Transl: Destin	ated ation IP	T C	1

1:1 NAT – NAPT Lab

- 1) Note the final entry
- 2) Instructor will test by browsing to the IP Address of the station utilizing port 4443.



1:1 NAT – NAPT Lab

- 1) Click the check box next to the NAPT rule in the Select column
- 2) Click Delete





1:1 NAT Lab – Double NAT

Unrestricted © Siemens Industry, Inc. 2017 All rights

1:1 NAT – Double NAT Lab

- 1) Click the NETMAP tab
- 2) Select Type: Destination
- 3) Source Interface: vlan1 (Engineering)
- 4) Destination Interface: vlan3 (Controls)



SIEMENS

1:1 NAT – Double NAT Lab

- 1) In the box next to Source IP Subnet: enter 192.168.1.5/32
- 2) In the box next to Destination IP Subnet: enter 192.168.1.50/32
- 3) In the box next to Translated Destination IP Subnet: enter 10.0.0.1X/32 where X is the number of the station assigned to you

4) Click Create



1:1 NAT – Double NAT Lab

- 1) Note the newly added Destination NAT rule
- 2) Select Type: Source



SIEMENS

1:1 NAT – Double NAT Lab

- 1) In the box next to Source IP Subnet: enter 192.168.1.5/32
- 2) In the box next to Translated Source IP Subnet: enter 10.0.0.50/32
- In the box next to Destination IP Subnet: enter 10.0.0.1X/32 where X is the number of the station assigned to you

4) Click Create



SIEMENS

1:1 NAT – Double NAT Lab

- 1) Note final configuration
- 2) Test configuration by trying to ping 192.168.1.50

	ANCE S615 WEB Man	× +	-										x
(€) 🛛 📈	192.168.1.1					67% C ⁴	Q. Search		☆ 自	•	⋒		≡
🙆 Most Visi	ited 🥹 Getting Started	We	eb <mark>Slice</mark>	Gallery									
SIEMENS	192.168.1.1/SC	ALAN		S615							a	English	999 06:57
Welcome admin	NETMAP												? 🔒
Logout	Masquerading NAPT Source NAT	NETMAP	2										
* Wizaros	Time	Source											
* mormation	Source interface	vlan1 ((Engine	erina)									
* System	Destination Interface	vlan1 ((Engine	ering)									
▶ interfaces	Source IP Subnet												
*Layer 2	Translated Source IP Subnet												
+Layer 3	Translated Destination IP Subret												
+Static Routes		Colort	Turn	Courses interations	Destination Interface	Province ID Pulment	Translated Source IP	Portiention ID Subart	Translated De	stination IP			
* Subnets		JOIEU.	The	Source intendoe	Destination internatio	Source IP Sourier	Subnet	Destination of Subries	Subnet		6		
►NAT			Destination	vlan1	vlan3	192.168.1.5/32	-	192.168.1.50/32	10.0.0.10/32				
*Security			Source	vlan1	vian3	192.168.1.5/32	10.0.0.50/32	10.0.0.10/32	5				
		2 entries.											
	Create Delete Refresh												

1:1 NAT – Write Startup Config Lab

- 1) Navigate to and click on System
- 2) Navigate to and click on Configuration
 - A. Alternatively, note the hot link at the top of the screen will go to the correct screen
- 3) Click Write Startup Config button
- 4) Acknowledge the Success Popup



	Welcome admin	System Configuration
	Logout	Trial Mode Active - Press 'Write Startup Config' button to make your settings persistent
	Logoar	
	▶Wizards	Telnet Server
	▶ Information	SSH Server
ne	▼Svstem	HTTPS Server only SMTP Client
	Configuration	Syslog Client
	▶ General	DCP Server: Read/Write
	▶Restart	
	▶Load&Save	Time: Manual
	▶Events	SNMP: SNMPv1/v2c/v3 V
	▶SMTP Client	SNMPv1/v2 Read-Only
	▶ SNMP	SNMPv1 Traps
	System Time	Configuration Mode: Trial
	Auto Logout	Write Startup Config
	Syslog Client	Set Values Refresh
	Fault Monitoring	
	▶ PLUG	
	▶ Ping	
	▶ DNS	
	▶ DHCP	
	▶ cRSP / SRS	
	Proxy Server	
	▶SINEMA RC	
	►Interfaces	
	▶Layer 2	
	▶Layer 3	
	▶ Socurity	



Firewall Lab

Unrestricted © Siemens Industry, Inc. 2017 All rights

Firewall - Initial Lab

- 1) Navigate to and click on Security
- 2) Navigate to and click on Firewall
- 3) Click the box next to Activate Firewall
- 4) Click Set Values

	: S615 WEB Man × +
() (htt	ps://192.168.1.1
Most Visited	🥑 Getting Started 🏹 Web Slice Gallery
SIEMENS	192.168.1.1/SCALANCE S615
Welcome admin	Firewall General
▶Wizards	General Predefined IPv4 IP Services ICMP Services IP Protocols IP Rules
▶In formation	CO His Treat Is 2000
▶System	UDP Idle Timeout [s]: 300
Interfaces	ICMP Idle Timeout [s]: 300
▶Layer 2 ▶Layer 3	Set Values Refresh
*Security	
▶Users	
▶Passwords	
▶Certificates	
Firewall	
▶IPsec VPN	
▶ OpenVPN Client	

