

Catalyst Secure Template

Version 1.21, 11/14/2002

Stephen Gill
E-mail: gillsr@cymru.com
Published: 11/01/2002

Contents

Introduction	2
Topology	3
Design Principles	4
Interfaces	5
Ports	5
Default	5
Trunking	5
ARP Spoof Prevention	6
VLANs	8
VTP	9
Services	9
Disabled	9
Enabled	9
System Settings	10
Logins and Passwords	10
Authentication	10
System Time	11
Time Zone	11
NTP	11
Management	11
MOTD Banner	11
Console Access	12
SNMP Access	12
Remote Access	12
Logging and Exceptions	13
Conclusion	13
References	14
Further Reading	14
Appendix A	15

Introduction

In keeping with the theme of developing security strategies for critical pieces of network infrastructure [1], we present a brief treatise on hardening Cisco switches. Switches are often critical components that can serve several purposes in a given network including network segmentation, link aggregation, port monitoring, and more. Here we attempt to minimize the risk of network misuse by securing the Cisco switch using similar techniques to hardening Cisco routers.

Topology

Before delving into the details of our recommended hardening measures, we present a topology diagram on which the configuration details are based.

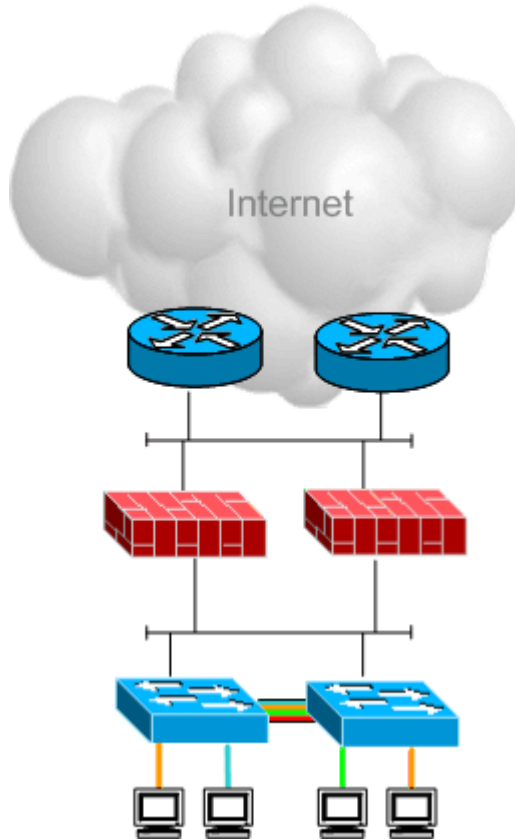


Figure 1 - Catalyst Topology

As packets enter the network they must pass through two intermediate layer 3 hops before making it to one of the servers. The switches are responsible for determining which of the three VLANs packets should be forwarded to based on port assignments and MAC address learning.

The switches in use in this topology are IOS based 2924 series XL, not CatOS based. The switches are small but most of the concepts included within this paper can be ported to other platforms and code versions quite easily. We leave it as an exercise to the reader to do so if necessary. Following is a brief outline of the ports and their assignments:

Table 1 - Switch Port Assignments

Port	VLAN	Description
1	2	Red

Port	VLAN	Description
2	2	Red
3	2	Red
4	3	Orange
5	3	Orange
6	3	Orange
7	4	Blue
8	4	Blue
9	4	Blue
10	5	Green
11	5	Green
12	5	Green
13	1	Disabled
14	1	Disabled
15	1	Disabled
16	1	Disabled
17	1	Disabled
18	1	Disabled
19	1	Disabled
20	1	Disabled
21	1	Disabled
22	10	Management access to switch
23	999:2-5	Trunk to other 2948XL. Native VLAN 999
24	999:2-5	Trunk to other 2948XL. Native VLAN 999

For information on securing other switch platforms, please reference the appendix.

Design Principles

Certain design principles are more straightforward than others when it comes to securing switched networks. Switches are not built for security and it is up to the administrator to ensure that the infrastructure cannot be easily defeated to compromise the network or data within. One of the simplest methods of network segmentation is to employ the use of VLANs for broadcast domain separation. VLAN assignments usually mirror IP subnets in that the broadcast domains are equal to one another. However, an interesting somewhat new method of securing intra-VLAN and intra-subnet traffic is to use Private VLANs.

