PBS 09

mgr inż. Roman Krzeszewski roman@kis.p.lodz.pl

mgr inż. Artur Sierszeń asiersz@kis.p.lodz.pl

mgr inż. Łukasz Sturgulewski luk@kis.p.lodz.pl

Wykład 09

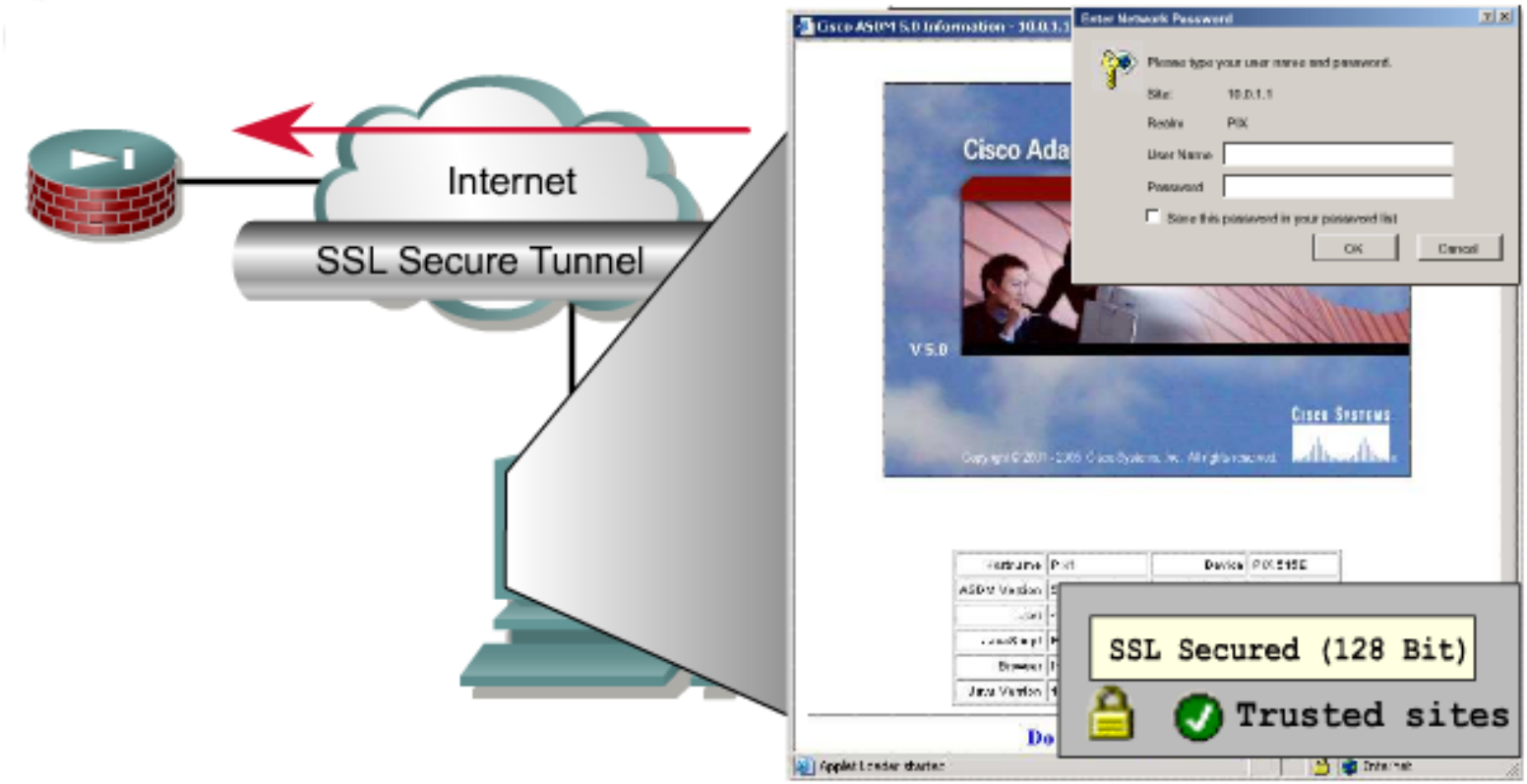
- **ASDM –**
  Adaptive Security Device Manager
  (pix)

- **HTTP Device Manager**
  (switch)

ASDM – Adaptive Security Device Manager

- **Adaptive Security Device Manager** (ASDM) jest narzędziem, bazującym na przeglądarce www, pozwalającym administratorowi na konfigurację i monitorowanie pracy PIX lub ASA za pomocą interfejsu graficznego bez znajomości linii poleceń.