Firewall – Predefined Rules Lab

SIEMENS

1) Note the predefined firewall rules

SIEMENS	192.16	8.1.1/	SCAL	ANC	E S61	15							
Welcome admin	Predefine	d IPv4											
Wizards	General Pred	efined IPv4	IP Servic	es ICMP	Services	P Protocols	IP Rules						
Information	Allow devic	ce services:		10		16 1			x.	22		10	
System	Interface vlan1	All	HTTP	HTTPS	TFTP	DNS	SNMP	Teinet	IPsec VPN	SSH	DHCP	Ping	
Interfaces	vlan2 vlan3												
Layer 2	Set Values	Refresh							he trate				
Security													
▶Users													
▶Passwords													
▶Certificates													
Firewall													
▶IPsec VPN													
▶ OpenVPN Client													

Firewall – IP Services Lab

- 1) Click the IP Services tab
- 2) In the box next to Service Name: enter HTTPS
- 3) Click Create

SIEMENS

	192.168.	1.1/S	CALANCE S	615		
Welcome admin	Internet Prot	ocol (IP) Services			
Logout			10000			
Vizards	General Predefin	ed IPv4	P Services ICMP Service:	s IP Protocols	IP Rules	_
formation	Service Name: H	ITTPS				
System	s	elect	Service Name	Transport	Source Port (Range)	Destination Port (Range)
nterfaces	0	entries.				
ayer 2	Create Delete	Refresh				
ayer 3	N					
ecurity						
•Users						
▶ Passwords						
Certificates						
Firewall						
▶IPsec VPN						
▶OpenVPN Client						

Firewall – IP Services Lab

1) Ensure that the dropdown for Transport shows TCP

▶Wizards

▶System

▶Interfaces

▶Layer 2

▶Layer 3

*Security Users

> Firewall ▶ IPsec VPN ▶ OpenVPN Client

Information

- Ensure the Source Port (Range) box 2) shows *
- In the box under Destination Port 3) (Range) enter the value 443
- Click Set Values 4)

SIEMENS 192.168.1.1/SCALANCE S615 Internet Protocol (IP) Services Welcome admin Logout General Predefined IPv4 IP Services ICMP Services IP Protocols IP Rules Service Name: Source Port **Destination Port** Service Name Select Transport (Range) (Range) * 443 HTTPS TCP 1 entry. Create Delete Set Values Refresh ▶ Passwords ▶Certificates

Unrestricted © Siemens Industry, Inc. 2017 All rights reserved.

Firewall – IP Rules Lab

SIEMENS

1) Click on the IP Rules Tab

SIEMENS

192.168.1.1/SCALANCE S615

Welcome admin	Internet I	Protoc	ol (IP) Ru	lles							
Logout											
₩izards	General Pre	defined	IPv4 IP Se	rvices ICMP	Services IP Pr	otocols IP Rules					
Information	IP Version:	IPv4 👻									
▶Svstem		Select	Protocol	Action	From	То	Source (Range)	Destination (Range)	Service	Log	Precedence
▶Interfaces		0 entries	S.								
▶Layer 2	Create E	Delete	Refresh								
▶Layer 3											
*Security											
⊌Users											
▶ Passwords											
▶Certificates											
Firewall											
▶IPsec VPN											
▶OpenVPN Client											

Unrestricted © Siemens Industry, Inc. 2017 All rights reserved.

Firewall – IP Rules Lab

- 1) Click Create
- 2) Set Action to Accept
- 3) Set From to vlan1 (Engineering)
- 4) Set To as Device
- 5) Enter Source (Range) as 0.0.0/0
- 6) Enter Destination (Range) as 192.168.1.0/24
- 7) Set Service as HTTPS
- 8) Set Log as critical
- 9) Click Set Values

IP Version:	IPv4 ▼]										
	Select	Protocol	Action		From	То	Source (Range)	Destination (Range)	Service	Log		Precedence
		IPv4	Accept	•	vlan1 (Engineering▼	Device •	0.0.0/0	192.168.1.0/24	HTTPS 🔻	critical	T	0
	1 entry.											
Create	elete	et Values Ref	resh									

Firewall – Disable Predefined IPv4 HTTPS Lab

SIEMENS

- Click on the Predefined IPv4 tab 1)
- 2) Under the HTTPS column in the vlan1 row **uncheck** the box
- 3) Click Set Values

Welcome admin	Predefine	d IPv4										
Wizards	General Pred	efined IPv4	IP Services	ICMP	Services	IP Protocols	IP Rules		-	-	-	-
Information	Allow devic	All		TTDS	TETD	DNS	SNMD	Telnet	IDeec V/DN	CCH	DHCD	Ding
System	vlan1	~ "		[]]						331		ring V
Interfaces	vlan2											
Layer 2	Set Values	Refresh										
Layer 3		v										
Security												
▶Users												
▶ Passwords												
▶ Certificates												
▶Firewall												
+IPsec VPN												

Firewall – Test HTTPS Lab

- 1) Navigate to https://192.168.1.1
- 2) There will be a security exception that will need to be confirmed
- 3) You should be taken to the secure web page for the S615

	S615 WEB Man × +
🔶 🛈 💁 http	ps://192.168.1.1
Most Visited	😕 Getting Started 🚺 Web Slice Gallery
SIEMENS	192.168.1.1/SCALANCE S615
Welcome admin Logout	SCALANCE S615
 >Wizards >Information >System >Interfaces >Layer 2 >Layer 3 >Security 	<complex-block></complex-block>
	System Name: sysName Not Set
	Device Type: SCALANCE S615
	PLUG Configuration: ACCEPTED
\sim	PLUG License: ACCEPTED

