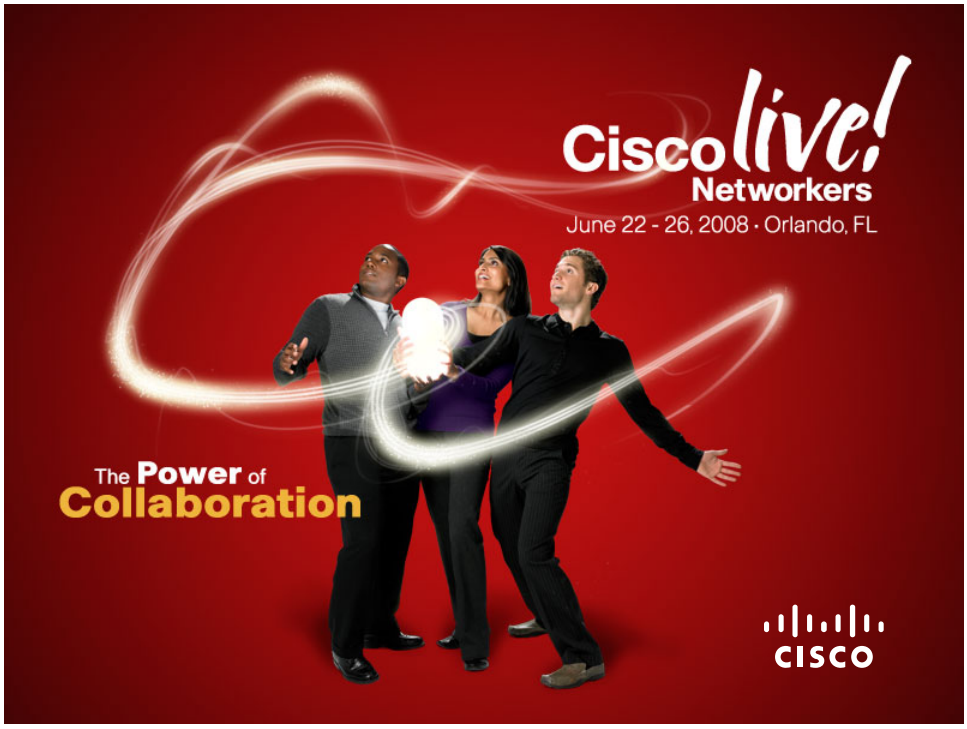


CISCO

Cisco live! Networkers

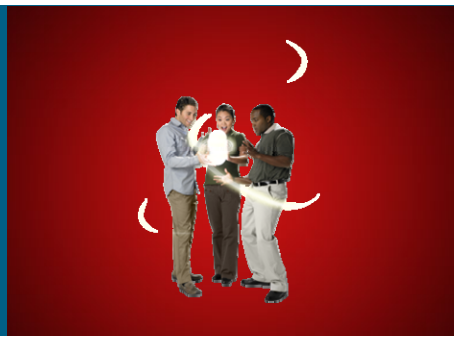
Troubleshooting LAN Protocols

BRKRST-3131

Agenda

- Session Overview
- Troubleshooting Layer 1, Layer 2, and Layer 3 Connectivity Issues
- Spanning Tree Protocol
- Security
- Common Issues for High CPU Utilization

Session Overview



Related Sessions

- RST-3141: Troubleshooting Cisco Catalyst 3750, 3550, and 2900 Series Switches by **Michel Peters**

  Tuesday 2:00 PM, Wednesday 4:30 PM, Thursday 4:30 PM

- RST-3142: Troubleshooting Cisco 4500 Series Switches by **Wendy Hower**

  Tuesday 4:30 PM, Thursday 10:30 AM

- RST-3143 Troubleshooting Catalyst 6500 Series Switches by **Barnaby Dianni**

  Wednesday 2:00 PM, Thursday 2:00 PM, Thursday 4:30 PM

Networking Concepts and Operations

- Be familiar with switching and routing concepts
- Understand the configurations on network devices
- Know what features are active and where
- Be familiar with Cisco's web sites