ASDM


Internet
SSL Secure Tunnel
Enter Network Password
Please type your user name and password.
Site: 10.0.1.1
Realm PIX
User Name
Password
Store this password in your password list
OK
Cancel
Cisco Ada
V 5.0
Cisco Systems
SSL Secured (128 Bit)
Trusted sites

Konfiguracja ASDM na PIX

- Włączenie ASDM:
  - **PIX(config)# http server enable**
- IP hosta i nazwa interfejsu, z którego będzie możliwy dostęp do ASDM:
  - **PIX(config)# http *ip_address netmask if_name***
- Nazwa PIX'a i nazwa domeny, w której się znajduje:
  - **PIX(config)# hostname *name***
  - **PIX(config)# domain-name *name***
- Autoryzacja użytkownika z serwera RADIUS:
  - **PIX(config)# aaa authentication http console *MYRADIUS***

Uruchomienie ASDM

- **Stacja robocza:**
  - Zainstalowana Java w wersji min. 1.4.2.
  - Przeglądarka obsługująca SSL.
  - Wyłączone blokowanie „wyskakujących okienek”.
- **Uruchamianie ASDM:**
  - https://10.2.0.1
  - [Run ASDM Applet]

Cisco ASDM 5.2 for ASA - 10.2.0.1

File Options Tools Wizards Help Search: Find

Home | Configuration | Monitoring | Back | Forward | Packet Tracer | Refresh | Save | Help

ASA Main System | Intrusion Prevention

Device Information

General | License

Host Name:	ZiMSK-PIX.test.com		
ASA Version:	7.2(3)	Device Uptime:	0d 5h 36m 20s
ASDM Version:	5.2(3)	Device Type:	ASA 5510
Firewall Mode:	Routed	Context Mode:	Single
Total Flash:	256 MB	Total Memory:	256 MB

Interface Status

Interface	IP Address/Mask	Line	Link	Kbps
dmz	176.16.0.1/16	up	up	0
inside-ADMIN	10.1.0.1/16	up	up	0
inside-DYR	10.10.0.1/16	up	up	0
inside-PRAC	10.20.0.1/16	up	up	0
inside-SERWERY	10.2.0.1/16	up	up	105

Select an interface to view input and output Kbps

VPN Tunnels

IKE: 0 IPSec: 0 WebVPN: 0 SVC: 0

System Resources Status

CPU — 19% — 17:56:38

CPU Usage (percent) — 100, 50, 0 — 17:56:38

Memory — 53MB — 17:56:38

Memory Usage (MB) — 234, 117, 0 — 17:56:38

Traffic Status

Connections Per Second Usage — 2, 1, 0 — 17:56:38

UDP: 0 TCP: 0 Total: 0

'outside' Interface Traffic Usage (Kbps) — 2, 1, 0 — 17:56:38

Real time 'outside' Interface Traffic Usage (Kbps), refreshed every 10 seconds

Input Kbps: 0 Output Kbps: 0

Latest ASDM Syslog Messages — Configure ASDM Syslog Filters

ASDM logging is disabled. To enable ASDM logging with informational level, click the button below.

Enable Logging

Device configuration loaded successfully. | rad | 15 | 04.01.08 17:56:38 UTC

Cisco ASDM 5.2 for ASA - 10.2.0.1

File Options Tools Wizards Help Search: Find

Home | Configuration | Monitoring | Back | Forward | Packet Tracer | Refresh | Save | Help

Interfaces | Security Policy | NAT | VPN | IPS | CSD Manager | Routing | Global Objects | Properties

Configuration > Interfaces

Interface	Name	Enabled	Security Level	IP Address	Subnet Mask	VLAN	Management Only	MTU
Ethernet0/0		Yes				native	No	
Ethernet0/0.1	inside-ADMIN	Yes	100	10.1.0.1	255.255.0.0	vlan1	No	1 500
Ethernet0/0.2	inside-SERWERY	Yes	95	10.2.0.1	255.255.0.0	vlan2	No	1 500
Ethernet0/0.10	inside-DYR	Yes	90	10.10.0.1	255.255.0.0	vlan10	No	1 500
Ethernet0/0.20	inside-PRAC	Yes	80	10.20.0.1	255.255.0.0	vlan20	No	1 500
Ethernet0/1	dmz	Yes	50	176.16.0.1	255.255.0.0	native	No	1 500
Ethernet0/2	outside	Yes	0	192.168.1.1	255.255.255.0	native	No	1 500
Ethernet0/3		No				native	No	
Management0/0		No				native	No	

