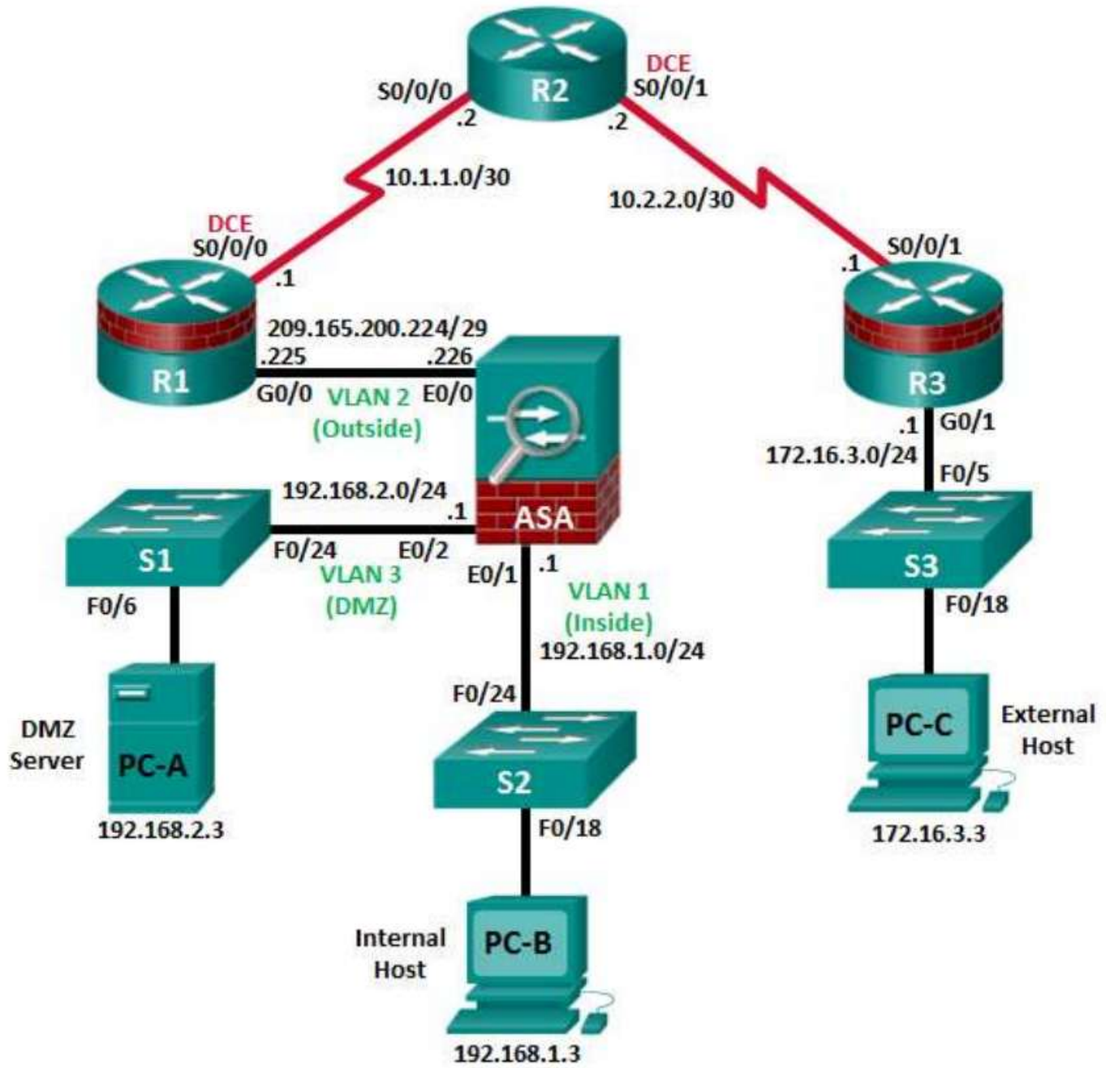
Table of Contents

Wednesday, 18 February 2026 11.26

CCNA Security 2.0



'All Commands' include many of the commands taught in Network Security Courses.
You will also find commands that were helpful to some students, but that you didn't see in the courses.

This is NOT a 'monkey see monkey do' manual but it is up to you to choose which commands to use and when.