  Configuration guides

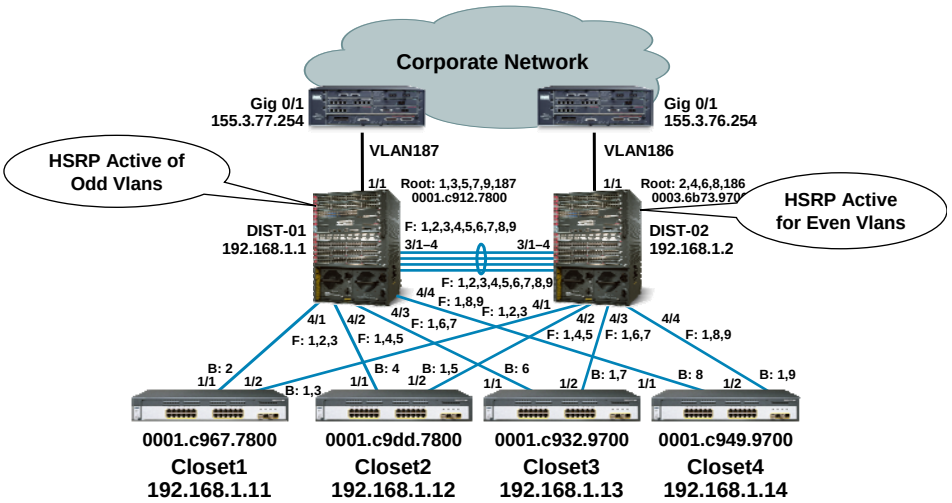
  Release notes

  Troubleshooting tips

  Software download page

Building Codes Reduce the Severity of Disasters

Network Diagram



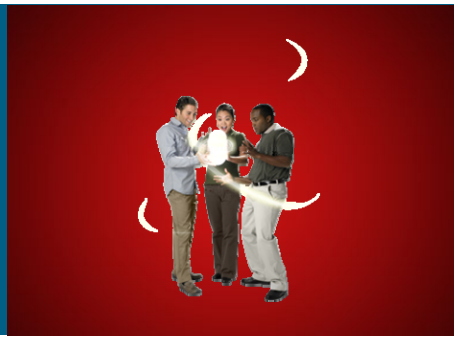
Have a Plan

- Don't assume anything
- Define the problem
- Understand what is working and what is not
- Is it intra-VLAN or inter-VLAN issue?
- Perform basic troubleshooting
- Keep the network diagram handy
- Keep a protocol analyzer handy
- Keep modem access ready for TAC support

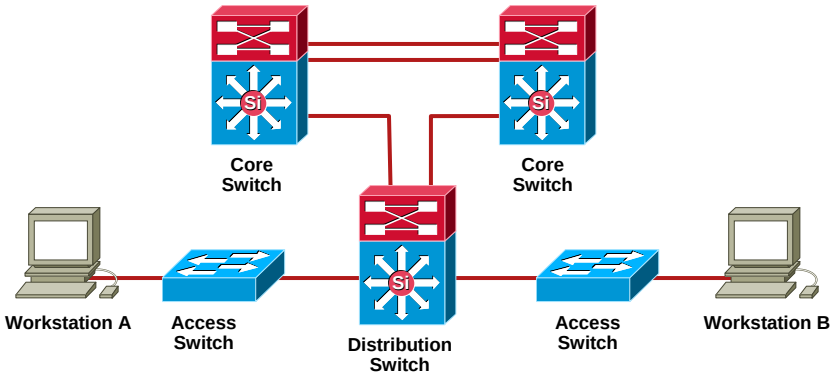
Agenda

- Session Overview
- Troubleshooting Layer 1, Layer 2, and Layer 3 Connectivity Issues
- Troubleshooting Spanning Tree Protocol
- Security
- Common Issues for High CPU Utilization

Troubleshooting Layer 1, Layer 2 and Layer 3 Connectivity Issues

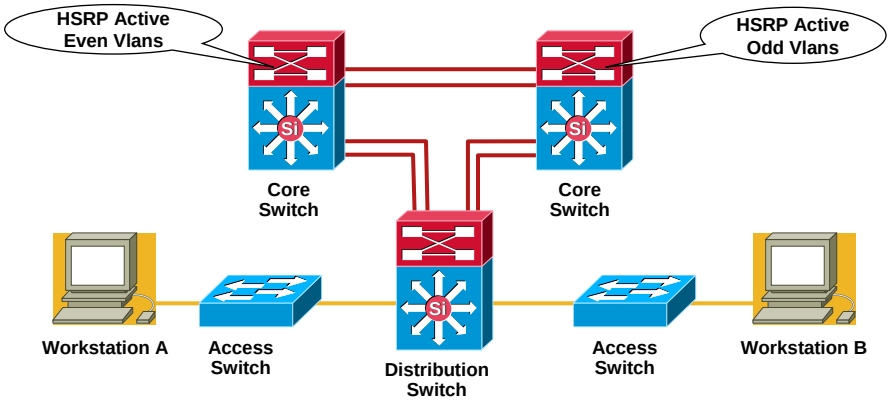


Define Problems



- Performance: latency, jitter, packet loss
- Connectivity: link, reachability

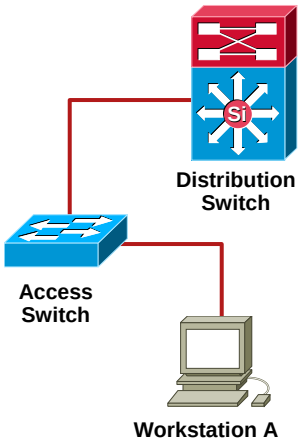
Troubleshooting Methodology



- Define issue between two specific stations
- Determine path of respective packets
- Begin systematic examination of path devices

Troubleshooting Layer 1

- Connectivity
  - Do we have a link?
- Traffic
  - Are packets passing?
  - How many?
- Speed/duplex
  - Do both sides match?



