Cisco Catalyst 3750 Smartports Series Switches Smartports Macros

March 8, 2004

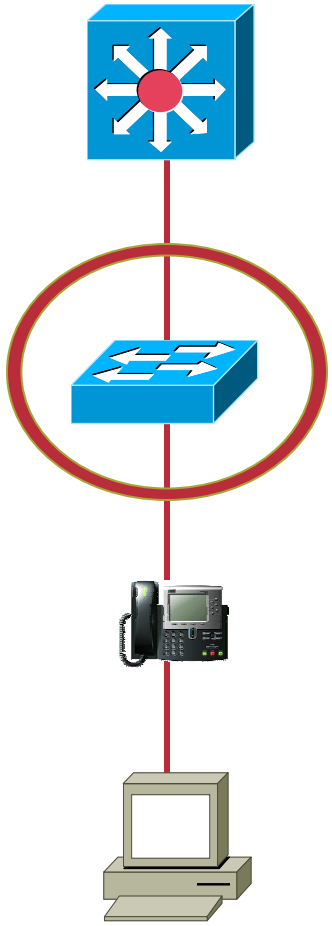
Smartports Global Configuration
Cisco Catalyst 3750

! Enable dynamic port error recovery for link state failures
errdisable recovery cause link-flap
errdisable recovery interval 60

! VTP requires Transparent mode current Best Practice
vtp domain [smartports]
vtp mode transparent

! Enable aggressive mode UDLD on all fiber uplinks
udld aggressive

! Enable Rapid PVST+ and Loopguard
spanning-tree mode rapid-pvst
spanning-tree loopguard default
spanning-tree extend system-id



Technical Whys
Global Configuration

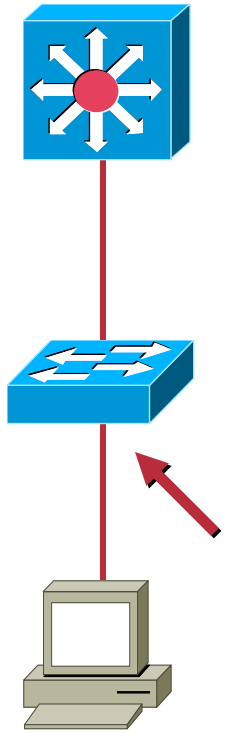
- udld aggressive
  - Software backup to GBIC hardware features
  - Helps prevent spanning tree issues
- errdisable recovery cause link-flap
- errdisable recovery interval 60
  - When a link-flap occurs, disable the port for 60 seconds
  - The default is 5 minutes, which is too long.
  - This feature can help prevent a link-flap from causing network stability issues

Technical Whys
Global Configuration

- **spanning-tree mode rapid-pvst**
  - **Enable 802.1w per VLAN Spanning Tree**
  - **Allows quicker convergence times**
- **spanning-tree loopguard default**
  - **Helps prevent errant spanning tree loops**
- **spanning-tree extend system-id**
  - **Allows for VLAN IDs greater than 1024**

Smartports IOS Standard Desktop
Cisco Catalyst 3750


```
! Reset all end-station interfaces to default configuration (global command)
default interface range FastEthernet[1]/0/[1 – 48]

! Basic interface - Enable data VLAN only
interface range FastEthernet[1]/0/[1 – 48]
 switchport access vlan $AVID
 switchport mode access

! Enable port security limiting port to a single MAC addresses
! Ensure age is greater than one minute and use inactivity timer
 switchport port-security

! “Port-security maximum 1” is the default and will not
! Show up in the config
 switchport port-security violation restrict
 switchport port-security aging time 2
 switchport port-security aging type inactivity

! Configure port as an edge network port.
! Ensure that another switch cannot become active on this interface.
 spanning-tree portfast
 spanning-tree bpduguard enable
```



Technical Whys
Desktop Configuration

- **default interface**

  Used to return the interface to a known configuration state

- **switchport port-security**

  Turn on port level mac address security

- **switchport port-security maximum 1 (or 3 for phones)**

  If port-security is turned on, the default number of allowed mac-addresses is 1. For an IP phone, we need 3 – one for the workstation, one for the phone on the voice Vlan and one for the phone on the native Vlan for CDP.