Private VLANs are only available on certain platforms, but they allow the administrator to divide a single IP subnet into several broadcast domains to increase security. Essentially Private VLANs isolate traffic into multiple distinct broadcast domains within a single VLAN and IP subnet. Communication between VLANs can be isolated on a per port or per VLAN basis. These are known as isolated and community VLANs respectively.

Private VLANs are an excellent way of reducing the amount of traffic that any port can see within an IP subnet. Unfortunately administrators cannot

rely on switches to restrict frame forwarding because it is very easy to spoof ARP messages and cause all or selective traffic within a VLAN to be received by an attacker if he is directly connected to the switch. Dsniff was written specifically for the purpose of switch sniffing. [2]

Eliminating the possibility of switch sniffing requires some foresight and planning. Following is a quick checklist of items to reduce this possibility along with other malicious switch activity:

- Disable unused ports and unused services
- Filter BPDUs on end stations
- Disable trunk negotiation and CDP on end stations
- Enable port security and disable ports that violate a 1 MAC limit
- Secure router and firewall MAC addresses and disable ports that spoof them
- Secure switch management access
- Use private VLANs to reduce end station visibility.

Interfaces

Ports

Securing switch ports can be tedious work but sometimes necessary. Following are some guidelines for securing these interfaces including standard, trunk, and ARP spoof mitigation settings.

Default

In an ideal world, unused ports should be disabled to reduce the chances of port misuse. Additionally, unless otherwise required, active ports should have Cisco Discovery Protocol (CDP), trunking, and spanning tree explicitly disabled. By the same token, to avoid spanning-tree attacks, bpdudfilter should be enabled on ports that do not wish to send or receive BPDUs. Settings may vary depending on switch platform and code version.

```
interface FastEthernet0/1
  no ip address
  no cdp enable
  switchport mode access
  switchport nonegotiate
  shutdown
  spanning-tree portfast
  spanning-tree bpdudfilter enable
!
```

The 'switchport host' command has the effect of setting several of the parameters above automatically.

Trunking

When trunking is necessary, a dedicated VLAN other than VLAN 1 should be used to avoid the possibility of VLAN hopping and double tagged

802.1q attacks. Avoiding the use of VLAN 1 all together will keep it from being used in access mode on any non-trunked ports. The native VLAN number selected should not be used for any other purposes other than for VLAN trunking. The native VLAN should also be the same on both ends of the trunk. The VLANs allowed to traverse the trunk should be restricted to only those that are necessary both for performance and for security reasons.

```
interface FastEthernet0/23
  description Trunk Port
  no ip address
  no cdp enable
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk native vlan 999
  switchport trunk allowed vlan 2-10,1002-1005
  no shutdown
!

interface FastEthernet0/24
  description Trunk Port
  no ip address
  no cdp enable
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk native vlan 999
  switchport trunk allowed vlan 2-10,1002-1005
  no shutdown
!
```

The default method of frame distribution in redundant channel links is by MAC address. Wherever channels are configured it is advisable to use source and destination IP frame distribution instead. This will increase the likelihood of equal frame distribution. It is possible that if MAC distribution is enabled, while two primary gateways are forwarding traffic through one another, all traffic could traverse the same physical link because their MAC addresses are not changing. Unfortunately in this code version we only have the option of choosing source or destination but not both.

Ports 23 and 24 are joined into a channel group and are treated as one logical port.

```
interface FastEthernet0/23
  port group 1 distribution destination
!

interface FastEthernet0/24
  port group 1 distribution destination
!
```

ARP Spoof Prevention

MAC Limiting

One method of reducing the possibility of MAC address spoofing is to limit the number of addresses that are allowed to be received on a switch port at any given time. Below, only one MAC address is allowed to be on a

port at once. If this number is exceeded before the previous MAC address is aged out (default of 5 minutes), then the port in question will be automatically shutdown awaiting manual intervention. Mac aging time can be tuned with the 'mac aging-time <time>' command.

```
interface FastEthernet0/1
  port security
  port security max-mac-count 1
  port security action shutdown
!
```

MAC Hardcoding

As if that weren't enough, it may also be advisable to secure ports associated with key devices such as routers and firewalls by hard coding their MAC addresses into the switch configuration. This way, any port that tries to usurp the secured MAC address will also be disabled as a security violation.

```
mac-address-table secure AAAA.BBBB.CCCC fastethernet 0/1
mac-address-table secure AAAA.BBBB.CCCC fastethernet 0/2
```

As stated previously, private VLANs offer some level of protection but it is felt that the methods used above are sufficiently restrictive to reduce the need for intra-VLAN separation.