Link Comes up for 10/100 Mbs but Not for 1000Mbps

- Is one of the four pairs in a category 5 cable broken?
- The Time Domain Reflectometry (TDR) test can be run without having to disconnect the cables to determine if there are any broken wires in them
- Helps network administrator to discriminate between cables that can support the upgrade to higher speed and the ones that cannot
- TDR support is available for copper ports at this time, no support for optical as of today

Cable Fault—Time Domain Reflectometry (TDR)

- TDR determines cable faults
- Cat 5 cable has four cable pairs
- TDR detects faults in cable pairs such as opens or shorts
- TDR determines position of cable fault
- TDR test is invasive, link will be down for the test duration
- TDR test shows the result for each of the four cable pairs

Cable Fault—TDR

```
Router#test cable-diagnostics tdr interface GigabitEthernet3/1
Link state may be affected during TDR test
TDR test started on interface Gi3/1
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

```
Router#show cable-diagnostics tdr int g3/1

TDR test last run on: April 27 1:29:58
Interface Speed Pair Cable length        Distance to fault   Channel Pair status
--------- ----- ---- ------------------- ------------------- ------- -----------
-
Gi3/1     100   1-2  N/A                 N/A                 Pair A  Terminated

                3-4  N/A                 N/A                 Pair B  Terminated

                5-6  N/A                 5    +/- 2  m       Invalid Short

                7-8  N/A                 5    +/- 2  m       Invalid Short
```


Digital Optical Monitoring (DOM)

- Digital Optical Monitoring DOM is an industry-wide standard, known as “Digital Diagnostic Monitoring Interface for Optical Transceivers” (or SFF-8472 ftp://ftp.seagate.com/sff/SFF-8472.PDF), intended to define a digital interface to access real-time transceivers operating parameters such as:
  - Optical TX power
  - Optical RX power
  - Laser bias current
  - Temperature
  - Transceiver supply voltage
- With DOM the user has capability of performing in-service transceiver monitoring and troubleshooting operations

DOM Support on Cisco Transceivers

- DOM capabilities is **supported** on selected GBIC, SFP, Xenpak, X2 and XFP.
- Refer to the DOM Compatibility Matrix for details.
- The following conditions must be met for a particular transceiver type to qualify as supported:
  - –Cisco engineering has successfully verified the DOM functions during the qualification process of the transceiver.
  - –All the modules that Cisco has been shipping under a particular Product ID have DOM-capable hardware.
  - –Cisco manufacturing tests and verifies DOM support before each module is shipped to customers.
- Sometimes not all three conditions are met and DOM commands may work on transceivers which are not “DOM-supported.” An example could be XENPAK-10GB-ER.

Digital Read-Backs Interpretation

- Of the five digital diagnostic read-backs, the most relevant ones are Optical TX and RX power as well as temperature. The operating ranges of these three values is unique (available on the data sheets) across all modules of the same type (e.g. all DWDM Xenpaks).
- The supply voltage is specified in the data sheet of most transceivers. Typical values are 5V for GBICs, 3.3V for SFPs. In 10 G transceivers there are three voltage supplies 1.8, 3.3 and 5V. Not always all three voltages are utilized, hence this information is not called out in the data sheet.
- Note that the voltage supply read-back monitors just one voltage supply: this works on GBICs and SFPs which have one voltage supply, but with 10G pluggables which have three separate voltages, this parameter is not applicable.

Accessing DOM

- transceiver type all; [no] monitoring
  This command turns on/off the DOM monitoring process for all transceiver types in the system

```
Router(config)#transceiver type all
Router(config-xcvr-type)#monitoring

Router(config-xcvr-type)#end
```

- DOM is accessible also via CLI interface with the "show interface transceiver" command

```
#show interfaces transceiver

++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.

N/A: not applicable, Tx: transmit, Rx: receive.

mA: milliamperes, dBm: decibels (milliwatts).
Optical      Optical

          Temperature  Voltage   Current   Tx Power  Rx Power

Port      (Celsius)    (Volts)   (mA)      (dBm)     (dBm)

-----  -------   -------  ------  --------  --------  ------   ----------

Gi1/2     50.5         5.06      28.8      1.3       -9.6
```


show interface <int> transceiver detail

```
#show interfaces Te3/1 transceiver detail

[SKIP]
                                High Alarm  High Warn  Low Warn   Low Alarm

      Temperature               Threshold   Threshold  Threshold  Threshold

Port     (Celsius)              (Celsius)   (Celsius)  (Celsius)  (Celsius)
-------------------------------------------------------------------------------- ---
Te3/1    31.6                   79.1        74.1       4.1        -0.8

Voltage                         Threshold   Threshold  Threshold  Threshold

Port     (Volts)                (Volts)     (Volts)    (Volts)    (Volts)
-------------------------------------------------------------------------------
Te3/1    0.00                   0.00        0.00       0.00       0.00