Basic Router Setup

15 August 2018 10:55

```
!--------------------------------------
! Basic Device Setup (ROUTER)
!--------------------------------------
Enable
config terminal

interface s x/x
 ip address…
 clock rate 64000 ---(on DCE I/F only)

no ip domain-lookup

router ospf <process-id>
 router-id <id in DDN>
 passive-interface <int>
 network <net> <wm> area <area no>

sh ip ospf neighbor
sh ip ospf interface
sh ip protocols
sh ip route

clear ip ospf process


!-----------------------------------------
! Clock administration
!-----------------------------------------
calender set 08:00:00 Apr 7 2016(set HW clock)
clock set 08:00:00 Apr 7 2016(set software clock)

clock update-calender(set HW clock from SW clock)
Ntp update-calender(set HW clock from NTP clock)

Show clock detailed


!-----------------------------------------
! User administration
!-----------------------------------------
username user01 algorithm-type scrypt secret <PW>

0=Clear Text
5=Md5
6=Sha256
7=Cisco light encrypted
9=Scrypt (IOS 15.4 or later)



!--------------------------------------
! CDP/LLDP
!--------------------------------------
lldp run
show lldp neighbors detailed

cdp run
show lldp neighbors detailed
```

```
!-------------------------------------------------------------------
! Basic Router Setup - CCNA Security
!-------------------------------------------------------------------
security passwords min-length 10
enable algorithm-type scrypt secret <cisco12345> ---(TYPE 9)

line console 0
 password <ciscocon>
 exec-timeout 5 0
 login local ---(check user against local defined users)
 logging synchronous

line aux 0
 password <ciscoauxpass>
 exec-timeout 5 0
 login

line vty 0 4
 password <ciscovtypass>
 exec-timeout 5 0
 transport input <protocol> --- telnet (Telnet access only)
                                --- SSH (SSH access only)
                                --- telnet SSH (Telnet and SSH access)

 login local ---(check user against local defined users)

service password-encryption

banner motd #<text>#


Telnet <IP#>
```

```
!-----------------------------------------
! NTP Server
!-----------------------------------------
Clock set 08:00:00 Dec 16 2015 (SW clock)
Calender set 08:00:00 Dec 16 2015 (HW clock)

Clock timezone CET +2
Clock summer-time CET recurring

ntp authentication-key <#> md5 <PW>
ntp trusted-key <#>
ntp authenticate
ntp master <#>

show clock



!-----------------------------------------
! NTP Client
!-----------------------------------------
Clock timezone CET +2
Clock summer-time CET recurring

ntp authentication-key <#> md5 <PW>
ntp trusted-key <#>
ntp authenticate
ntp server <IP> key <#>
Ntp update-calender (routers only)

Show clock [detailed]
Show ntp associations
```

```
!-----------------------------------------------
! SSH server setup
!-----------------------------------------------
ip domain-name <DOM>
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
ip ssh version 2
ip ssh time-out 90
ip ssh authentication-retries 2

show ip ssh
show users ---(Who is online now?)


!---------------------------------------
! SSH Client
!---------------------------------------

SSH v1:
ssh -l cisco -c 3des 10.13.1.99

SSH v2:
ssh -v 2 -c aes256-cbc -m hmac-sha1-160 -l cisco 10.31.1.99

-l = Log in using this user name
-v = Specify SSH Protocol Version
-c = Select encryption algorithm
-p = Connect to this port#
-m = Select HMAC algorithm
-o = Specify options
WORD  IP address or hostname of a remote system
```

```
!------------------
! IOS Resilience
!------------------
secure boot-image

Secure boot-config

Show secure bootset


!-----------------------------------------------
! SCP server setup
!-----------------------------------------------
Need SSH Server already enabled

aaa new-model
aaa authentication login default local
aaa authorization exec default local
Ip scp server enable

On Client:
Copy scp: flash: ---(Get file from SCP server)
<IP add of SCP server>
<login name>
<File name>
<Dest. File name>
<Password for login>

Show flash
More <File Name> ---(Show content of this file>
```