Page 91

Firewall – Disable Predefined IPv4 Rules Lab

SI

*Wiz

Info

▶Sys

HLay

*Sec +U +F +C +F

1) If HTTPS succeeded, navigate back to the Predefined IPv4 tab

- Under the HTTP column in the vlan1 row uncheck the box
- 3) Acknowledge the Warning
- 4) Uncheck all of the other boxes for vlan1
- 5) Click Set Values

eral Predefined IPv4 IP Services ICMP Services IP Protocols IP R Allow device services: Interface All HTTP HTTPS TFTP DNS SNM vian1 vian2 vian3 vian3 vian3 vian4	IP Services ICMP Services IP Protocols IP R HTTP HTTPS TFTP DNS SNMF Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configurati	4 IP Services ICMP Services IP Protocols IP R Warning: disabling both HTTP and HTTPS Warning: disabling both HTTP and HTTPS HTTP HTTPS TFTP DNS SNMF OF Image: disable of the second
eral Predefined IPv4 IP Services ICMP Services IP Protocols IP R Allow device services: Interface All HTTP HTTPS TFTP DNS SNM vian1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	IP Services ICMP Services IP Protocols IP R HTTP HTTPS TFTP DNS SNM O O O O O O O O O O O O O	4 IP Services ICMP Services IP Protocols IP River access to the web-based configuration. HTTP HTTPS TFTP DNS SNMF Image: Configuration access to the second acces to the second acces to the second access to the second access t
Allow device services: nterface All HTTP HTTPS TFTP DNS SNMP vian1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	HTTP HTTPS TFTP DNS SNMF	HTTP HTTPS TFTP DNS SNMF
Allow device services: Interface All HTTP HTTPS TFTP DNS SNMF vlan1 0 0 0 vlan2 0 0 0 Set Values Refresh	HTTP HTTPS TFTP DNS SNMF Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Image: Configuration Ima	HTTP HTTPS TFTP DNS SNMF
Interface All HTTP HTTPS TFTP DNS SNM vlan1	HTTP HTTPS TFTP DNS SNMF	HTTP HTTPS TFTP DNS SNMF
vlan1		
vlan2		
vlan3 Set Values Refresh		
Set Values Refresh		
Set Values Refresh		

Firewall – Create Drop Rule Lab

- 1) Click on the IP Rules tab
- 2) Click Create
- 3) Set Action to Drop
- 4) Set From to vlan1 (Engineering)
- 5) Set To as Device
- 6) Set Source (Range) as 0.0.0/0
- 7) Set Destination (Range) as 0.0.0/0
- 8) Set Service to all
- 9) Set Log to critical
- 10) Set Precedence to 50
- 11) Click Set Values





Firewall – Ping Test Lab

- 1) Ping 192.168.1.1
- 2) Ping 192.168.1.50



Firewall – Analyze Firewall Log Lab

- 1) Navigate to and click on Information
- 2) Navigate to and click on Log Tables
- 3) Click on the Firewall Log tab
- 4) Identify the ACCEPT and DROP messages

SIEMENS

192.168.1.1/SCALANCE S615 Welcome admin **Firewall Log Table** Logou Event Log Security Log Firewall Log ▶Wizards Severity Filters Information nfo Info ▶ Start Page Warning + Versions Critical ▶ ARP Table Log Tables Restart System Up Time System Time Log Message Severity + Faults tcp:50757->443 DHCP Server DROP(50) in:vlan1 out:lo len:60 +LLDP 03/23/2017 s-mac:B8:CA:3A:D7:C7:28 d-mac:20:87:56:15:C1:30 2d 01:20:16 2 - Critical 10:47:55 s-ip:192.168.1.68 d-ip:192.168.1.1 ▶ Routing icmp:8:0 ▶ IPsec VPN ACCEPT(0) in:vlan1 out:lo len:52 ▶ SINEMA RC 03/23/2017 s-mac:B8:CA:3A:D7:C7:28 d-mac:20:87:56:15:C1:30 2d 01:20:13 2 - Critical 10:47:52 s-ip:192.168.1.68 d-ip:192.168.1.1 ▶ OpenVPN tcp:50756->443 Client DROP(50) in:vlan1 out:lo len:60 03/23/2017 s-mac:B8:CA:3A:D7:C7:28 d-mac:20:87:56:15:C1:30 ▶System 2d 01:20:12 2 - Critical 10:47:51 s-ip:192.168.1.68 d-ip:192.168.1.1 icmp:8:0 Interfaces ACCEPT(0) in vlan1 out lo len:52 62 entries. ▶Layer 2 Clear ▶Layer 3 Refresh **▶**Security

Firewall – Create HTTP Service Lab

- 1) Navigate to and click on Security
- 2) Navigate to and click on Firewall
- 3) Click on the IP Services tab
- 4) Enter HTTP in the box next to Service Name:
- 5) Click Create
- 6) Ensure Transport is TCP
- 7) Ensure Source Port (Range) is *
- 8) Enter the value 80 in the box under Destination port on the HTTP row

SIEMENS 192,168,1,1/SCALANCE S615 Welcome admin Internet Protocol (IP) Services Logout General Predefined IPv4 IP Services ICMP Services IP Protocols IP Rules **▶**Wizards Service Name: Information Source Port **Destination Port** Select Service Name Transport ▶System (Range) (Range) HTTP TCP * * 80 ▶Interfaces * HTTPS TCP 443 ▶Layer 2 2 entries ▶Layer 3 Create Delete Set Values Refresh *Security ▶Users Passwords Certificates Firewall + IPsec VPN ▶ OpenVPN Client

Firewall – Create HTTP Rule Lab

- 1) Click on the IP Rules tab
- 2) Click on Create to create a new rule
- 3) Enter the parameters below for an HTTP rule (shown on the second line)