Add | Edit | Delete

☐ Enable traffic between two or more interfaces which are configured with same security levels

☐ Enable traffic between two or more hosts connected to the same interface

Apply | Reset

rad 15 04.01.08 17:58:48 UTC

Cisco ASDM 5.2 for ASA - 10.2.0.1

File Options Tools Wizards Help Search: Find

Home | Configuration | Monitoring | Back | Forward | Packet Tracer | Refresh | Save | Help

Interfaces
Security Policy
NAT
VPN
IPS
CSD Manager
Routing
Global Objects
Properties

Configuration > Security Policy > Access Rules

Access Rules | AAA Rules | Filter Rules | Service Policy Rules

Add | Edit | Delete | Find | Rule Diagram | Show Log | Packet Tra

Filter: --Select-- | Filter | Clear | Rule Query...

No	Enab...	Source	Destination	Service	Action	Log
inside-DYR (2 implicit incoming rules)						
1		any	Any less secure net...	ip	Permit	
2		any	any	ip	Deny	
inside-PRAC (5 incoming rules)						
1	✓	any	dmz-network/16	ftp	Permit	
2	✓	any	any	http	Permit	
3	✓	any	any	any	Deny	
4	✓	any	any	ip	Deny	
5		any	any	ip	Deny	
inside-SERWERY (2 implicit incoming rules)						
1		any	Any less secure net...	ip	Permit	
2		any	any	ip	Deny	
outside (4 incoming rules)						
1	✓	any	192.168.1.80	8080	Permit	
2	✓	any	192.168.1.80	2121	Permit	
3	✓	any	any	echo-reply	Permit	
4		any	any	ip	Deny	

Rule Flow Diagram

Source Address — Service — Action — Destination Address

Addresses | Services | Time Ranges

Add | Edit | Delete | Fir

Type: All

Name

- IP Address Objects
  - any
  - inside-ADMIN-network/16
  - inside-SERWERY-networ...
  - inside-DYR-network/16
  - inside-PRAC-network/16
  - dmz-network/16
  - 176.16.0.9
  - outside-network/24
  - 192.168.1.80

Apply | Reset | Advanced...

rad | 15 | 04.01.08 18:00:28 UTC

Cisco ASDM 5.2 for ASA - 10.2.0.1

File Options Tools Wizards Help Search: Find

Home | Configuration | Monitoring | Back | Forward | Packet Tracer | Refresh | Save | Help

Interfaces
Security Policy
NAT
VPN
IPS
CSD Manager
Routing
Global Objects
Properties

Configuration > NAT

Add Edit Delete Find Rule Diagram Packet Trace

Filter: --Select-- Filter Clear Rule Query...

No	Type	Real Source	Real Destination	Translated Interface	Translated Address
dmz					
1	Static	176.16.0.9 TCP http	any	outside	192.168.1.80 TCP 8080
2	Static	176.16.0.9 TCP ftp	any	outside	192.168.1.80 TCP 2121
3	Dynamic	any	any	outside	192.168.1.50
inside-DYR					
1	Dynamic	any	any	dmz	176.16.0.10
2				outside	192.168.1.10
inside-PRAC					
1	Dynamic	any	any	dmz	176.16.0.20
2				outside	192.168.1.20

Rule Flow Diagram

Source Address — NAT Type — Destination Address

Addresses | Services | Global Pools

Add Edit Delete Find

Type: All

Name

- IP Address Objects
  - any
  - inside-ADMIN-network/16
  - inside-SERVERY-network...
  - inside-DYR-network/16
  - inside-PRAC-network/16
  - dmz-network/16
  - 176.16.0.9
  - outside-network/24
  - 192.168.1.80

Enable traffic through the firewall without address translation

Apply Reset

rad 15 04.01.08 17:57:38 UTC

Cisco ASDM 5.2 for ASA - 10.2.0.1

File Options Tools Wizards Help Search: Find

Home Configuration Monitoring Back Forward Packet Tracer Refresh Save Help

Interfaces
VPN
IPS
Routing
Properties
Logging

Monitoring > Routing > Routing > Routes

- Routing
  - OSPF LSAs
    - Type 1
    - Type 2
    - Type 3
    - Type 4
    - Type 5
    - Type 7
  - OSPF Neighbors
  - Routes

Routes

Each row represents one route. AD is the administrative distance.