Securing the router

01 May 2019 14:04

```
!----------------------------------------
! Securing the Control Plane (OSPF)IOS 15.4
!----------------------------------------
key chain <NAME>
 key <#>
 key-string <WORD>
 cryptographic-algorithm hmac-sha-256

interface s x/x/x
 ip ospf authentication key-chain <NAME>

show ip ospf interface s x/x/x
show ip ospf neighbor
show ip route
```

```
!----------------------------------------
! Securing the Control Plane (OSPF)on 1841/2811
!----------------------------------------

interface s x/x/x
 ip ospf authentication
 ip ospf authentication-key cisco
or
interface s x/x/x
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 cisco

show ip ospf interface s x/x/x

show ip ospf neighbor
show ip route
```

```
!-----------------------------------
! AutoSecure
!-----------------------------------
Script to secure based on experience:

auto secure

Makes a backup of previous config
(pre_autosecure.cfg)
```

```
!-----------------------------------
! Access security
!-----------------------------------
security passwords min-length #
service password-encryption

enable algorithm-type <MD SCRYPT SHA256 secret>

banner <modt exec login> ^C WORD ^C
```

```
!-----------------------------------
! Login enhancement
!-----------------------------------
login block-for <sec> attempts <#> within <sec>
login quiet-mode access-class <ACL# or name>
login delay <sec>
login on-success log <every or #>
login on-failure log <every or #>

security authentication failure rate <rate> log

show login failures
```

```
!----------------------------------------
! AAA and Local Authentication
!----------------------------------------
aaa new-model
aaa authentication login default <local local-case enable none>
aaa authentication login <NAME> group <local local-case enable none>

Special set for special access:
aaa authentication login <NAME> local

Line vty 0 4
 login authentication <NAME> ---(all others use defaults)

debug aaa authentication
```

```
!----------------------------------------
! AAA and RADIUS Authentication
!----------------------------------------
aaa new-model
aaa authentication login default group radius none
aaa authentication login <NAME> group radius

Radius server <Server Name or IP>
Address ipv4 <IP> ---(Default ports for RADIUS is 1645+1646
Key <WORD>

Line vty 0 4
Login authentication <NAME>

End

Address ipv4 <IP> auth-port 1812 acct-port 1813

debug aaa authentication
```

```
!----------------------------------------
! AAA and Local Authorization
!----------------------------------------
aaa new-model
aaa authorization exec default <local local-case enable none>

debug aaa authorization
```

```
!----------------------------------------
! AAA and RADIUS Authorization
!----------------------------------------
aaa new-model
aaa authorization exec default group radius none

Radius server <Server Name or IP>
Address ipv4 <IP> ---(Default ports for RADIUS is 1645+1646
Key <WORD>

debug aaa authorization
```

```
!-----------------------------------
! User/command privilege control
!-----------------------------------
Privilege exec level 10 reload
Privilege exec level 10 erase
enable algorithm-type scrypt secret level 10 cisco10
```

```
!----------------------------------------
! Administrative Roles
!----------------------------------------
Need AAA already enabled

enable view
<PW> ---(Admin PW giving access to root view)

Parser view admin1
Secret <PW> ---(PW giving access to this view)
Commands exec include all show
Commands exec include all config terminal
Commands exec include all debug
End

Show parser view

Enable view <Name>
<PW>
```

```
!-----------------------------------
! Views control
!-----------------------------------
Need AAA already enabled
enable view
Password: <WORD>

parser view <NAME>
secret <WORD>
Command exec include all <command>

parser view <NAME> superview
secret <WORD>
view <existing view NAME>

No parser view

Show parser view
```

```
!----------------------------------------
! WEB Server
!----------------------------------------
ip http server
ip http authentication <local/aaa/enable>

ip http secure-server
```

IPS

17-08-2016 12:55

```
!----------------------------------------
! IPS Setup
!----------------------------------------

mkdir ipsdir If present can be deleted by:

crypto key pubkey-chain rsa
named-key realm-cisco.pub signature
key-string
[KEY string from realm-cisco.pub.key.txt]
Quit

ip ips name iosips
ip ips config location flash:ipsdir

ip http server
ip ips notify sdee
ip ips notify log
clock set 01:20:00 8 march 2015
logging 192.168.1.3

interface serial0/0/0
ip ips iosips in

copy tftp://[TFTP IP #]/IOS-[version]-CLI.pkg idconf

ip ips signature-category
 category all
retired true
Exit
category ios_ips basic
retired false
exit

ip ips signature-definition
 signature 2004 0
status
 retired false
 enabled true
 engine
 event-action produce-alert
 event-action deny-packet-inline
 event-action reset-tcp-connection
 exit
 exit



dir flash:ipsdir

show logging
show ip ips signature count
show ip ips all
```

```
!----------------------------------------
! Basic Router Setup - CCNA Security
!----------------------------------------
Perform basic Router setup
Enable
Config terminal

username admin01 algorithm-type scrypt secret cisco12345

security passwords min-length 10
enable algorithm-type scrypt secret <cisco12345> ---(TYPE 9)

interface s x/x
 ip address…
 clock rate 64000 ---(on DCE I/F only)

no ip domain-lookup

ip domain-name ccnasecurity.com
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024

ip ssh version 2
ip ssh time-out 90
ip ssh authentication-retries 2

line console 0
 exec-timeout 5 0
 login local
 logging synchronous

line aux 0
 exec-timeout 5 0
 login local

line vty 0 4
 exec-timeout 5 0
 transport input ssh
 login local

service password-encryption

banner motd #<text>#
```

Zone Based FW

14-06-2017 11:12

```
!----------------------------------------
! Zone Based Firewall
!
zone security INSIDE
Zone security INTERNET
```

Creates the zones.

```
class-map type inspect match-any <Class-Map-Inside-Protocols>
 match protocol tcp
 match protocol udp
 match protocol icmp
```

Identify the trafic for inspection..

```
policy-map type inspect <Policy-Map-Inside-To_Outside>
 class type inspect <Class-Map-Inside-Protocols>
  inspect
 class type inspect class-default
  drop
```

When the identified trafic is met, what do with it.
Any other trafic (class default) i dropped.

```
zone-pair security <Zone-Pair-Security-Inside-To-Outside> source INSIDE destination INTERNET
 service-policy type inspect <Policy-Map-Inside-To_Outside>
```

When trafic moves between the 2 zones what ryules is to be enforced.

```
Interface X/X/1
Zone-member security INSIDE
Interface X/X/2
Zone-member security INTERNET
```

Make the physical port member of a zone

```
zone security DMZ
```

Creates the last zone.

```
class-map type inspect match-any <Class-Map-DMZ-Protocols>
 match protocol http
 match protocol https
 match protocol dns
```

Identify the trafic for inspection..

```
policy-map type inspect <Policy-Map-DMZ-To_Outside>
 class type inspect <Class-Map-DMZ-Protocols>
  inspect
 class class-default
  drop
```