Current                         Threshold   Threshold  Threshold  Threshold

Port     (milliamperes)         (mA)        (mA)       (mA)       (mA)
-------------------------------------------------------------------------------
Te3/1    99.2                   130.0       130.0      20.0       10.0

Optical
Transmit Power                  Threshold   Threshold  Threshold  Threshold

Port     (dBm)                  (dBm)       (dBm)      (dBm)      (dBm)
-------------------------------------------------------------------------------
Te3/1    -3.3                   3.5         3.0        -1.0       -1.5

Optical
Receive Power                   Threshold   Threshold  Threshold  Threshold

Port     (dBm)                  (dBm)       (dBm)      (dBm)      (dBm)
-------------------------------------------------------------------------------

Te3/1    -28.5        --        -6.5        -7.0       -24.1      -24.5
```

With 10 GE Interfaces the Value Is Usually 0, Because There the Voltage Supply Is Not Unique Unlike in GBICs and SFPs

Is Physical Interface Up? Troubleshooting Layer 1

```
IOS# show interface GigabitEthernet 1/1
GigabitEthernet1/1 is up, line protocol is up (connected)
 Hardware is Gigabit Ethernet Port, address is 0009.435f.8300 (bia 0009.435f.8)
 MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
   reliability 255/255, txload 1/255, rxload 1/255
 Encapsulation ARPA, loopback not set
 Keepalive set (10 sec)
 Full-duplex, 1000Mb/s, link type is auto, media type is SX
 output flow-control is off, input flow-control is on
 ARP type: ARPA, ARP Timeout 04:00:00
 Last input 00:00:00, output never, output hang never
 Last clearing of "show interface" counters never
 Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
 Queuing strategy: fifo
 Output queue: 0/40 (size/max)
 5 minute input rate 89000 bits/sec, 141 packets/sec
 5 minute output rate 23000 bits/sec, 24 packets/sec
   226241448 packets input, 14733424090 bytes, 0 no buffer
   Received 224084097 broadcasts (201828280 multicast)
   0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
   0 input packets with dribble condition detected
   35622 packets output, 5452233 bytes, 0 underruns
   0 output errors, 0 collisions, 0 interface resets
   0 babbles, 0 late collision, 0 deferred
   0 lost carrier, 0 no carrier
   0 output buffer failures, 0 output buffers swapped out
```

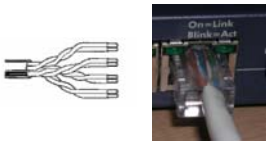
Are Input/Output Counters Incrementing

Check for Any errors/crc/collisions

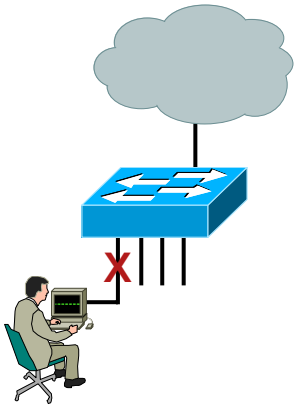
Symptoms of Port Start-Up Delay

- Dynamic Host Configuration Protocol (DHCP) address is not resolved
- 802.1x Client failing or delayed to get authenticated

Category 5 Cable



Is It a Physical Layer Issue?



Port Start-up Delay—Problem and Solution

- On linkup it takes up to 30–45 seconds for packets to flow
- Three things contribute to delay in packet forwarding on link up
  - Spanning Tree
  - Trunk auto-negotiation
  - Channel auto-negotiation

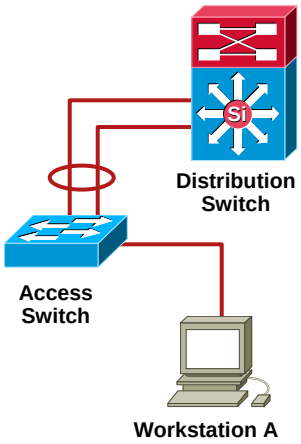
```
IOS(config)#interface range fastethernet 2/1 - 48
IOS(config-if)#switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled
```


Check Duplex Setting and Verify Topology—Layer 1 Troubleshooting