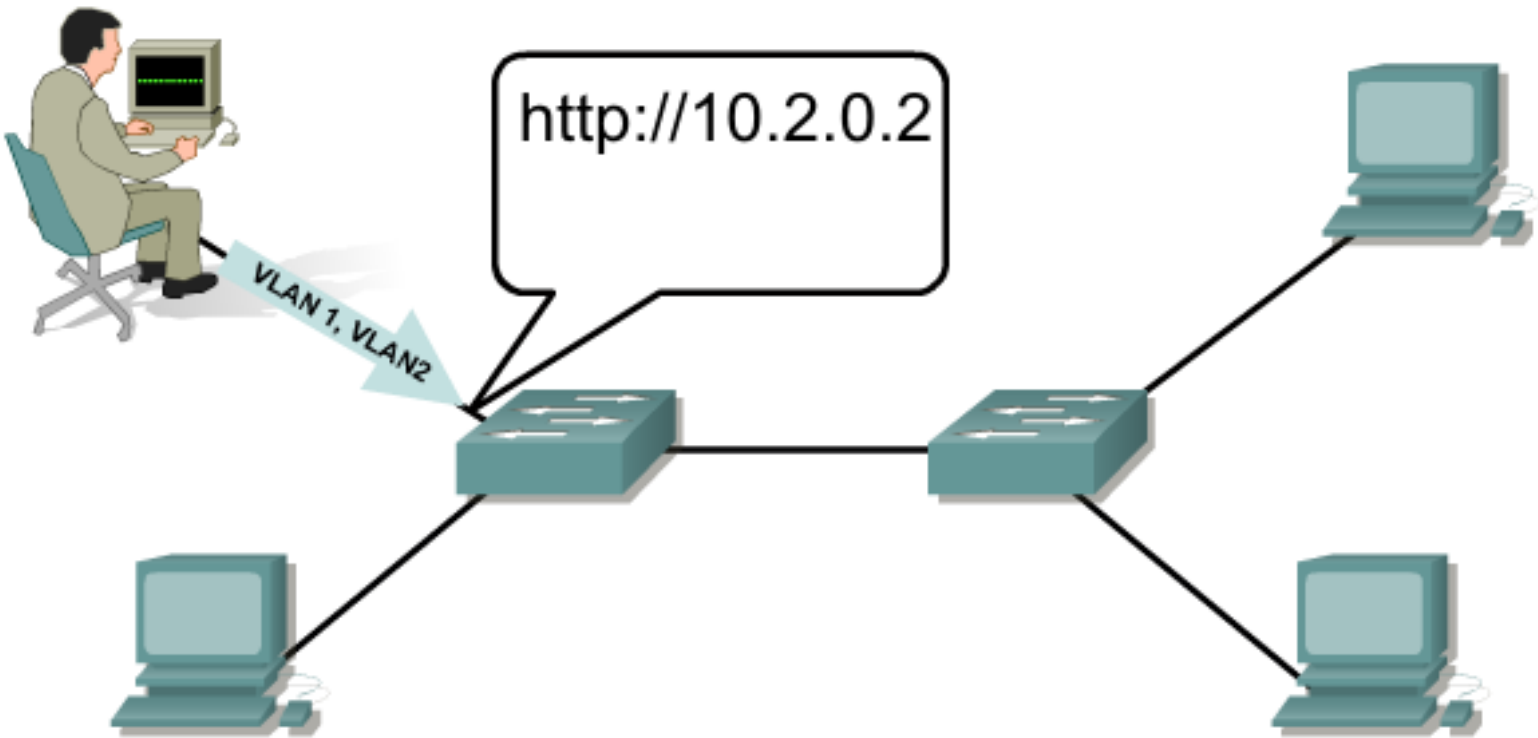
Protocol	Type	Destination IP	Netmask	Gateway	Interfac
CONNECTED	C	10.10.0.0	255.255.0.0	-	inside-D
CONNECTED	C	10.2.0.0	255.255.0.0	-	inside-S
CONNECTED	C	10.1.0.0	255.255.0.0	-	inside-A
CONNECTED	C	10.20.0.0	255.255.0.0	-	inside-Pl
CONNECTED	C	176.16.0.0	255.255.0.0	-	dmz
CONNECTED	C	192.168.1.0	255.255.255.0	-	outside
STATIC	S* DEFAULT	0.0.0.0	0.0.0.0	192.168.1.2	outside