When the identified trafic is met, what do with it.
Any other trafic (class default) i dropped.

```
zone-pair security <Zone-Pair-Security-Inside-To-Outside> source DMZ destination INTERNET
 service-policy type inspect <Policy-Map-DMZ-To_Outside>
```

When trafic moves between the 2 zones what ryules is to be enforced.

```
Interface X/X/3
Zone-member security DMZ
```

Make the physical port member of a zone

```
NOTE:
Now there are rules going from DMZ to INTERNET and from INSIDE to INTERNET.
All other directions is ruled by the default rule: Trafic going from one zone to
another zone is NOT allowed  if no specific rule exists.

The “self” zone is a special default security zone. This zone relates to traffic that
originates in or is destined to the control plane of the router itself (e.g. routing
protocols, SSH, SNMP, etc.). By default, all traffic is allowed into the “self” zone.
```

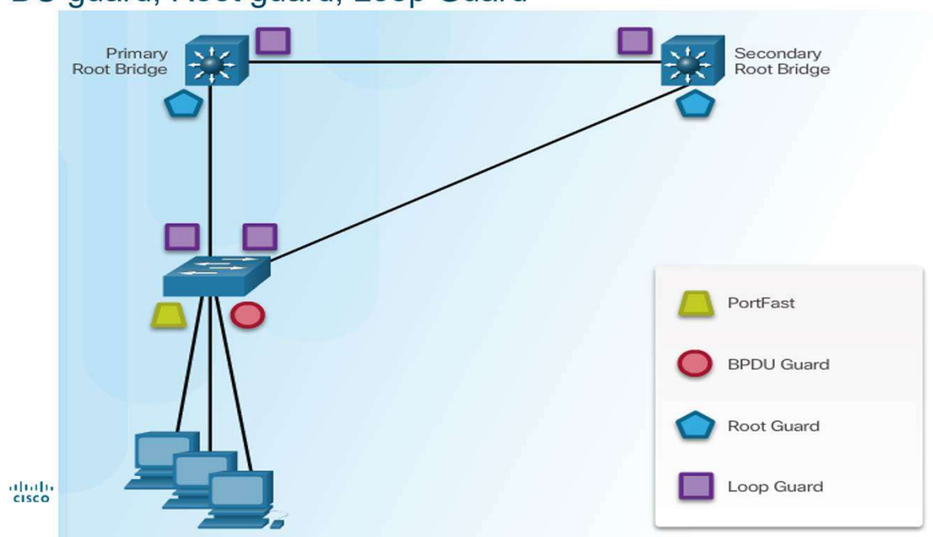
Source Interface Member of Zone?	Destination Interface Member of Zone?	Zone-Pair Exists?	Policy Exists?	Result
YES (self-zone)	YES	NO	N/A	PASS
YES (self-zone)	YES	YES	NO	PASS
YES (self-zone)	YES	YES	YES	INSPECT
YES	YES (self-zone)	NO	N/A	PASS
YES	YES (self-zone)	YES	NO	PASS
YES	YES (self-zone)	YES	YES	INSPECT
NO	NO	N/A	N/A	PASS
YES	NO	N/A	N/A	DROP
NO	YES	N/A	N/A	DROP
YES (private)	YES (private)	N/A	N/A	PASS
YES (private)	YES (public)	NO	N/A	DROP
YES (private)	YES (public)	YES	NO	PASS
YES (private)	YES (public)	YES	YES	INSPECT

Securing L2

Wednesday, 18 February 2026 10.31

```
!----------------------------------------
! 2960/3560/3650 differences
!----------------------------------------
2950 switche
Need a space before and after comma between
interfaces in "interface range" command.
No encapsulation command (dot1.q only)

3650 switche
Uses Gigabitports all over
gi 1/0/1-24
gi 0/0 is for managesment
No encapsulation command (dot1.q only)

3560 switche
Define trunk encapsulation: issue "switchport
trunk encapsulation dot1q" on all trunk
interfaces before making it a trunk.
```