```
Router#show cdp neighbors detail
-------------------------
Device ID: 6500
Entry address(es):
 IP address: 10.205.0.1
Platform: cisco WS-C6506, Capabilities: Router Switch IGMP
Interface: GigabtEthernet3/1, Port ID (outgoing port): GigabitEthernet2/1
Holdtime : 138 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) s3223_rp Software (s3223_rp-ADVIPSERVICESK9_WAN-M), Version 12.2(18)SXF7
2, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by cisco Systems, Inc.
Compiled Thu 19-Jan-06 02:44 by dchih

advertisement version: 2
VTP Management Domain: 'Cisco'
Native VLAN: 1
Duplex: full
```

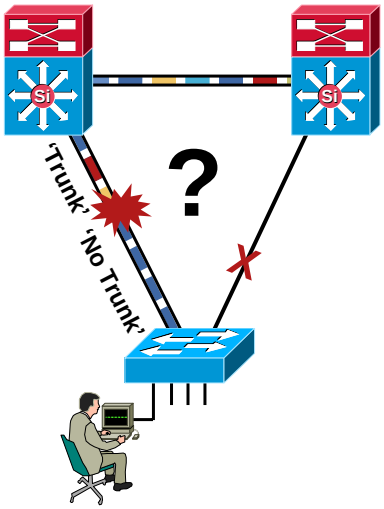
Troubleshooting Layer 2

- Trunk
  - Desirable | ON?
- Channel
  - Desirable | ON?
- Bridge table
  - MAC address learned correctly?
- Spanning Tree
  - Ports forwarding as expected?



Trunk—Problem Trunk Fails to Form

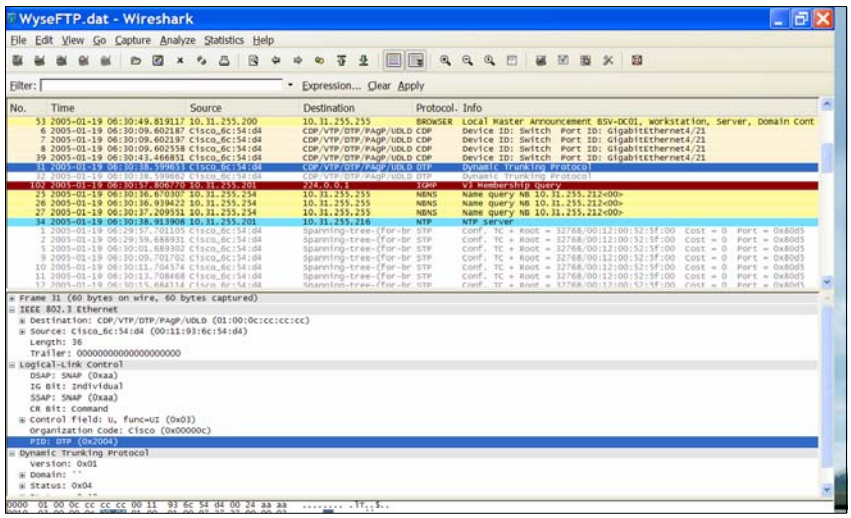
- A trunk is a link between two devices that carries multiple VLANs simultaneously
  - ISL—Inter-Switch Link; Cisco proprietary
  - IEEE 802.1q—standards-based trunk encapsulation
- Endpoint mismatch
- Inconsistent DTP configuration



Dynamic Trunk Protocol (DTP)

- What is DTP?
  - Automates ISL/802.1Q trunk configuration; operates between switches
  - Does not operate on routers; not supported on 2900XL or 3500XL
- DTP synchronizes the trunking mode on link ends (i.e., native VLAN mismatch, VLAN range mismatch, encapsulation, etc.)
- DTP state on ISL/dot1Q trunking port can be set to “auto”, “on”, “off”, “desirable”, or “non-negotiate”
- Runs over link layer; assumes point-to-point link
- DTP destination mac address is 01-00-0C-CC-CC-CC
- Port should be able to operate as an access port—to fall back to access mode
- During negotiation do not participate in STP
- VLAN1 should be added to trunk; in ISL DTP pkts send on VLAN1 and for access or 802.1Q on native vlan
- The HDLC protocol type for DTP is 0x2004 which is the SNAP format

DTP Packet Capture



Trunk—Solution
Trunking Modes

	Uses DTP	Forms Trunk with Off	Forms Trunk with Auto	Forms Trunk with Desirable	Forms Trunk with On	Forms Trunk with No Negotiate
Off	No	No	No	No	No	No
Auto	Yes	No	No	Yes	Yes	No
Desirable	Yes	No	Yes	Yes	Yes	No
On	Yes	No	Yes	Yes	Yes	Yes
No Negotiate	No	No	No	No	Yes	Yes

Trunk—Problem
Trunk Fails to Form

- Take help of CDP to verify topology
- One side configured for non-negotiate and other side desirable

```
Router#show cdp neighbors detail
------------------------
Device ID: 6500
Entry address(es):
 IP address: 10.205.0.1
Platform: cisco WS-C6506, Capabilities: Router Switch IGMP
Interface: GigabitEthernet3/1, Port ID (outgoing port): FastEthernet2/1
Holdtime : 138 sec
Version :
Cisco Internetwork Operating System Software
IOS (tm) s3223_rp Software (s3223_rp-ADVIPSERVICESK9_WAN-M), Version 12.2(18)SXF
2, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by cisco Systems, Inc.
Compiled Thu 19-Jan-06 02:44 by dchih

advertisement version: 2
VTP Management Domain: 'Cisco'
Native VLAN: 1
Duplex: full