Refresh

Last Updated: 04.01.08 16:16:40

Data Refreshed Successfully. rad 15 04.01.08 17:58:28 UTC

HTTP Device Manager



Konfiguracja HTTP Device Manager

- Włączenie HTTP Device Manager:
  - **Switch(config)# ip http server**
- Konfiguracja hasła na tryb #:
  - **Switch(config)# enable secret level 15 *pass***
- Do autoryzacji w HTTP Device Manager wymagane będzie hasło na tryb #:
  - **Switch(config)# ip http authentication enable**

10.10.1.2 : Cisco Device Manager - Windows Internet Explorer

http://10.10.1.2/xhome.htm

10.10.1.2 : Cisco Device Manager

Catalyst 2950 Series Device Manager - Switch

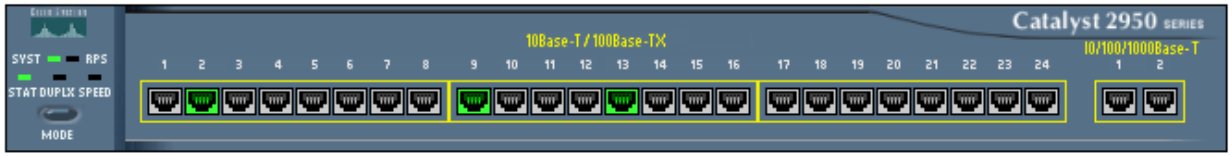
Refresh | Print | Smartports | Legend | Help

Cisco Systems

Uptime: 55 minutes

Next refresh in **57** seconds

View : Status



Move the pointer over the ports for more information

Contents

- Dashboard
- Monitor
- Configuration
- Tools
- Network Assistant

Dashboard

Switch Information

Host Name:	Switch
Type:	WS-C2950T-24
IP Address:	10.10.1.2
MAC Address:	00:12:DA:B7:E6:40
Serial Number:	FOC0851W1KY
Software:	12.1(22)EA1b
Contact:	
Location:	

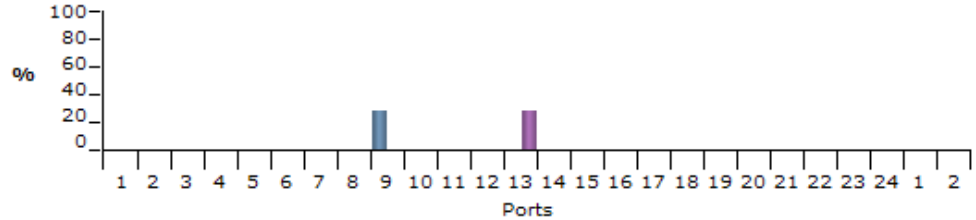
Switch Health

View Trends

Bandwidth Used	Packet Error	Fan
0%	0%	OK

Port Utilization

View Trends | View Port Statistics



Legend: Receive Transmit

Done | Internet | 100%

10.10.1.2 : Cisco Device Manager - Windows Internet Explorer

http://10.10.1.2/xhome.htm

10.10.1.2 : Cisco Device Manager

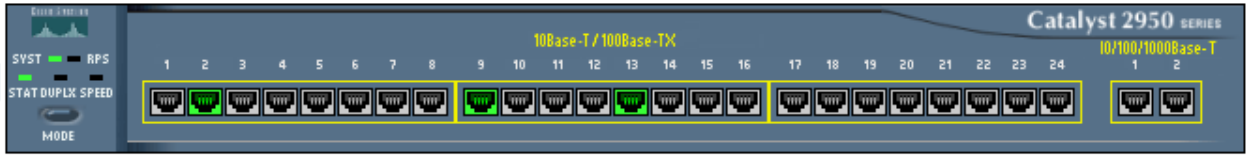
Catalyst 2950 Series Device Manager - Switch