BPDU guard, Root guard, Loop Guard

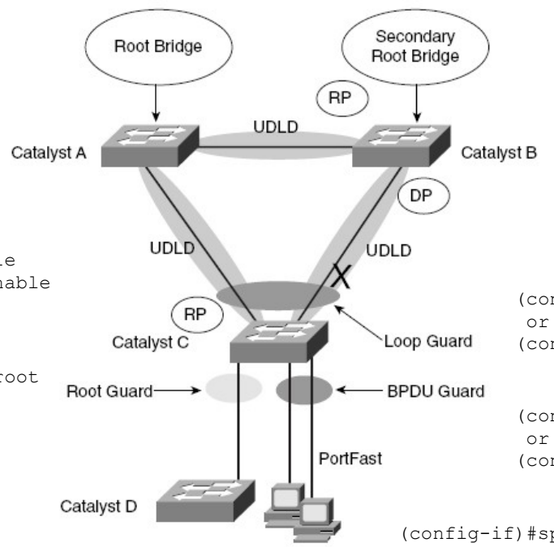



```
!-------------------------------------
! Securing TRUNK ports
!-------------------------------------
spanning-tree vlan 1 root primary
spanning-tree loopguard default (default for all STP enabled ports)


interface fastethernet 0/1
encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 99
switchport nonegotiate
spanning-tree guard root !only ports AWAY from Root Switch
spanning-tree guard loop !Alternative to loopguard default.
                         !Only ports WITHOUT guard root

Evt. ranges:
interface range fa 0/1 - 10, fa 0/11

show spanning-tree
show interface trunk
show interface fa 0/x trunk
show interface fa 0/x switchport
```

```
!--------------------
! show run extensions
!--------------------
show run | begin 0/1
```

```
!------------------------------------------------------
! Logging port security
!------------------------------------------------------
 logging logfile messages 6
 logging level port-security 5
 logging event link-status default
```

```
!------------------------------------------------------
! Securing access ports
!------------------------------------------------------
switchport mode access
switchport access vlan <vid>

spanning-tree portfast (on each port)
spanning-tree bpduguard enable (on each port)


spanning-tree portfast default (default for all access ports)

spanning-tree portfast bpduguard default
! (default for all access ports)
! Bemærk at på noget nyere udstyr hedder det:
! spanning-tree portfast edge bpduguard default

switchport port-security (REMEMBER this turns feature ON)
switchport port-security mac-address xxxx.xxxx.xxxx
switchport port-security max 3
switchport port-security violation shutdown
switchport port-security aging time [sec]

switchport protected

show spanning-tree summary
show spanning-tree interface fa 0/1 detail
show spanning-tree inconsistentports
show interfaces fa 0/1
show port-security
show port-security interface fa 0/1
show port-security address
```




```
(config)#spanning-tree udld enable
(config-if)#spanning-tree udld enable

(config-if)#spanning-tree guard root

(config)#spanning-tree loopguard default
 or
(config-if)#spanning-tree guard loop

(config)#spanning-tree portfast bpduguard default
 or
(config-if)#spanning-tree bpduguard enable

(config-if)#spanning-tree portfast
```

Protecting against **unexpected** BPDUs

Protecting against **sudden loss** of BPDUs

Root guard: Apply to ports where root is never expected. -> root-inconsistent

BPDU guard: Apply to all user ports where PortFast is enabled. -> errdisable

Loop guard: Apply to nondesignated ports but okay to apply to all ports.

UDLD: Apply to all fiber-optic links between switches (must be enabled on both ends).

Permissible combinations on a switch port:

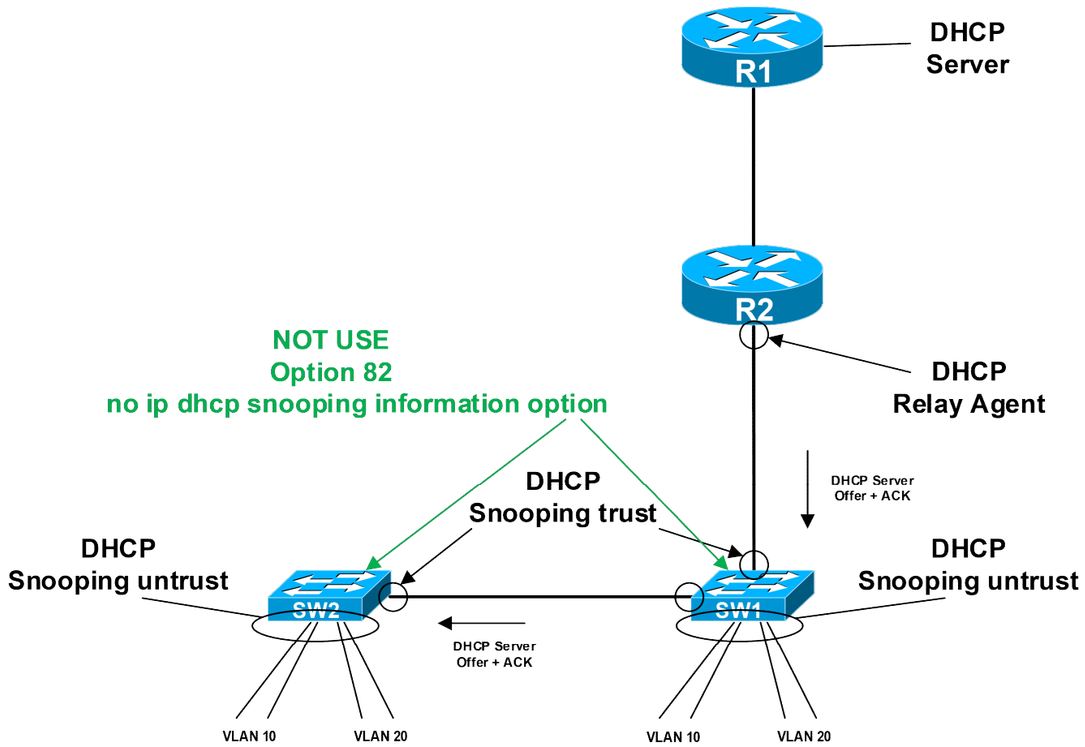
- Loop guard and UDLD
- Root guard and UDLD