Multicast

If the firewalls in this topology were running HSRP (IE, Cisco routers with firewall IOS), then one could restrict all HSRP traffic (224.0.0.2) to only be sent to a specific set of known router ports. Instead of using the "secure" directive, "static" entries can be defined for multicast MAC addresses as follows:

```
mac-address-table static 0000.5E00.0002 fastethernet 0/1
mac-address-table static 0000.5E00.0002 fastethernet 0/2
```

The multicast MAC address [0000.5E00.0002] translates to the all-routers IP address 224.0.0.2. The effectiveness of restricting HSRP traffic to router ports relies on the ability to disable CGMP and / or IGMP snooping on the switch. If multicast groups are required disabling these may not be a viable option. Keep in mind that disabling CGMP may also have adverse effects in certain topologies by requiring multicast traffic to be broadcast to all ports within a broadcast domain instead of to the required subset.

```
no cgmp
```

Sticky MACs

For those who are perhaps more willing to deal with a higher administrative burden, you can also configure switch ports to convert

dynamically learned MAC addresses to sticky MAC addresses and subsequently add them to the running configuration. This will prevent users from staying within the single MAC limit by changing their MAC address to match that of another device on the local LAN segment. The secure MAC and the MAC limits above should protect against most methods of ARP spoofing, but will not protect from instances where users change their address to match that of another station. It will also not protect someone from ARP cache poisoning unless the switch has the ability to validate ARP to IP correlations.

The following command will convert all dynamic MAC addresses to sticky secure MAC addresses.

```
switchport port-security mac-address sticky
```

All sticky secure MAC addresses will be added to the running configuration but will not become part of the startup configuration file unless you save them. Saving them in the startup configuration has the added benefit of not having to relearn MAC entries upon switch reboot.

VLANS

Often administrators are tempted with the use of VLAN 1 as the primary management VLAN. This is the Cisco default VLAN and is used to house unassigned ports. However, it is generally recommended that VLAN 1 not be used. Instead, all management traffic should be moved to a separate VLAN such as VLAN 2, leaving all unassigned ports in the default VLAN. Unassigned and inactive ports should remain outside the management VLAN to reduce the risk of unauthorized access. For additional security, unassigned ports can be disabled as well, but placing them in an unused VLAN has a similar effect at a reduced management cost.

It is a great idea to establish a VLAN standard with names and numbers whereby VLANs serve the same purpose regardless of location. Once a standard is defined, descriptions should be added to each of the VLANs to describe their purpose. Here we create VLAN 10, assign it an IP address and make it the management VLAN.

```
interface VLAN10
 ip address 10.0.1.10 255.255.255.0
 description Management VLAN
 management
 no ip directed-broadcast
 no ip route-cache
!
```

Switches use VLAN 1 as the default VLAN for most things including Native trunking VLAN and management. It is a good idea to avoid the use of VLAN 1 all together.

```
interface VLAN1
  description Never use
  shutdown
!
```

VTP

VLAN trunking protocol (VTP) is an automated method of distributing VLAN configuration information throughout a management domain. The use of this tool can be quite harmful if a reassigned switch that houses a newer VTP database number is installed in a management domain while in server mode. All switches that are running VTP could potentially lose their VLAN information if much caution isn't observed when first installing a new switch. Unless there is a great need for this service, we recommend disabling VTP to reduce the risk of configuration loss. Cost benefit ratio seem to be justified here.

```
vtp mode transparent
```

MD5 authentication should be used if VTP is absolutely necessary.

```
vtp password <password>
```

Services

Disabled

Certain system services are not necessary and should be disabled by default. The finger service and UDP and TCP small servers fall well within this category.

```
no service finger
no service tcp-small-servers
no service udp-small-servers
```

CDP may or may not be required in your network environment. In this topology we have chosen to disable CDP individually on every port and globally on the switch as well for good measure.

```
no cdp advertise-v2
no cdp run
```

Enabled

In contrast, other services are often helpful such as those listed below.

```
! encrypt passwords with MD5
service password-encryption
service nagle
service tcp-keepalives-in
service tcp-keepalives-out
! log significant VTY-Async events
service pt-vty-logging
```