Select	Protocol	Action	From	То	Source (Range)	Destination (Range)	Service		Log		Precedence-
	IPv4	Accept	👽 vlan1 (Enginee 👻	Device	• 0.0.0.0/0	192.168.1.0/24	HTTPS		critical	-	0
	IPv4	Accept	👻 vlan1 (Enginee 👻	Device	• 0.0.0.0/0	192.168.1.0/24	HTTP	-	none		1
	IPv4	Drop	💂 vlan1 (Enginee 🚽	Device	.0.0.0/0	0.0.0/0	all	-	critical	-	50



Firewall – Create ICMP Service Lab

- 1) Click on the ICMP Services tab
- 2) Enter PingRequest in the box next to Service Name:
- 3) Click Create
- 4) Select Echo Request (8) from the dropdown under Type
- 5) Click Set Values

SIEMENS	192.168	.1.1/	SCALA	NCE S6	15			
Welcome admin	Internet Co	ntrol M	essage Pr	otocol <mark>(ICM</mark> P) Services	Ē		
Wizards	General Predefi	ined IPv4	IP Services	ICMP Services	IP Protocols	IP Rules		
Information	Service Name:							
System		Select	Service Name PingRequest	Protocol ICMPv4	Type	i o Request (8)	Code Code -	-
Interfaces		1 entry.						
Layer 2	Create Delet	e Set Va	lues Refresh	1				
Layer 3			2					
Security								
*Users								
▶Passwords								
▶ Certificates								
Firewall								
* IPsec VPN								
▶OpenVPN Client								

- 1) Click on the IP Rules tab
- 2) Click on Create to create a new rule
- 3) Enter the parameters below for a PingRequest rule for vlan1 to Device and vlan1 to vlan3
- 4) Click Set Values
- 5) Test both HTTP and Ping

General Pred	lefined IF	Pv4 IP Service	s ICMP Serv	ices	IP Protocols IP	Rules						
IP version:	IPv4 ▼											
	Select	Protocol	Action	F	From	То	Source (Range)	Destination (Range)	Service	Log	-	Precedence
		IPv4	Accept	• \	vlan1 (Engineeri 🔻	Device •	0.0.0/0	192.168.1.0/24	HTTPS T	critical	•	0
		IPv4	Accept	• \	vlan1 (Engineeri 🔻	Device •	0.0.0/0	192.168.1.0/24	HTTP 🔻	none	•	1
		IPv4	Accept	• \	vlan1 (Engineeri 🔻	Device •	0.0.0/0	0.0.0/0	PingRequest V	none	•	2
		IPv4	Accept	• \	vlan1 (Engineeri 🔻	vlan3 (Controls) •	0.0.0/0	0.0.0/0	PingRequest V	none	•	3
		IPv4	Drop	• \	vlan1 (Engineeri 🔻	Device •	0.0.0/0	0.0.0/0	all 🔻	critical	•	50
	5 entries	i.										
Create D	elete Se	et Values Refre	esh									

SIEMENS

Unrestricted © Siemens Industry, Inc. 2017 All rights reserved.

Firewall – Reset Lab

			SCALANCE S61	15 WEB Man × +
1)	Delete a	all NETMAP Entries	🛈 <u> https://</u>	/192.168.1.1
		B M	Nost Visited 🧕	Getting Started 🚺 Web Slice Gallery
2)	Disable	Firewall		
/		SIE	EMENS	100 460 4 4/00 AL ANOE 0045
	SCALANCE 56	5615 WEB Man × +		92.168.1.1/SCALANCE 5615
	🗲 🛈 🔏 192.16	168.1.1 C ^a Q Search ☆ 自 🕹 🍙 👽 🚍 W	Velcome admin F	irewall General
	Most Visited	🦻 Getting Started 🚺 Web Slice Gallery	Logout	
	1995	English - Go an	rds	neral Predefined IPv4 IP Services ICMP Services IP Protocols IP Rules
	SIEMENS		mation	Activate Firewall
		192.168.1.1/SCALANCE S615 03/22/2017 12:58:18		TCP Idle Timeout [s]: 86400
	Welcome admin	NETMAP	em	UDP Idle Timeout [s]: 300
	Logout	🗖 ? 占 rfa	faces	ICMP Idle Timeout [s]: 300
	▶Wizards	Masquerading NAPT Source NAT NETMAP	er 2 [Set Values Refresh
	▶ Information	Type: Source	er 3	
	▶Svstem	Source Interface: vlan1 (Engineering)	irity	
	h lotorfocco	Destination Interface: vlan1 (Engineering)	sers	
	Fintenaces	Translated Source IP Subnet	isswords	
	▶Layer 2	Destination IP Subnet:	ertificates	
	▼Layer 3	Translated Destination IP Subnet	rewall	
	► Static Routes	Select Type Source Interface Destination Interface Source IP Subnet Translation Subnet	sec VPN	
	► NAT	✓ m P Sie	ient	
	▶ Security	0 entries.		
		Create Delete Refresh		

Firewall – Write Startup Config Lab

- 1) Navigate to and click on System
- 2) Navigate to and click on Configuration
 - A. Alternatively, note the hot link at the top of the screen will go to the correct screen
- 3) Click Write Startup Config button
- 4) Acknowledge the Success Popup