Router#show interfaces gigabitEthernet 3/1 trunk

Port      Mode     Encapsulation Status     Native vlan
Gi3/1     desirable  802.1q     not-trunking 1
```

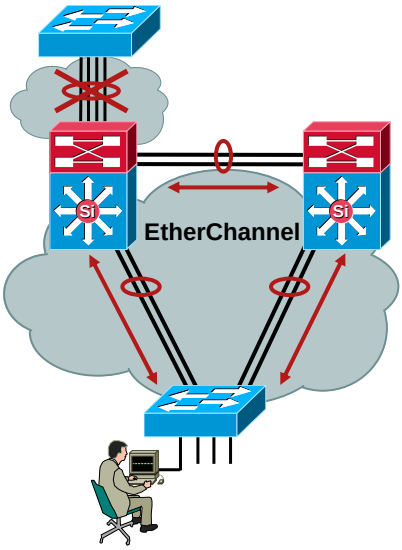

Trunk—Commands
Show Interfaces Switchport (Cisco IOS)

- show interfaces <int> switchport
- show interfaces trunk

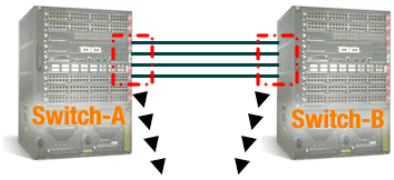
```
Router#sh int g3/1 trunk

Port  Mode     Encapsulation Status    Native vlan
Gi3/1  desirable 802.1q      trunking  1

Port  Vlans allowed on trunk
Gi3/1  1-4094

Port  Vlans allowed and active in management domain
Gi3/1  1-58,60-899,902-998,1000-1001

Port  Vlans in spanning tree forwarding state and not pruned
Gi3/1  1-58,60-899,902-998,1000-1001
```


Channel—Problems
Channel Fails to Form

- A channel is a method of grouping multiple physical links between two devices into a single logical link
  - EtherChannel® (PAgP)—Cisco proprietary port channeling
  - IEEE 802.3ad (LACP)—standards-based port channeling
- Incorrect configuration
- Port is err-disabled



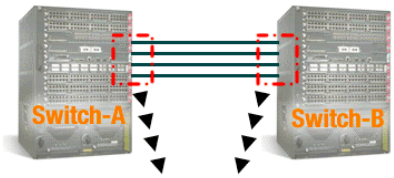
Mix of Modes Allowing PAGP to Form Channel



Which mix of modes allows PAGP to form an Etherchannel

Switch A	Switch B	Result
AUTO	AUTO	No EtherChannel group created
AUTO	DESIRABLE	EtherChannel group created
DESIRABLE	AUTO	EtherChannel group created
DESIRABLE	DESIRABLE	EtherChannel group created

Mix of Modes Allowing LACP to Form Channel



Which mix of modes allows LACP to form an Etherchannel

Switch A	Switch B	Result
PASSIVE	PASSIVE	No EtherChannel group created
PASSIVE	ACTIVE	EtherChannel group created
ACTIVE	PASSIVE	EtherChannel group created
ACTIVE	ACTIVE	EtherChannel group created

Channel—Solution
Channel Modes

z	Uses PAgP or LACP	Forms Channel with Off	Forms Channel with Auto	Forms Channel with Desirable	Forms Channel with On
Off	No	No	No	No	No
Auto (Passive)	Yes	No	No	Yes	No
Desirable (Active)	Yes	No	Yes	Yes	No
On	No	No	No	No	Yes

Channel—Problems
Channel Fails to Form

- Misconfiguration—auto on one side and on on the other

```
2w3d: %PM-4-ERR_DISABLE: channel-misconfig error detected on Po10, putting Gi4/9 in err-disable state
2w3d: %EC-5-UNBUNDLE: Interface GigabitEthernet4/9 left the port-channel
```

```
C4510-B#show etherchannel summary
Flags: D - down    P - in port-channel
   I - stand-alone s - suspended
   R - Layer3   S - Layer2
   U - in use   f - failed to allocate aggregator
   u - unsuitable for bundling
   w - waiting to be aggregated
   d - default port


Number of channel-groups in use: 1
Number of aggregators:      1

Group Port-channel Protocol  Ports
------+-------------+-----------+-------------------------------
10   Po10(SD)     -    Gi4/9(D)  Gi4/10(D)
```


Channel—Commands

Show Interfaces EtherChannel (Cisco IOS)

- show interfaces port-channel <1-269> etherchannel

```
IOS#show interfaces port-channel 1 etherchannel
Age of the Port-channel       = 00d:00h:03m:10s
Logical slot/port             = 14/1         Number of ports = 2
GC                     = 0x00010001          HotStandBy port = null
Passive port list             = Fa3/45 Fa3/46
Port state             = Port-channel L3-Ag Ag-Inuse

Ports in the Port-channel:

Index   Load    Port    EC state
----------+------------+------------+-------------
 0      55      Fa3/45  desirable-sl
 1      AA      Fa3/46  desirable-sl