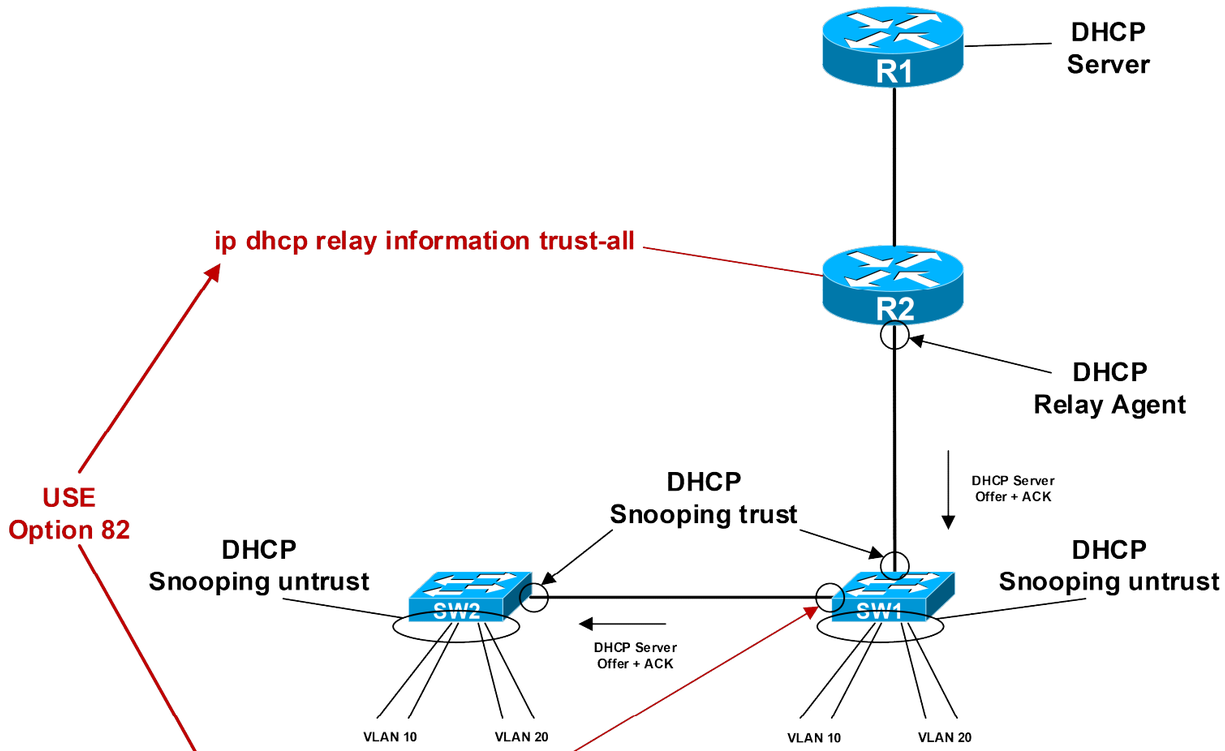
Not permissible on a switch port:

- Root guard and Loop guard
- Root guard and BPDU guard

DHCP Snooping (option 82)

22 August 2018 14:54



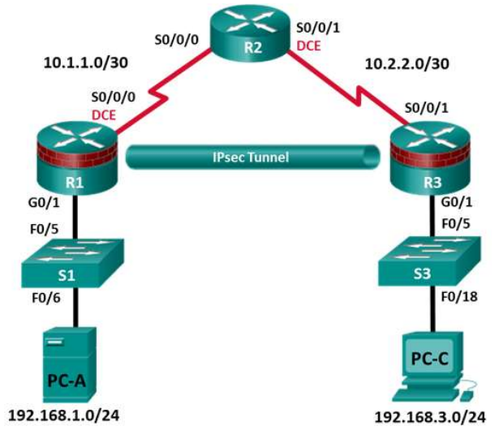



```
!-------------------------------------
! DHCP Snooping (no option 82)
!-------------------------------------
ip dhcp snooping
ip dhcp snooping vlan <>
no ip dhcp snooping information option
!
! On all links where DHCP server packets are expected
int <>
 ip dhcp snooping trust

! On all untrusted ports (optional)
int <>
 ip dhcp snooping limit rate <>


sh ip dhcp snooping
```

```
!-------------------------------------
! DHCP Snooping (use option 82)
!-------------------------------------
ip dhcp snooping
ip dhcp snooping vlan <>
ip dhcp snooping information option
!
! On all links where DHCP server packets are expected
int <>
 ip dhcp snooping trust

! On all untrusted ports (optional)
int <>
 ip dhcp snooping limit rate <>

! The following according to drawing
! ip dhcp relay information trust-all
! ip dhcp snooping information option allow-untrusted

sh ip dhcp snooping
```