- **switchport port-security aging type inactivity**

  "Unlearn" mac-addresses once they have not been used for a while. The type of "inactivity" is needed in order for CDP from IP phones to be stable. During the mac relearn process, packets can become out-of-order/dropped. Using type "inactivity" helps prevent this once a mac address is learned – especially for voice traffic.

- **switchport port-security aging time 2**

  2 minutes is the shortest time possible and not have keep-alive problems with CDP.

  Also, IP Phones do not signal the switch when a workstation is unplugged. Without specifying an aging time, the mac address would never age out.

- **switchport port-security violation restrict**

  Do not take the port down when a violation occurs. Instead, allow the mac-addresses that we have already seen to continue working. All other traffic is dropped. Necessary with IP phones.

Technical Whys
Desktop Configuration (continued)

- **spanning-tree portfast**

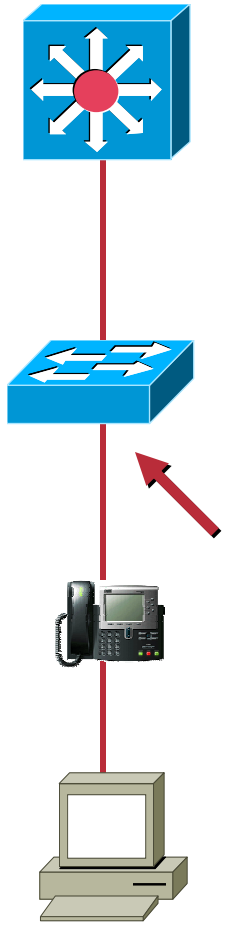
  This allows the port to pass traffic soon after the port becomes active – without waiting for spanning tree (~3 sec)

- **spanning-tree bpduguard enable**

  Disable the port if a switch/bridge is attached to this port. Inhibits errant network topologies and rogue switches.

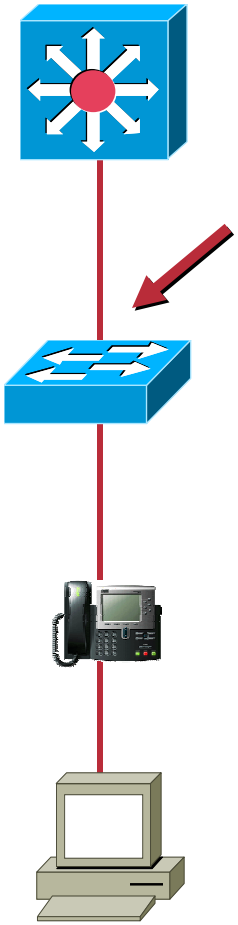
Smartports IOS Standard Desktop with IP Phone Cisco Catalyst 3750


```
! Reset all end-station interfaces to default configuration (global command)
default interface range FastEthernet0/[1 – 48]

! VoIP enabled interface - Enable voice (VVID) and data VLAN
interface range FastEthernet0/[1 - 48]
 switchport access vlan $AVID
 switchport mode access
 switchport voice vlan $VVID

! Enable port security limiting port to 3 MAC addresses. Ensure age is
! greater than one minute and use inactivity timer
 switchport port-security
 switchport port-security maximum 3
 switchport port-security violation restrict
 switchport port-security aging time 2
 switchport port-security aging type inactivity

! Enable auto-qos to extend trust to attached Cisco phone
 auto qos voip cisco-phone

! Configure port as an edge network port
 spanning-tree portfast
 spanning-tree bpduguard enable
```