System Settings

Settings that aren't quite classified as system services are often lumped into the IP category. Following are some IP settings that should generally be disabled.

```
no ip domain-lookup
no ip finger
no ip host-routing
no ip source-route
```

ICMP redirects should not be necessary in a well-designed network; therefore they should be disabled unless a specific need for them has been shown. In those small cases the network would be better suited with a re-design rather than relying on redirects. [3]

```
no ip icmp redirect
```

The HTTP server service is enabled on switches by default and should be disabled. We recommend disabling this service to reduce the amount of overhead and decrease the potential risks associated with the accessibility of this service.

```
no ip http server
```

Finally, it may be helpful to enable a certain settings to improve performance when community with the switch directly including Path MTU (RFC 1191) and TCP Selective ACK (RFC 2018).

```
ip tcp path-mtu-discovery
ip tcp selective-ack
```

Logins and Passwords

Authentication

Manageability and accounting can be improved by implementing AAA. AAA allows for the enforcement of security policies on all network devices including switches, routers, firewalls, and hosts. It relies on the existence of a RADIUS or TACACS server.

The options surrounding the configuration of AAA are quite extensive. Rather than include a simple example in this paper, administrators are encouraged to consult CCO for information on how to configure AAA for Cisco switches.

System Time

Time Zone

It is recommended that all devices on a given network share a standardized time setting. For world-wide companies, this is usually most easily accomplished by setting the time zone to GMT. This will simplify troubleshooting and problem determination by providing a consistent format for event logging eliminating the need for time zone correlation.

```
clock timezone Europe/London 0 0
```

NTP

Network Time Protocol (NTP) synchronization is important because it greatly increases the level of accuracy with event correlation during troubleshooting or security incident investigation. Switches should point to a trusted NTP server and use MD5 authentication where available. MD5 authentication decreases the risk of the system clock being modified unknowingly, especially if external servers are used. Authenticated NTP should be enabled to aid in research and troubleshooting.

```
! Define an authentication key pair for NTP and
! whether it will be trusted or untrusted
ntp authentication-key <id> md5 <secret_key>
! Set IP of the NTP server and key number
ntp server <ip_addr> key <id>
ntp server <ip_addr> prefer
! Enable NTP authentication.
ntp authenticate
! Set NTP trusted key number
ntp trusted-key <id>
```

To complete the NTP configuration, access to the NTP servers should be restricted with an ACL.

```
! Special ACL used for protecting NTP
access-list 3 permit <ip_addr> <mask>
!
ntp access-group peer <ip>
```

Management

MOTD Banner

Strongly worded login banners are recommended because they are used to communicate access notifications and warnings for unauthorized use. The wording of the banner needs to be both strong and unambiguous, and needs to fall within the legal boundaries of a given network's security policies. One suggestion is to use the banner below following a consistent pattern with banners on other network devices such as routers and servers.

```
banner motd ^
```

```

*****
* [WARNING] secure-switch-01
* This system is owned by [COMPANY]. If you are not
* authorized to access this system, exit immediately.
* Unauthorized access to this system is forbidden by
* company policies, national, and international laws.
* Unauthorized users are subject to criminal and civil
* penalties as well as company initiated disciplinary
* proceedings.
*
* By entry into this system you acknowledge that you
* are authorized access and the level of privilege you
* subsequently execute on this system. You further
* acknowledge that by entry into this system you
* expect no privacy from monitoring.
*****
^

```

Console Access

A password should be assigned to the console port along with a session timeout. Session timeouts ensure that connections will be disconnected after a specified period of inactivity to close idle sessions and to limit susceptibility to bypassing of session authentication. A ten minute timeout should be adequate for console login purposes.

```

line con 0
  session-timeout 10
  password 7 <password>
!

```

SNMP Access

SNMP community strings should be modified from the default to restrict user access to read-only privileges and only from trusted sources. The following entries are recommended:

```

! Send traps to specified destination
snmp host <ip> traps <community>
! Enable system traps
snmp enable traps
! Special ACL used for protecting SNMP
access-list 4 permit <ip_addr> <mask>
! Restrict access to read-only from trusted source
snmp community <community> ro 4

```

Additional restrictions should be placed on who is permitted to query the MIBs (Management Information Base). SNMP queries could potentially reveal information that is to be kept private. Further limiting SNMP access is recommended by configuring statements restricting queries to a particular subset of the MIB tree with the 'snmp view' command. Keep in mind that community strings for SNMP are sent in plain text.