Refresh | Print | Smartports | Legend | Help

Uptime: 58 minutes

Next refresh in **39** seconds

View : Status



Move the pointer over the ports for more information

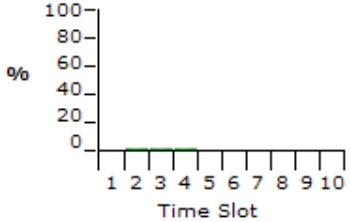
Contents

- Dashboard
- Monitor
  - Trends
  - Port Status
  - Port Statistics
- Configuration
- Tools
- Network Assistant

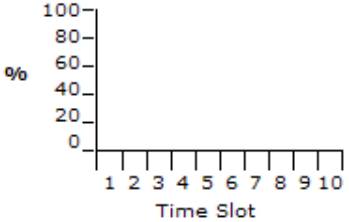
Trends

Switch Health

Bandwidth Utilization: 1%



Packet Error: 0%

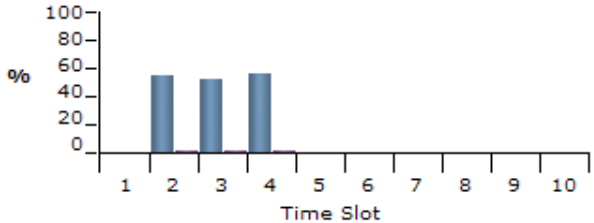


Port Utilization

View Port Statistics

Connected Port: Fa0/9

Receive Utilization: 56% Transmit Utilization: 1%



Legend: Receive Transmit

Done | Internet | 100%

10.10.1.2 : Cisco Device Manager - Windows Internet Explorer

http://10.10.1.2/xhome.htm

Live Search

10.10.1.2 : Cisco Device Manager

Page Tools

Catalyst 2950 Series Device Manager - Switch

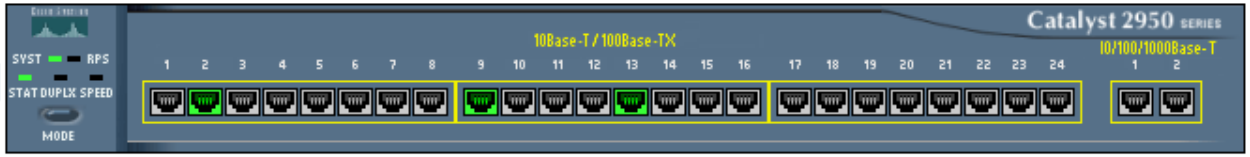
Refresh Print Smartports Legend Help

Cisco Systems

Uptime: 58 minutes

Next refresh in **16** seconds

View : Status



Move the pointer over the ports for more information

Contents

- Dashboard
- Monitor
  - Trends
  - Port Status
  - Port Statistics
- Configuration
- Tools
- Network Assistant

Port Status

Port	Description	Status	VLAN	Speed	Duplex
Fa0/2			1	100	full
Fa0/3			1		
Fa0/4			1		
Fa0/5			1		
Fa0/6			1		
Fa0/7			1		
Fa0/8			1		
Fa0/9			1	100	full
Fa0/10			1		
Fa0/11			1		
Fa0/12			1		
Fa0/13			1	100	full

Done Internet 100%

10.10.1.2 : Cisco Device Manager - Windows Internet Explorer

http://10.10.1.2/xhome.htm

10.10.1.2 : Cisco Device Manager

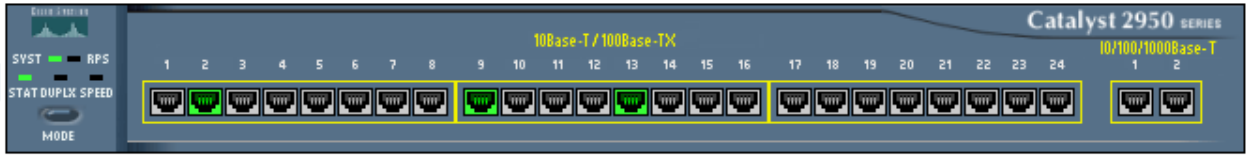
Catalyst 2950 Series Device Manager - Switch