	Welcome admin	System Configuration
	Logout	Trial Mode Active - Press 'Write Startup Config' button to make your settings persiste
	<u>Logoa</u>	
	♦Wizards	Telnet Server
	▶Information	SSH Server
b a	Finiornation	HTTPS Server only
ne	▼System	SMTP Client
	► Configuration	Syslog Client
	General	DCP Server: Read/Write
	▶Restart	
	▶Load&Save	Time: Manual
	▶Events	SNMP: SNMPv1/v2c/v3
	▶SMTP Client	SNMPv1/v2 Read-Only
	▶SNMP	SNMPv1 Traps
	▶System Time	Configuration Mode: Trial
	►Auto Logout	Write Startup Config
	▶Syslog Client	Sof Values Defresh
	Fault	
	Monitoring	
	▶ PLUG	
	▶ Ping	
	DNS	
	► DHCP	
	▶ cRSP / SRS	
	Proxy Server	
	▶ SINEMA RC	
	►Interfaces	
	▶Layer 2	
	▶Layer 3	
	▶ Security	
	Foecunty	





SIEMENS SINEMA Remote Connect Help 😯 9/19/2017, 6:50:24 PM O Language: English -User name: Password: Log on Unrestricted © Siemens Industry, Inc. 2017 Page 103

SINEMA Remote Connect Lab

- Browse to https://172.16.10.250 1)
- Login using the appropriate credentials 2)
 - A. username: stationOX (where X is the station number)
 - B. password: Admin!123



Lab – Device Creation

1) Click on Create

SIEMENS	SINEMA Remote Connect	Help 🚱	9/26/2017, 11:26:47 AM O	Language: English 🔹
Logged on as "station05"	Devices			
Remote connections Devices Participant groups Mu account	i no filter active Search filter: All Precise match Apply filter Show all			
	Name of the device VPN address Remote subnet Virtual local LAN Status Location Type of connection VPN connection mode Actions Create Import			

Unrestricted © Siemens Industry, Inc. 2017 All rights reserved.

Lab – Device Creation

- Enter a StationOX_S615 (where X is the station number) 1)
- Enter additional (optional) information 2)
- Select the Type of connection as Permanent 3)

Click Next 4)

Page 105

lick Next	SIEMENS		SINEMA Remote Connect								
	Logged on as "admin"		New device								
	Log off	3	Device	VPN connection mode	Network settings	Group memberships	Password	Device overview			
	Exit dialog		Connection parameter	ers:							
			*Name of the dev	vice: Station01_S615							
			GSM num	ber:							
			Device informati	on:							
			Ту	ype: SCALANCE S615							
			Ven	dor: Siemens							
			Locat	ion: Training Class							
			*Type of connect	ion: Permanent	•						
			SMS gateway provi	der:	•						
			Comm	ent: Your Comment Here							
Unrestricted © Siemens Industry, Inc. 20				Nevt							
Page 105				INCXL							

Lab – Device Creation

- 1) Leave the default settings
- 2) Click Next

Page 106

SIEMENS	SINEMA Remote	Connect				
Logged on as "admin"	New device					
Log off	Device VF	PN connection mode	Network settings	Group memberships	Password	Device overview
Exit dialog	Connection parameters: * VPN connection mode: Ipsec profile: Fixed IP address: OpenVPN connection pa	OpenVPN Request virtual IP add Use fixed IP address arameters:	Iress			
	IP address:	IP address of the connection Back	P Connection port	IP protocol	Actions	ocol: tcp • Add

Lab – Device Creation

- 1) Check box next to Connected local subnets
 - A. Local LAN IP address
 - . 192.168.1.1
 - B. Network mask
 - 1. 255.255.255.0
 - C. Check next to Device is a network gateway.

2) Click Add

- 3) Check box next to NAT for local subnet
 - A. Virtual local LAN IP address
 - I. 172.17.X.1(where X is the station number)
 - B. Network mask
 - l. 255.255.255.0
- 4) Click Next

SINEMA Remo New device Device	VPN connection mode			
C New device	VPN connection mode			
Device	VPN connection mode			
		etwork settings Gr	oup memberships Pas	ssword
Connection paramete	rs: bnets			
Local LAN IP ad	dress:			
Network	mask:	Device is a network	gateway	Add
	Local subnet	Network	gateway	Actions
	192.168.1.1/24	Yes		×
1:1 NAT NAT for local subner Virtual local LAN IP ad Network	192.168.1.1/24 192.168.1.1/24 dress: 172.17.6.0 mask: 255.255.255.0	Yes	168.1.1/24 •	X
	Virtual local LAN	Local subnet	Network gateway	Actions
			ganaay	
	Connection parameter Connected local su Local LAN IP ad Network	Connection parameters: Connected local subnets Local LAN IP address: Network mask: Local subnet 192.168.1.1/24 1:1 NAT NAT for local subnet Virtual local LAN IP address: 172.17.6.0 Network mask: 255.255.0 Virtual local LAN	Connection parameters: Connected local subnets Local LAN IP address: Network mask: Local subnet I2 Device is a network 192.168.1.1/24 Yes 1:1 NAT NAT for local subnet Virtual local LAN IP address: 172.17.6.0 Network mask: 255.255.255.0 Local subnet: 192.1	Connection parameters: Connected local subnets Local LAN IP address: Network mask: Local subnet 192.168.1.1/24 Yes 1:1 NAT NAT for local subnet Virtual local LAN IP address: 172.17.6.0 Network mask: 255.255.255.0 Local subnet: 192.168.1.1/24 • Network gateway Network gateway Network gateway Network gateway

Back

Next

SINEMA Remote Connect Lab – Device Creation

- 1) Check the appropriate Group membership based on station number (EvenStations or OddStations)
 - Do not click on the EvenUsers or OddUsers
- 2) Click Next

__ _ _ _ _ .

SIEMENS	SINEMA Remote Connect									
Logged on as "station05"	Group membe	rs /								
Log off	Device	VPN connection mode	Network settings	Group memberships	Password	Device overview				
C Exit dialog	 EvenStations EvenUsers Back 	Dodds Oddu Next	Stations Jsers							

SIEMENS

Unrestricted © Siemens Industry, Inc. 2017 All rights reserved.
Lab – Device Creation

- 1) Enter and confirm password A. Admin!123
- 2) Click Next

Logged on as "station05"		New device					
Log off	3	Device	VPN connection mode	Network settings	Group memberships	Password	Device overview
Exit dialog		Name of the device: * New password: * Confirm password:	Station05_S615 Back	Next			

Unrestricted © Siemens Industry, Inc. 2017 All rights reserved.