Remote Access

Session filtering should equally be enabled for remote sessions to deny all unauthorized hosts from accessing to the switch. Depending on your

code version, SSH may also be available and should be preferred over telnet. All access is logged using the Access List logging feature and sessions are automatically timed out after 10 minutes of inactivity.

```
! Standard ACL used for restricting telnet access
access-list 1 permit <ip_addr> <mask> log

line vty 0 10
 session-timeout 10
 password 7 <password>
 access-class 1 in
 ! SSH may not be available on your IOS
 transport input ssh
!
```

More restrictive access can be assigned to a smaller subset of the available VTYs to reduce the chances of VTY depletion even from trusted sources.

```
! Special ACL used for protecting VTY
access-list 2 permit <ip_addr> <mask> log

line vty 11 15
 session-timeout 10
 password 7 <secret_password>
 access-class 2 in
 ! SSH may not be available on your IOS
 transport input ssh
!
```

Logging and Exceptions

A management configuration would not be complete without system logging. All logs should be forwarded to a remote syslog server for storage and review. Below we enable syslog logging with a few basic settings.

```
logging on
logging <IP>
logging buffered 16384
logging console
logging trap
logging facility LOCAL0
```

If possible, system exceptions (core dumps) should be copied to a remote TFTP server for posthumous review and analysis.

```
exception dump <IP>
exception core-file secure-switch-01
```

Conclusion

In this paper we have presented a template designed to guide security administrators towards hardening their Cisco switches. Whether they be deployed at the edge or in the core, switches are critical pieces of network infrastructure. Thus it is important to follow certain security guidelines when deploying these to ensure network data integrity and confidentiality. By following the principles set forth in this document, the administrator will

be well on his or her way towards reducing the risk of network intrusion or malicious misuse at a switch level.

References

[1] Security Templates

Cisco

<http://www.cymru.com/Documents/secure-ios-template.html>
<http://www.cymru.com/Documents/secure-bgp-template.html>

Bind

<http://www.cymru.com/Documents/secure-bind-template.html>

Juniper

<http://www.cymru.com/gillsr/documents/junos-template.pdf>
<http://www.cymru.com/gillsr/documents/junos-bgp-template.pdf>
<http://www.cymru.com/gillsr/documents/junos-bgp-appnote.pdf>

Riverstone

http://www.tigerteam.net/secureros/secure_ros.html
http://www.tigerteam.net/secureros/secure_bgp.html

Netscreen

<http://www.cymru.com/gillsr/documents/screenos-hardening-appnote.pdf>

[2] Song, Doug. Dsniff.

<http://monkey.org/~dugsong/dsniff/>

[3] Gill, Stephen. "ICMP Redirects are ba'ad mkay?", June 2002.

<http://www.cymru.com/gillsr/documents/icmp-redirects-are-bad.pdf>

Further Reading

For the reader who is interested in finding out more information on Layer 2 attacks and potential mitigation methods, several papers have been dedicated on the subject. Following is a sample of such documentation.

[1] Dugan, Stephen. "Protecting Your Cisco Infrastructure Against the Latest Attacktics", Feb 2002.

<http://www.blackhat.com/presentations/win-usa-02/dugan-winsec02.ppt>

[2] Covenry, Sean. "Hacking Layer 2: Fun with Ethernet Switches", July 2002.

<http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-convery-switches.pdf>

[3] Nicolas Fischbach, Sebastien Lacoste-Seris. "Protecting Your IP Network Infrastructure", May 2002.
<http://www.securite.org/presentations/secip/CSWcore02-SeclP-v1.ppt>

[4] Laurent Licour, Vincent Royer. "The IP Smartspoofing", October 2002.
<http://www.althes.fr/ressources/avis/smartspoof-en.pdf>