Refresh | Print | Smartports | Legend | Help

Uptime: 59 minutes

Next refresh in **2** seconds

View : Status



Move the pointer over the ports for more information

Contents

- Dashbo
- Monitor
  - Tren
  - Port
  - Port
- Configu
- Tools
- Networ

Port Statistics

Overview | Transmit Detail | Receive Detail

	Port	Transmitted (bytes)	Total Transmitted (pkts)	Received (bytes)	Total Received (pkts)	Total Transmit Errors (pkts)	Total Receive Errors (pkts)
	Fa0/8	64	1	64	1	0	0
	Fa0/9	25531589	398835	1658180430	1542074	0	0
	Fa0/10	64	1	64	1	0	0
	Fa0/11	64	1	64	1	0	0
	Fa0/12	64	1	64	1	0	0
	Fa0/13	1658308456	1545385	25402071	395493	0	0

Clear Counters | Cancel

Done | Internet | 100%

10.10.1.2 : Cisco Device Manager - Windows Internet Explorer

http://10.10.1.2/xhome.htm

10.10.1.2 : Cisco Device Manager

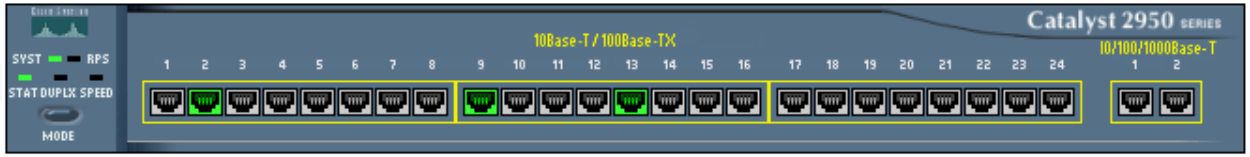
Catalyst 2950 Series Device Manager - Switch

Refresh | Print | Smartports | Legend | Help

Uptime: 1 hour, 3 minutes

Next refresh in **46** seconds

View : Status



Move the pointer over the ports for more information

Contents

- Dashboard
- Monitor
  - Trends
  - Port Status
  - Port Statistics
- Configuration
  - Smartports
  - Port Settings
  - Express Setup
  - Restart / Reset
- Tools
- Network Assistant

Port Settings

Port	Description	Enabled	Speed	Duplex
Fa0/1		☑	Auto	Auto
Fa0/2		☑	Auto	Auto
Fa0/3		☑	Auto	Auto
Fa0/4		☑	Auto	Auto
Fa0/5		☑	Auto	Auto
Fa0/6		☑	Auto	Auto
Fa0/7		☑	Auto	Auto

Submit | Cancel

Done | Internet | 100%

10.10.1.2 : Cisco Device Manager - Windows Internet Explorer

http://10.10.1.2/xhome.htm

10.10.1.2 : Cisco Device Manager

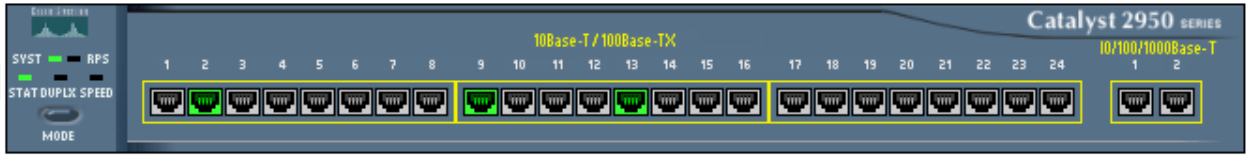
Catalyst 2950 Series Device Manager - Switch

Refresh | Print | Smartports | Legend | Help

Uptime: 1 hour, 3 minutes

Next refresh in **11** seconds

View : Status



Move the pointer over the ports for more information

Contents

- Dashboard
- Monitor
  - Trends
  - Port Status
  - Port Statistics
- Configuration
  - Smartports
  - Port Settings
  - Express Setup
  - Restart / Reset
- Tools
- Network Assistant

Network Settings

Management Interface (VLAN ID): 1

IP Address: 10 . 10 . 1 . 2 Subnet Mask: 255.255.255.0

Default Gateway: . . .

Switch Password: ••••• Confirm Switch Password:

Optional Settings

Host Name: Switch

System Contact: System Location:

Telnet Access: ○ Enable ◉ Disable

Telnet Password: Confirm Telnet Password:

Submit | Cancel

Done | Internet | 100%

Wykład HTTP Manager

KONIEC