Page 109



Lab – Device Creation

Confirm settings are correct 1)

Click Finish 2)

SINEMA Remote Connect Devices / Station05_S615 VPN connection mode Network settings Group memberships Password Device overview Device information: IP address of the VPN server 172.16.10.250 6 ß 192.168.10.225 IP address of the Web server 172.16.10.250 B 192.168.10.225 B Web server port 443 B Fingerprint: 8C:DD:54:0B:BC:2A:FB:03:1E:09:FB:71:4D:A2:94:19:3F:29:30:78 6 Name of the device: Station05_S615 Local LAN IP address: Local subnet Network gateway 192.168.1.1/24 Yes Virtual local LAN IP address: Virtual local LAN Local subnet Network gatewa 172.17.5.0/24 192.168.1.1/24 Device-specific virtual LAN: Virtual local LAN Local host Network gateway Type Vendo Location Type of connection: Permanent SMS gateway provider Comment Groups: OddStation

IPsec certificate:

Local ID:

VPN connection mode: OpenVPN IPsec profile: Request virtual IP address: Yes Fixed IP address

SIEMENS

O Exit dialog

 $\boldsymbol{\mathcal{C}}$

Device

ID of the partner

Back Finish

SINEMA Remote Connect Lab – Device Creation

1) Click on the information button

Logged on as "station05"		Devices										
Log off	C											
 Remote connections Devices Participant groups My account 		i no filter active Search filter: All	.		९ ि Prec	ise match Apply fil	ter	Show all				
		Name of the device	VPN address	\$	Remote subnet	Virtual local LAN	Status	Location	Type of connection	◆ VPN connection mode	Actions	
		Station05_S615	None		192.168.1.1/24	172.17.5.0/24	O offline		Permanent	OpenVPN	0 °° (요 속 # 봄 !!
		Create	Import	С	opy Dele	ete						

SIEMENS

SINEMA Remote Connect Lab – Device Creation

SIEMENS

1) Note the Device ID and Fingerprint

A. These are needed to set up the S615

	Logged on as "station05"		Devices / Station	n05_S615					
	Log off	3	Device	VPN connec	tion mode	Network settings	Group memberships	Change password	Device overview
	C Exit dialog		Device inform	ation:					
			Dev	ice ID: 17					
			IP address of the VPN	server 172.16	.10.250			6	
				192.16	8.10.225			6	
			IP address of the Web	server 172.16	.10.250			ß	
				192.16	8.10.225			6	
			Web serve	er port 443				6	
			Finge	erprint: 8C:DD	54:0B:BC:2A	:FB:03:1E:09:FB:71:4D:	:A2:94:19:3F:29:30:78	6	
			Name of the d	levice: Station	05_S615				
			Local LAN IP ad	dress: Local	subnet	Network gatewa	ау		
				192.16	8.1.1/24	Yes			
							N (1)	_	
			virtual local LAN IP ad	dress: Virtual		Local subnet	Network gates	vay	
Unrestricted © Siemens Industry, Inc. 2017 All ri				172.17	.5.0/24	192.168.1.1/24	Yes		

Lab – S615 Configuration - Fingerprint

- 1) SINEMA RC Address A. 172.16.10.250
- 2) SINEMA RC Port
 - A. 443
- 3) Verification Type
 - A. Fingerprint
- 4) Fingerprint
 - A. Enter noted fingerprint from SRC information page (recommend to copy and paste)
- 5) Device ID
 - A. Enter noted Device ID from SRC information page
- 6) Device Password
 - A. Password entered when configuring device in SRC
- 7) Leave Optional Settings as default
- 8) Click Set Values
- 9) Click Check Box to Enable SINEMA RC
- 10) Click Set Values



SIEMENS	192.168.1.1/SC	ALANCE S6	15
Welcome admin	SINEMA Remote Conn	ect (SINEMA RC)	
Logout			
►Wizards		Enable SINEMA RC	
Information		Server Settings	
▼System	SINEMA RC Address:		
▶Configuration	SINEMA RC Port:	443	
▶General			
▶Restart		Server Verification	
▶Load&Save	Verification Type:	Fingerprint	1
▶Events	Fingerprint:		
▶SMTP Client	CA Certificate:	-	
▶SNMP			
♦System Time		Device Credentials	
►Auto Logout	Device ID:	0	
►Syslog Client	Device Password:		
Fault Monitoring		Optional Settings	
Normoning		Auto Firewall/NAT Rules	s
> Pipe	Type of connection:	Auto 🔻	1
P Filig	Use Proxy:	none 🔻	1
NDHCP	Autoenrollment Interval [min]:	60	
boRSD/SRS			
Draw Sanar			
SINEMA RC	Set Values Refresh		
▶ Interfaces			
▶Layer 2			
▶Layer 3			
▶Security			