Time since last port bundled:  00d:00h:02m:49s  Fa3/46
```


Troubleshooting Layer 2: EtherChannel

```
IOS# show etherchannel load-balance
Source XOR Destination IP address
Native#


IOS-cat6k# remote login switch
Trying Switch ...
Entering CONSOLE for Switch
Type "^C^C^C" to end this session

test etherchannel load-balance interface port-channel number {ip | l4port |
mac} [source_ip_add | source_mac_add | source_l4_port] [dest_ip_add |
dest_mac_add | dest_l4_port]

IOS-cat6k-sp# test etherchannel load-balance interface port-channel 1 ip
1.1.1.1 2.2.2.2
Would select Gi1/1 of Po1


IOS-cat4k# show platform software etherchannel port-channel 1 map ip 1.1.1.1
2.2.2.2
Map port for Ip 1.1.1.1, 2.2.2.2 is Gi1/1(Po1)
NOTE: Software forwarded traffic will use Gi1/1(Po1)
```


Making Sure Spanning Tree Is Forwarding Vlan on Right Interface

```
IOS# show spanning-tree interface gigabitEthernet 1/1

Vlan       Role Sts Cost   Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
VLAN0001     Root FWD 3     128.833 P2p
```

```
Router#sh int g3/1 trunk

Port  Mode    Encapsulation Status   Native vlan
Gi3/1  desirable 802.1q     trunking  1

Port  Vlans allowed on trunk
Gi3/1  1-4094

Port  Vlans allowed and active in management domain
Gi3/1  1-58,60-899,902-998,1000-1001

Port  Vlans in spanning tree forwarding state and not pruned
Gi3/1  1-58,60-899,902-998,1000-1001
```


Am I Seeing Mac Address on Correct Interface? Layer 2: Bridging

```
IOS# show mac-address-table dynamic interface port-channel 1
Codes: * - primary entry

 vlan  mac address     type  learn   qos      ports
------+----------------+--------+-----+---+--------------------------
*  1   0001.c912.7bff  dynamic No     --        Po1
```

```
IOS# show mac-address-table ?
 address     address keyword
 aging-time  aging-time keyword
 count       count keyword
 dynamic     dynamic entry type
 interface   interface keyword
 module      display entries in DFCcard
 multicast   multicast info for selected wildcard
 static      static entry type
 vlan        vlan keyword
 |           Output modifiers
 <cr>
```

```
IOS# show spanning-tree interface gigabitEthernet 1/1

Vlan       Role Sts Cost   Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
VLAN0001     Root FWD 3     128.833 P2p
```


Troubleshooting Layer 3: Route/ARP

```
IOS# show ip route 162.123.74.1
Routing entry for 162.123.74.0/24
 Known via "eigrp 1", distance 170, metric 130816, type external
 Redistributing via eigrp 1
 Last update from 10.1.1.1 on Vlan1, 00:01:13 ago
 Routing Descriptor Blocks:
 * 10.1.1.1, from 10.1.1.1, 00:01:13 ago, via Vlan1
   Route metric is 130816, traffic share count is 1
   Total delay is 5010 microseconds, minimum bandwidth is 1000000 Kbit
   Reliability 255/255, minimum MTU 1500 bytes
   Loading 1/255, Hops 1
```

```
IOS# show ip arp 10.1.1.1
Protocol Address     Age (min) Hardware Addr  Type  Interface
Internet 10.1.1.1        4  0001.c912.7bfc ARPA  Vlan1
```


Troubleshooting: Useful Tools

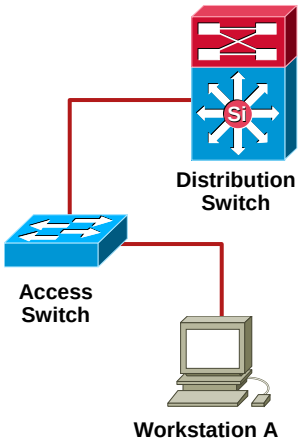
```
IOS# ping
Protocol [ip]:
Target IP address: 10.1.1.1
Repeat count [5]: 1
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.1.1.2
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]: r
Number of hops [ 9 ]: 3
Loose, Strict, Record, Timestamp, Verbose[RV]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
Packet has IP options: Total option bytes= 15, padded length=16
 Record route: <*>
  (0.0.0.0)
  (0.0.0.0)
Reply to request 0 (1 ms). Received packet has options
 Total option bytes= 16, padded length=16
 Record route:
  (10.1.1.2)
  (10.1.1.1)
  (10.1.1.1)  <*>
 End of list
Success rate is 100 percent (1/1), round-trip min/avg/max = 1/1/1 ms
```


Path of Packet Troubleshooting: Useful Tools

```
IOS# ping 14.18.3.200

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 14.18.3.200, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
IOS-cat4k# traceroute mac ip 14.18.3.20 14.18.3.200
Translating IP to mac .....
14.18.3.20 => 0009.435f.86ff
14.18.3.200 => 0003.6b73.9aff