Appendix A

The following is a configuration template taken from the principles presented in this document and applied to the first switch in the topology.

```
hostname secure-switch-01
!
logging buffered 16386 debugging
enable secret 5 $1$2NJx$FZecPFaYaxxYKEWuZYBgF1
!
clock timezone Europe/London 0 0
!
mac-address-table secure AAAA.BBBB.CCCC fastethernet 0/1
mac-address-table secure AAAA.BBBB.DDDD fastethernet 0/2
mac-address-table static 0000.5E00.0002 fastethernet 0/1
mac-address-table static 0000.5E00.0002 fastethernet 0/2
no cdp advertise-v2
no cdp run
!
vtp mode transparent
!
no service finger
no service tcp-small-servers
no service udp-small-servers
!
! encrypt passwords with MD5
service password-encryption
service nagle
service tcp-keepalives-in
service tcp-keepalives-out
! log significant VTY-Async events
service pt-vty-logging
!
no ip domain-lookup
no ip finger
no ip host-routing
no ip source-route
no ip icmp redirect
no ip http server
!
ip tcp path-mtu-discovery
ip tcp selective-ack
no cgmpp
ip domain-name test.com
!
interface FastEthernet0/1
no ip address
no cdp enable
switchport access vlan 2
switchport mode access
switchport nonegotiate
spanning-tree portfast
spanning-tree bpdupfilter enable
port security
port security max-mac-count 2
port security action shutdown
```

```

!
interface FastEthernet0/2
no ip address
no cdp enable
switchport access vlan 2
switchport mode access
switchport nonegotiate
spanning-tree portfast
spanning-tree bpdupfilter enable
port security
port security max-mac-count 2
port security action shutdown
!
interface FastEthernet0/3
no ip address
no cdp enable
switchport access vlan 2
switchport mode access
switchport nonegotiate
spanning-tree portfast
spanning-tree bpdupfilter enable
port security
port security max-mac-count 1
port security action shutdown
!
interface FastEthernet0/4
no ip address
no cdp enable
switchport access vlan 3
switchport mode access
switchport nonegotiate
spanning-tree portfast
spanning-tree bpdupfilter enable
port security
port security max-mac-count 1
port security action shutdown
!
interface FastEthernet0/5
no ip address
no cdp enable
switchport access vlan 3
switchport mode access
switchport nonegotiate
spanning-tree portfast
spanning-tree bpdupfilter enable
port security
port security max-mac-count 1
port security action shutdown
!
interface FastEthernet0/6
no ip address
no cdp enable
switchport access vlan 3
switchport mode access
switchport nonegotiate
spanning-tree portfast
spanning-tree bpdupfilter enable
port security
port security max-mac-count 1
port security action shutdown
!
interface FastEthernet0/7
no ip address
no cdp enable
switchport access vlan 4
switchport mode access
switchport nonegotiate
spanning-tree portfast
spanning-tree bpdupfilter enable
port security
port security max-mac-count 1

```

```

    port security action shutdown
!
interface FastEthernet0/8
  no ip address
  no cdp enable
  switchport access vlan 4
  switchport mode access
  switchport nonegotiate
  spanning-tree portfast
  spanning-tree bpdupfilter enable
  port security
  port security max-mac-count 1
  port security action shutdown
!
interface FastEthernet0/9
  no ip address
  no cdp enable
  switchport access vlan 4
  switchport mode access
  switchport nonegotiate
  spanning-tree portfast
  spanning-tree bpdupfilter enable
  port security
  port security max-mac-count 1
  port security action shutdown
!
interface FastEthernet0/10
  no ip address
  no cdp enable
  switchport access vlan 5
  switchport mode access
  switchport nonegotiate
  spanning-tree portfast
  spanning-tree bpdupfilter enable
  port security
  port security max-mac-count 1
  port security action shutdown
!
interface FastEthernet0/11
  no ip address
  no cdp enable
  switchport access vlan 5
  switchport mode access
  switchport nonegotiate
  spanning-tree portfast
  spanning-tree bpdupfilter enable
  port security
  port security max-mac-count 1
  port security action shutdown
!
interface FastEthernet0/12
  no ip address
  no cdp enable
  switchport access vlan 5
  switchport mode access
  switchport nonegotiate
  spanning-tree portfast
  spanning-tree bpdupfilter enable
  port security
  port security max-mac-count 1
  port security action shutdown
!
interface FastEthernet0/13
  no ip address
  no cdp enable
  switchport mode access
  switchport nonegotiate
  shutdown
  spanning-tree portfast
  spanning-tree bpdupfilter enable
  port security