SINEMA Remote Connect Lab – S615 Configuration

Browse to Information > SINEMA RC 1)

Unrestricted © Siemens Industry, Inc. 2017 All rights reserved

2) Verify the Status is established

CIENCENC

SIEMENS		
	192.168.1.1/SCALANCE S615	
Welcome admin	SINEMA Remote Connect (SINEMA RC) Information	
Logout		
Logoat		1
Nizards	Status: established	
nformation	Remote Address: 172.16.10.250	
h Start Daga	Tunnel Interface Address: 10.8.1.2	
Versions	Connected Local Subnet(s): 192.168.1.0/24 translated to 172.17.5.0/24	
♦ARP Table	Connected Remote Subnet(s): 10.8.1.0/24	
Log Tables	10.8.0.0/24	
Faults	Figure tick 80:00:54:00:00:54:00:50:45:00:50:74:40:40:25:00:20:70	
▶DHCP Server	Fingerprint: 6C:DD:54:0B:BC:2A:FB:03:TE:09:FB:71:4D:A2:94:19:3F:29:30:76	
►LLDP		
▶Routing		
▶IPsec VPN	Refresh	
SINEMA RC		
▶OpenVPN Client		
System		
nterfaces		
Layer 2		
Layer 3		
Security		

SIEMENS

Page 114

SIEMENS

Lab – S615 Configuration - Certificate

- 1) Go back to SINEMA Remote Connect (log back in if necessary)
 - A. Click the key icon on the line of the device for the correct station.
 - B. Save file to Desktop

Logged on as "station05"		Devices								
Log off	3									
 Remote connections Devices Participant groups My account 		i no filter active Search filter: All	×	🥄 🗆 Pri	ecise match Apply fi	ilter Show	v all			
		Name of the device	VPN address	♣ Remote subnet	Virtual local LAN	Status	Location 🗘	Type of connection \$	VPN connection mode \$	Actions
		Station05_S615	None	192.168.1.1/24	172.17.5.0/24	O offline		Permanent	OpenVPN	ፀ « 凸 <mark>ዲ 🛊 볼</mark> II
		Create	Import	Сору De	elete					

Lab – S615 Configuration - Certificate

- 1) Log back in to the S615
- 2) Uncheck box next to Enable SINEMA RC
 A. SINEMA RC needs to be disabled to make modifications
- 3) Set Values

SIEMENS	192 168 1 1/SC	ALANCE S615
Walcomo admin	SINEMA Remote Conn	
Welcome admin	SINEWA Remote Com	ect (SINEWA RC)
Logout		
▶Wizards		Enable SINEMA RC
►Information		
▼System		Server Settings
Configuration	SINEMA RC Address:	142
Coniguration	SINEMA RC POIT:	443
Bestart		Server Verification
Prestant	Verification Type:	Eingerprint I
Loadosave	Fingerprint:	
▶ Events	CA Certificate:	
SMIP Client		
▶SNMP		Device Credentials
▶System Time	Device ID:	0
▶Auto Logout	Device Password:	
♦ Syslog Client		
Fault Monitoring		Optional Settings
▶PLUG		Auto Firewall/NAT Rules
▶Ping	Type of connection:	Auto
▶DNS	Use Proxy:	none
▶DHCP	Autoenrollment Interval [min]:	60
▶cRSP/SRS		
▶Proxy Server		
►SINEMA RC	SotValuos Pofrash	
	Set values Reliesn	
Interfaces		
▶Layer 2		
►Layer 3		
▶Security		

Lab – S615 Configuration - Certificate

- 1) Browse to System > Load&Save
- 2) Click on the Passwords tab
- 3) X509Cert
 - A. Enter the password used for the device and again in the confirmation space
 - B. Click the check box under Enabled
- 4) Click Set Values

SIEMENS

SIENIENS						
	192.168.1.	1/SCALANCE S	615			
Welcome admin	Passwords					
<u>Logout</u>		-				
▶ Wizards	HTTP TFTP Passwor	as	_	_		_
▶ Information	Туре	Description	Enabled	Password	Password Confirmation	Status
-Custan	HTTPSCert	HTTPS Certificate				-
▼System	X509Cert	X509 Certificates		•••••	•••••	-
Configuration	O-Dichard Defen	-				
General	Set values Refres	in				
▶ Restart						
▶ Load&Save						
Events						
SMIP Client						
Sinivip						
Auto Logout						
Svelog Client						
Fault Monitoring						
▶ PLUG						
▶Ping						
▶DNS						
▶DHCP						
▶cRSP/SRS						
▶ Proxy Server						
▶SINEMA RC						
▶ Interfaces						
Layer 2						
▶Layer 3						
▶ Security						

Unrestricted © Siemens Industry, Inc. 2017 All rights reserved.

Lab – S615 Configuration - Certificate

- Browse to System > Load&Save 1)
- Click on the HTTP tab 2)
- 3) X509Cert
 - A. Click Load
 - B. Select the file and click Open
 - C. Acknowledge that the File was successfully loaded

			WID .	SOALANOL MIMOPO MID
	Open File	×	RunningCLI	'show running-config all' CLI settings
📷 Home	Image: Market		StartupInfo	Startup Information
E Desktop	Name	✓ Size Modified	Users	Users and Passwords
Documents	E Station05_S615,p12	3.2 kB 16:30	X509Cert	X509 Certificates
Downloads				
📷 Music			Refresh	
Pictures				
Wideos				
Shared				
Other Locations				
				File was successful
		Cancel Open		
		Cancel Open		