VPN Site to Site - IPSec

13. januar 2016 14:06

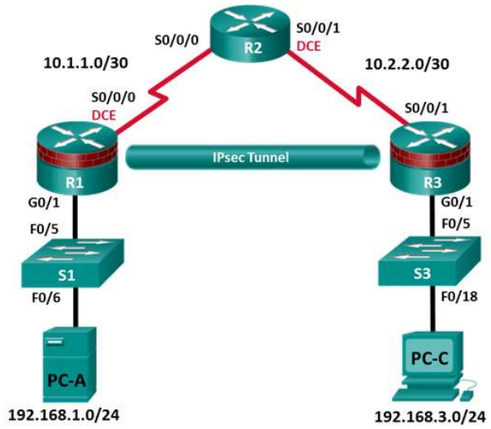



```
!----------------------------------------
! VPN - Site to Site, Site A
!----------------------------------------

crypto isakmp enable

crypto isakmp policy 10
 hash sha
 authentication pre-share
 group 14
 lifetime 3600
 encryption aes 256
 end

crypto isakmp key cisco123 address 10.2.2.1

crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
crypto ipsec security-association lifetime seconds 1800

access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

crypto map CMAP 10 ipsec-isakmp
match address 101
set peer 10.2.2.1
set pfs group14
set transform-set 50
set security-association lifetime seconds 900

Interface s 0/0/1
 crypto map CMAP

show crypto isakmp policy
show crypto ipsec transform-set
show crypto map
show crypto isakmp sa
show crypto ipsec sa
```

```
!----------------------------------------
! VPN - Site to Site, Site B
!----------------------------------------

crypto isakmp enable

crypto isakmp policy 10
 hash sha
 authentication pre-share
 group 14
 lifetime 3600
 encryption aes 256
 end

crypto isakmp key cisco123 address 10.1.1.1

crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
crypto ipsec security-association lifetime seconds 1800

access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255

crypto map CMAP 10 ipsec-isakmp
match address 101
set peer 10.1.1.1
set pfs group14
set transform-set 50
set security-association lifetime seconds 900

Interface s 0/0/1
 crypto map CMAP

show crypto isakmp policy
show crypto ipsec transform-set
show crypto map
show crypto isakmp sa
show crypto ipsec sa
```

VPN Site to Site - IPSec with GRE

16 August 2018 14:51




```
!----------------------------------------
! VPN - Site to Site, Site A
!----------------------------------------

Interface Tunnel 0
 ip address 192.168.99.1 255.255.255.0
 tunnel source Serial 0/0/0
 tunnel destination 10.2.2.1


crypto isakmp enable

crypto isakmp policy 10
 hash sha
 authentication pre-share
 group 14
 lifetime 3600
 encryption aes 256
 end

crypto isakmp key cisco123 address 10.2.2.1

crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
crypto ipsec security-association lifetime seconds 1800

access-list 101 permit gre host 10.1.1.1 host 10.2.2.1

crypto map CMAP 10 ipsec-isakmp
match address 101
set peer 10.2.2.1
set pfs group14
set transform-set 50
set security-association lifetime seconds 900

Interface s 0/0/0
 crypto map CMAP

show crypto isakmp policy
show crypto ipsec transform-set
show crypto map
show crypto isakmp sa
show crypto ipsec sa
```

Remember to add the GRE link to your routing protocol on Site A +B

```
!----------------------------------------
! VPN - Site to Site, Site B
!----------------------------------------

Interface Tunnel 0
 ip address 192.168.99.2 255.255.255.0
 tunnel source Serial 0/0/1
 tunnel destination 10.1.1.1

crypto isakmp enable

crypto isakmp policy 10
 hash sha
 authentication pre-share
 group 14
 lifetime 3600
 encryption aes 256
 end

crypto isakmp key cisco123 address 10.1.1.1

crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
crypto ipsec security-association lifetime seconds 1800

access-list 101 permit gre host 10.2.2.1 host 10.1.1.1

crypto map CMAP 10 ipsec-isakmp
match address 101
set peer 10.1.1.1
set pfs group14
set transform-set 50
set security-association lifetime seconds 900

Interface s 0/0/1
 crypto map CMAP

show crypto isakmp policy
show crypto ipsec transform-set
show crypto map
show crypto isakmp sa
show crypto ipsec sa
```