Smartports IOS Switch Uplink
Cisco Catalyst 3750


```
! Reset all uplink interfaces to default configuration (global command)

default range GigabitEthernet0/[1 - 2]

! Uplink to Distribution
interface range GigabitEthernet0/[1 - 2]

! Define unique Native VLAN on trunk ports

 ! Define unique Native VLAN on trunk ports
 switchport trunk encapsulation dot1q
 switchport trunk native vlan $NVID
 #switchport trunk allowed vlan (VRANGE) #commented out to show capability

! Hardcode trunk and disable negotiation to speed up convergence
 switchport mode trunk
!
! Note:  Only add the following after both sides of the trunk have been configured
 switchport nonegotiate

! Configure autoqos to trust this interface
 auto qos voip trust
mls qos trust dscp

! 802.1w defines the link as pt-pt for rapid convergence
 spanning-tree link-type point-to-point
```



Technical Whys
IOS Switch Uplink

- **switchport nonegotiate**

  This command speeds convergence times; however, if issued before both sides of the trunk have been configured for 802.1q can cause the port to shutdown. The default trunk type is ISL on many switches. Once the trunk is up and configured for 802.1q, the "switchport nonegotiate" command can safely be entered.

- **switchport trunk allowed VLAN [data,voice,native]**

  This provides absolute control over which VLANs this switch will accept.

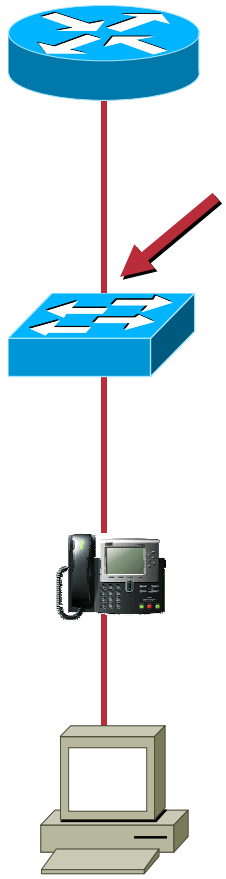
Recommended configuration on directly connected uplink switch for cisco-switch macro

Cisco.com

```
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 20
 switchport mode trunk
 mls qos trust cos
 auto qos voip trust
 macro description cisco-switch
 spanning-tree link-type point-to-point
```

Smartports IOS Router Uplink
Cisco Catalyst 3750


```
! Reset router uplink interface to default configuration
default interface FastEthernet0/[1]

! Router Uplink
interface FastEthernet0/[1]
switchport trunk encapsulation dot1q

! Define unique Native VLAN on trunk ports
 switchport trunk encapsulation dot1q
 switchport trunk native vlan $NVID
 #switchport trunk allowed vlan (VRANGE) #commented out to show capability

! Hardcode trunk and disable negotiation to speed up convergence
switchport mode trunk
switchport nonegotiate

! Configure autoqos to trust this interface
auto qos voip trust
mls qos trust dscp

! Ensure fast access to the network when enabling the interface.
! Ensure that switch devices cannot become active on the interface.
spanning-tree portfast
spanning-tree bpduguard enable
```



Recommended configuration on directly connected uplink router for cisco-router macro

- This configuration is based on an access switch connection to a branch router configured for data and voice vlans.

```
class-map match-all MEDIA
  match ip dscp 14
class-map match-all VOICE
  match ip dscp 46
class-map match-all CALL-CONTROL
  match ip dscp 26
class-map match-all MISSION-CRITICAL
  match ip dscp 18
!
policy-map output-L3-to-L2
  class VOICE
   set cos 5
  class CALL-CONTROL
   set cos 3
  class MISSION-CRITICAL
   set cos 2
  class MEDIA
   set cos 1
```

```
interface FastEthernet0/1
 no ip address
 no ip proxy-arp
 load-interval 30
 full-duplex
!
interface FastEthernet0/1.110
 description Voice-VLAN
 encapsulation dot1Q 109
 ip address 10.6.9.129 255.255.255.192
 service-policy output output-L3-to-L2
!
interface FastEthernet0/1.510
 description Data-VLAN
 encapsulation dot1Q 509
 ip address 10.6.9.1 255.255.255.128
service-policy output output-L3-to-L2
```

3750 global macro caveats

- **Example of global macro application:**

  Switch(config-if-range)# macro global apply cisco-global

- **vtp domain [smartports] –**

  There is a UI to configure this. This is applied by using the *'macro global apply cisco-global [smartports] <domain>*