SIEMENS

► Wiz

► Info

▼Sys

	152.100.1.	NOORLANCE SUIS				
Welcome admin	Load and Save v	ia HTTP				
Logout						
Nizards	HTTP TFTP Password	8				
nformation	Туре	Description	Load	Save	Delete	
	Config	Startup Configuration	Load	Save		
System	ConfigPack	Startup Config, Users and Certificates	Load	Save		
▶Configuration	Debug	Debug Information for Siemens Support		Save	Delete	
▶General	Firmware	Firmware Update	Load	Save		
▶Restart	HTTPSCert	HTTPS Certificate	Load	Save	Delete	
N oad & Save	LogFile	Event, Security, Firewall Logs		Save		
Loadosave	MIB	SCALANCE M MSPS MIB		Save		
×	RunningCLI	'show running-config all' CLI settings		Save		
	StartupInfo	Startup Information		Save		
ze Modified	Users	Users and Passwords	Load	Save		
2 kB 16:30	X509Cert	X509 Certificates	Load	Save		

102 168 1 1/SCALANCE S615



Lab – S615 Configuration - Certificate

- 1) Browse to Security > Certificates
- 2) Verify the Certificates Exist
 - Note the certificates all have a .pem extension

SIEMENS

	192.1	168.1.1/	SCALANCE S	615					
Welcome admin	Certifica	ates Overvie	ew						
Logout									
▶Wizards	Overview	Certificates							
►Information	Select	Туре	Filename	State	Subject DN	Issuer DN	Issue Date	Expiry Date	Used
▶System		Machine Cert	Station05 S615 Cert.pem	valid	CN=Station05_S615@P.1	CN=CA 000001 SINEMA RC	09/25/2017 16:50:58	09/27/2018 16:50:58	-
Interfaces		CA Cert	Station05 S615 CACert.pem	valid	CN=CA 000001 SINEMA RC	CN=CA 000001 SINEMA RC	09/18/2017 21:27:13	09/18/2027 21:27:13	-
▶Layer 2		Key File	Station05 S615 Key.pem	valid	CN=Station05_S615@P.1	CN=CA 000001 SINEMA RC	09/25/2017 16:50:58	09/27/2018 16:50:58	-
▶Layer 3	3 entries	3.							
-Security	Delete	Refresh							
▶Users									
▶Passwords									
► Certificates									
▶Firewall									
▶IPsec VPN									
♦ OpenVPN Client									

Unrestricted © Siemens Industry, Inc. 2017 All rights reserved.

Lab – S615 Configuration - Certificate

- 1) SINEMA RC Address A. 172.16.10.250
- 2) SINEMA RC Port
 - A. 443
- 3) Verification Type
 - A. CA Certificate
- 4) CA Certificate
 - A. certificate file (*.pem) in the dropdown (there should only be one file available for selection)
- 5) Device ID
 - A. Enter noted Device ID from SRC information page
- 6) Device Password
 - A. Password entered when configuring device in SRC
- 7) Leave Optional Settings as default
- 8) Click Set Values
- 9) Click Check Box to Enable SINEMA RC
- 10) Click Set Values

	and the second s	
Welcome admin	SINEMA Remote Conn	ect (SINEMA RC)
Logout		
Wizards		Enable SINEMA RC
Information		
		Server Settings
rSystem	SINEMA RC Address:	172.16.10.250
►Configuration	SINEMA RC Port:	443
▶General		
▶ Restart		Server Verification
▶Load&Save	Verification Type:	CA Certificate
▶Events	Fingerprint:	8C:DD:54:0B:BC:2A:FB:0
▶SMTP Client	CA Certificate:	Station05_S615_CACer
▶SNMP		
▶System Time		Device Credentials
►Auto Logout	Device ID:	17
►Syslog Client	Device Password:	
Fault Monitoring		Optional Settings
▶ PLUG		Auto Firewall/NAT Rule
▶ Ping	Type of connection:	Auto
▶DNS	Use Proxy:	none
▶DHCP	Autoenroliment Interval [min]:	60
▶cRSP / SRS		
Proxy Server		
SINEMA RC		
	Set Values Refresh	
Interfaces		
Layer 2		
Laver 3		
Layer 3		

▶ Security

SINEMA Remote Connect Lab – S615 Configuration

- 1) Browse to Information > SINEMA RC
- 2) Verify the Status is established

SIEMENS

192.168.1.1/SCALANCE S615 SINEMA Remote Connect (SINEMA RC) Information Welcome admin Logout ▶Wizards Status: established Remote Address: 172.16.10.250 ◄Information Tunnel Interface Address: 10.8.1.2 In Start Page Connected Local Subnet(s): 192.168.1.0/24 translated to 172.17.5.0/24 ►Versions ►ARP Table Connected Remote Subnet(s): 10.8.1.0/24 10.8.0.0/24 Log Tables 172.32.0.0/16 ▶Faults Fingerprint: -▶DHCP Server **▶LLDP** ▶Routing IPsec VPN Refresh ►SINEMA RC ▶OpenVPN Client ▶System ▶Interfaces Layer 2 Layer 3 ▶Security

SIEMENS



Thank you for attending!

Help us to better serve you! Please take a moment for our survey.

Add Survey Monkey Link and QR code to follow

SIEMENS

Rick Kluth



Rick Kluth Network Solutions Consultant

Murfreesboro, TN USA

Phone (919) 600-3029

Email: richard.kluth@siemens.com

Answers for industry.

SIEMENS

Patric Dove



Patric Dove Network Solutions Consultant

8850 Fallbrook Dr Houston, TX 77064

Phone (713) 855-7491

Email: patric.dove@siemens.com

Answers for industry.