VPN Site to Site - VTI with IPSec

Wednesday, 18 February 2026 11.26

```
! Statisk Virtual Tunnel Interface (VTI)
! Create ISAKMP Phase 1 profile
crypto isakmp policy <no>
  encryption <encryption algorithm>
  hash <hash algorithm>
  authentication <method>
  group <Diffie Hellman>
  lifetime <sec>                 ! Optional
  exit

! IF using PreSharedKey for authentication:
crypto isakmp key <pw> address <partner ip-addr or hostname>

! Create Transform-set for Phase 2
crypto ipsec transform-set <TransformSet-name> <encryption algorithm> <hash algorithm>
  mode tunnel
  exit

! Create IPSEC Phase 2 profile
crypto ipsec profile <Profile-name>
  set transform-set <TransformSet-name>
  exit

! Configure the tunnel interface
interface Tunnel1
  bandwidth <bandwidth>        ! Optional - used for routing prioritization
  ip address <ip address for tunnel> <mask for tunnel>
  ip mtu <mtu size>            ! Calculate your mtu based on added headers
  tunnel source <own outside ip-addr>
  tunnel destination <partners outside ip-addr or hostname>
  tunnel mode ipsec <protocol> ! Define as IPSEC tunnel & select transport-prot.
  tunnel protection ipsec profile <Profile-name>
! Optional - Add tunnel to your routing protocol

! Verify tunnel
show interfaces <int>   ! Check tunnel ip, protocol & protection
show crypto session     ! Check session status & peer
show crypto ipsec sa    ! Check packet encaps & decaps
                        !     MUST increase when pinging.
```

ASA

13. januar 2016 14:07

```
!--------------------------------------
! ASA - Clear Configuration
!--------------------------------------
enable
Password: <PW>

Config terminal
configure factory-default
(answer quesions)
exit

write erase (delete startup-config not supported)

reload


!-----------------------------------------
! ASA - Basic Configuration from a cleared config
! Prepare for ASDM
!-----------------------------------------

Config terminal

hostname CCNAS-ASA
domain-name ccnasecurity.com
passwd cisco (for Telnet use on lines)
enable password class

clock set 19:09:00 april 19 2015

interface vlan <#>
nameif inside
ip address <IP#> <MASK>
security-level 100

interface <int>
switchport access vlan <#>
no shutdown

http server enable
http <NET# or IP#> <MASK> inside

show version
show file system
show running-config
show start
show interface e0/0
show interface ip brief
show ip address (show ip int brief on a router)
show switch vlan
show run interface vlan 1
```

```
!-----------------------------------------
! ASA - Basic Configuration commands
!-----------------------------------------

route outside 0.0.0.0 0.0.0.0 <Next Hop IP/if>

object network INSIDE-NET
subnet <NET#> <MASK>
nat (inside,outside) dynamic interface
End

show run object
show run nat
show nat
show xlate
clear nat counters


Class maps - Define a match criterion.
Policy maps - Associate actions to the match criteria.
Service policies - Attach the policy map to an interface, or
globally to all interfaces of the appliance.

class-map inspection_default
match default-inspection-traffic
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect ip-options
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
```

```
!-----------------------------------------
! PAT
!-----------------------------------------
object network INSIDE-NET
subnet <NET#> <MASK>
nat (inside,outside) dynamic interface


!-----------------------------------------
! Static NAT
!-----------------------------------------
object network INSIDE-NET
subnet <NET#> <MASK>
nat (DMZ,outside) static <IP#>
```

```
!-----------------------------------------
! ASA - Basic Configuration commands
!-----------------------------------------
```

Add the inspection of protocol(s) to the policy map:

```
policy-map global_policy
 class inspection_default
 inspect <protocol name>

show run policy-map
```

Configure the ASA as a DHCP server:

```
dhcpd address <start IP# -<end IP#> inside
dhcpd option 3 ip <Default gateway IP#>
dhcpd dns <IP#>
dhcpd enable inside

show run dhcpd
```

Configuring AAA

```
aaa authentication ssh console LOCAL
```

Configuring SSH

```
crypto key generate rsa modulus 1024
ssh <NET# or IP#> <MASK> inside
ssh <NET# or IP#> <MASK> outside
ssh timeout 10

write mem
```

Configure the DMZ

```
interface vlan <#>
no forward interface vlan <#>
nameif DMZ
ip address <IP#> <MASK>
security-level 70
no shutdown

interface <int>
switchport access vlan <#>
no shutdown

show ip address
```

Configure static NAT to the DMZ server

```
object network [dmz-server]
Host <ip# of Server>
nat (dmz,outside) static <ext. Ip #>

access-list OUTSIDE-DMZ permit ip any host <ip# of Server>
access-group OUTSIDE-DMZ in interface outside
```

SNMP, Logging

30. marts 2016 13:23

```
!-------------------------------------------------------------------------
! SNMPv3
!-------------------------------------------------------------------------
ip access-list standard PERMIT-SNMP
permit 192.168.1.0 0.0.0.255
Exit

snmp-server view SNMP-RO iso included
snmp-server group SNMP-G1 v3 priv read SNMP-RO access PERMIT-SNMP
snmp-server user SNMP-Admin SNMP-G1 v3 auth sha Authpass priv aes 128 Encrypass
End

Show SNMP group
Show SNMP user
```

```
!-----------------------------------------------
! Logging
!-----------------------------------------------
Service timestamps log datetime msec
Logging host <IP>
Logging trap <#> or <WORD>---(severity level 0-7)
Logging source-interface s x/x/x
Logging on

Show logging
```

Severity	Keyword	Meaning
0	Emergencies	System is unusable
1	alerts	Immediate action required
2	critical	Critical conditions
3	errors	Error conditions
4	warnings	Warning conditions
5	notifications	Normal but significant condition
6	informational	Informational messages
7	debugging	Debugging messages