- **VLAN's should be pre-defined before any templates are applied because some templates will add in vlans, some will not.**

3750 desktop and macro application caveats

Cisco.com

- **Example of cisco-desktop macro application:**

  Switch(config)#interface range f0/1 - 48

  Switch(config-if-range)#macro apply cisco-desktop $AVID 2

  % Access VLAN does not exist. Creating vlan 2

  %Warning: portfast should only be enabled on ports connected to a single

  host. Connecting hubs, concentrators, switches, bridges, etc... to this

  interface when portfast is enabled, can cause temporary bridging loops.

  Use with CAUTION

  %Portfast will be configured in 48 interfaces due to the range command

  but will only have effect when the interfaces are in a non-trunking mode.

- **'Command ?' is available for applying macros. Meaning of each $ value is shown in help text.**
- **When multiple macros are overlaid or applied to the same interface, the 'macro description' shows each overlaid macro name.** ***This is for good use in macro application history and debugging assistance.***

  interface FastEthernet0/1

  macro description cisco-desktop | cisco-desktop | cisco-phone

- **The command "switchport port-security maximum 1" listed in the cisco-desktop macro will NOT show up in the running config, and is a default condition.**
- **VLAN's should be pre-defined before any templates are applied because some templates will create VLAN's, some will not.**

3750 Desktop w/ IP Phone macro application caveats

Cisco.com

- **Example of cisco-phone macro application:**

  Switch(config)#interface range f0/1 - 48

  Switch(config-if-range)#macro apply cisco-phone $AVID 2 $VVID 3

- **The same warnings from IOS that were displayed for the desktop macro are not standard across all platforms. This appears to come from interaction between autoqos and vlan commands being applied at the same time. It does not have a negative affect upon the operation of macro application.**
- **The VVID is NOT created by default much like the $AVID is on deploying the desktop profile. This needs to be documented. VLAN's should be pre-defined before any templates are applied because some templates will create VLAN's, some will not.**
- **'Command ?' is available for applying macros. Meaning of each $ value is shown in help text.**

3750 switch uplink macro application caveats

Cisco.com

- **Example of cisco-switch macro application:**

  Switch(config)#interface g0/1

  Switch(config-if-range)#macro apply cisco-switch $NVID 999

- **switchport trunk allowed vlan VRANGE – This command is commented out in the code currently but remains in order to show capability. However, it is recommended for trunk configuration. If this command is not included, then spanning-tree loops could occur. Most notably on VLAN1. Changing the native vlan will mitigate this threat somewhat, but that's only assuming there's not a mismatch across the link to begin with.**
- **switchport nonegotiate – This command is commented out for this macro, the reason being that if both sides are not configured for this, the port could be put in to err-disable state. This occurs only on ISL compatible switches. It is recommended that this be applied only after initial macro application and verification of the configuration on directly connected device.**
- **There is a plan for the commands above to be incorporated some time in the summer '04.**
- **VLAN's should be pre-defined before any templates are applied because some templates will create VLAN's, some will not.**

3750 router uplink macro application Caveats

Cisco.com

- **Example of cisco-switch macro application:**

  Switch(config)#interface g0/1

  Switch(config-if-range)#macro apply cisco-router $NVID 999

- **switchport trunk allowed vlan VRANGE – This command is commented out in the code currently but remains in order to show capability. However, it is recommended for trunk configuration. If this command is not included, spanning-tree loops could occur. Most notably on VLAN1. Changing the native vlan will mitigate this threat somewhat, but that's only assuming there's not a mismatch across the link to begin with.**
- **switchport nonegotiate – This command is commented out for this macro, the reason being that if both sides are not configured for this, the port could be put in to err-disable state. This occurs only on ISL compatible switches. It is recommended that this be applied only after initial macro application and verification of the configuration on directly connected device.**
- **There is a plan for the commands above to be incorporated some time in the summer '04.**
- **VLAN's should be pre-defined before any templates are applied because some templates will create VLAN's, some will not.**