```

```

port security max-mac-count 1
port security action shutdown
!
interface FastEthernet0/14
no ip address
no cdp enable
switchport mode access
switchport nonegotiate
shutdown
spanning-tree portfast
spanning-tree bpdupfilter enable
port security
port security max-mac-count 1
port security action shutdown
!
interface FastEthernet0/15
no ip address
no cdp enable
switchport mode access
switchport nonegotiate
shutdown
spanning-tree portfast
spanning-tree bpdupfilter enable
port security
port security max-mac-count 1
port security action shutdown
!
interface FastEthernet0/16
no ip address
no cdp enable
switchport mode access
switchport nonegotiate
shutdown
spanning-tree portfast
spanning-tree bpdupfilter enable
port security
port security max-mac-count 1
port security action shutdown
!
interface FastEthernet0/17
no ip address
no cdp enable
switchport mode access
switchport nonegotiate
shutdown
spanning-tree portfast
spanning-tree bpdupfilter enable
port security
port security max-mac-count 1
port security action shutdown
!
interface FastEthernet0/18
no ip address
no cdp enable
switchport mode access
switchport nonegotiate
shutdown
spanning-tree portfast
spanning-tree bpdupfilter enable
port security
port security max-mac-count 1
port security action shutdown
!
interface FastEthernet0/19
no ip address
no cdp enable
switchport mode access
switchport nonegotiate
shutdown
spanning-tree portfast
spanning-tree bpdupfilter enable

```

```

port security
port security max-mac-count 1
port security action shutdown
!
interface FastEthernet0/20
no ip address
no cdp enable
switchport mode access
switchport nonegotiate
shutdown
spanning-tree portfast
spanning-tree bpduguard enable
port security
port security max-mac-count 1
port security action shutdown
!
interface FastEthernet0/21
no ip address
no cdp enable
switchport mode access
switchport nonegotiate
shutdown
spanning-tree portfast
spanning-tree bpduguard enable
port security
port security max-mac-count 1
port security action shutdown
!
interface FastEthernet0/22
no ip address
no cdp enable
switchport mode access
switchport access vlan 10
switchport nonegotiate
spanning-tree portfast
spanning-tree bpduguard enable
port security
port security max-mac-count 1
port security action shutdown
!
interface FastEthernet0/23
description Trunk Port
no ip address
no cdp enable
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
switchport trunk allowed vlan 2-10,1002-1005
port group 1 distribution destination
no shutdown
!
interface FastEthernet0/24
description Trunk Port
no ip address
no cdp enable
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
switchport trunk allowed vlan 2-10,1002-1005
port group 1 distribution destination
no shutdown
!
interface VLAN1
description Never use
shutdown
!
interface VLAN10
ip address 10.0.1.10 255.255.255.0
description Management VLAN
management
no ip directed-broadcast

```

```

no ip route-cache
!
access-list 1 remark Restrict TELNET access
access-list 1 permit <ip_addr> <mask> log
!
access-list 2 remark More restrictive TELNET access
access-list 2 permit <ip_addr> <mask> log
!
access-list 3 remark Restrict NTP access
access-list 3 permit <ip_addr> <mask>
!
access-list 4 remark Restrict SNMP access
access-list 4 permit <ip_addr> <mask>
!
!
logging on
logging <IP>
logging buffered 16384
logging console
logging trap
logging facility LOCAL0
! Send traps to specified destination
snmp host <ip> traps <community>
! Enable system traps
snmp enable traps
! Restrict access to read-only from trusted source
snmp community <community> ro 4
!
banner motd ^
*****
* [WARNING] secure-switch-01 *
* This system is owned by [COMPANY]. If you are not *
* authorized to access this system, exit immediately. *
* Unauthorized access to this system is forbidden by *
* company policies, national, and international laws. *
* Unauthorized users are subject to criminal and civil *
* penalties as well as company initiated disciplinary *
* proceedings. *
* *
* By entry into this system you acknowledge that you *
* are authorized access and the level of privilege you *
* subsequently execute on this system. You further *
* acknowledge that by entry into this system you *
* expect no privacy from monitoring. *
*****
^
line con 0
session-timeout 10
password 7 <password>
!
line vty 0 10
session-timeout 10
password 7 <password>
access-class 1 in
! SSH may not be available on your IOS
transport input ssh
!
line vty 11 15
session-timeout 10
password 7 <secret_password>
access-class 2 in
! SSH may not be available on your IOS
transport input ssh
!
! Define an authentication key pair for NTP and
! whether it will be trusted or untrusted
ntp authentication-key <id> md5 <secret_key>
! Set IP of the NTP server and key number
ntp server <ip_addr> key <id>
ntp server <ip_addr> prefer

```

```
! Enable NTP authentication.
ntp authenticate
! Set NTP trusted key number
ntp trusted-key <id>
ntp access-group peer <ip>
!
exception dump <IP>
exception core-file secure-switch-01
```