Source 0009.435f.86ff found on IOS-cat4k
IOS-cat4k        (14.18.3.20   ) :   Vl1 => Gi1/1
Destination 0003.6b73.9aff found on IOS-cat4k
Layer2 trace completed.
IOS-cat4k#
IOS-cat4k# traceroute ?
 WORD    Trace route to destination address or hostname
 appletalk AppleTalk Trace
 clns    ISO CLNS Trace
 ip     IP Trace
 ipx    IPX Trace
 mac    Trace Layer2 path between 2 endpoints
 oldvines  Vines Trace (Cisco)
 vines   Vines Trace (Banyan)
 <cr>
```


Path of Packet Troubleshooting Summary

- Baseline applications
  - Define endpoints
  - Map expected path
  - Know features in path
- Change control
- Apply methodical process



What Caused VLANs to Disappear from My Network?

What Is Virtual Trunking Protocol (VTP)?

- Purpose: create/delete VLANs on a centralized switch (server) and have leaf (client) switches learn information
- Runs only on trunks
- Four modes:

  Server: updates clients/servers—stores VLAN info in NVRAM

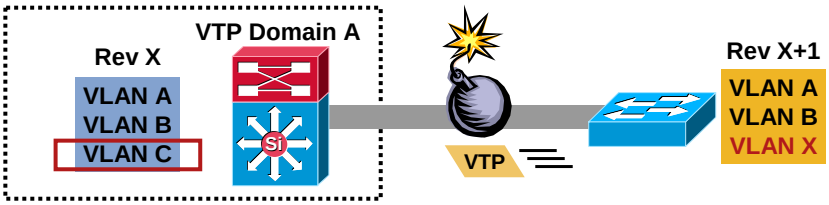
  Client: receive updates—cannot make changes

  Transparent: lets updates pass through

  Off: VTP turned off

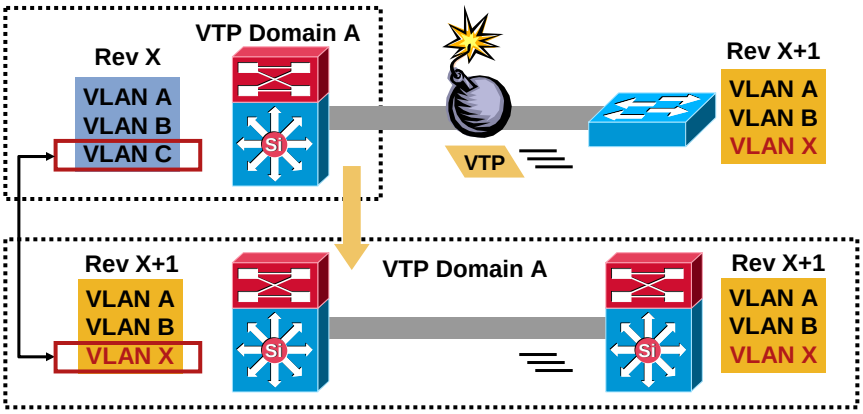
What Is VTP Configuration Rev. No?

VTP Configuration Revision Number Increments for Each VLAN Change



Aha! Now I Know What Happened

VTP Bomb Occurs when a VTP Server with a Higher Revision of the VTP Database (Albeit Loaded with Potentially Incorrect Information) Is Inserted into the Production VTP Domain Causing the Loss of VLAN Information on All Switches in that VTP Domain



VTP—Commands
Show VTP Status (Cisco IOS)

```
Native#show vtp status
VTP Version                     : 2
Configuration Revision          : 5
Maximum VLANs supported locally       : 1005
Number of existing VLANs              : 6
VTP Operating Mode              : Server
VTP Domain Name                       : mydomain
VTP Pruning Mode                      : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xE3 0xE9 0x3A 0x43 0x69 0x2A 0x59
Configuration last modified by 127.0.0.12 at 2-23-02 21:43:44
Local updater ID is 10.118.2.159 on interface Vl1
 (lowest numbered VLAN interface found)
```

VTP—Problem
How Can We Avoid This?

- Reset the configuration revision using domain name
- Change the VTP domain of the new switch to a bogus and non-existent VTP domain name, and then change the VTP domain back to the original name

```
WS-4507#show vtp status
VTP Version                     : 2
Configuration Revision          : 7
Maximum VLANs supported locally : 4094
Number of existing VLANs        : 16
VTP Operating Mode              : Server
VTP Domain Name                 : Networkers2007

WS- 4507(config)#vtp domain test
Domain name set to test.

WS-4507#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 16
VTP Operating Mode              : Server
VTP Domain Name                 : test
```

Zero-ize when Change Domain Name

VTP—Problem
How Can Avoid This?

- Reset the configuration revision using VTP mode
- Change the VTP type from server (the default) to transparent, and then change the mode back to client or server

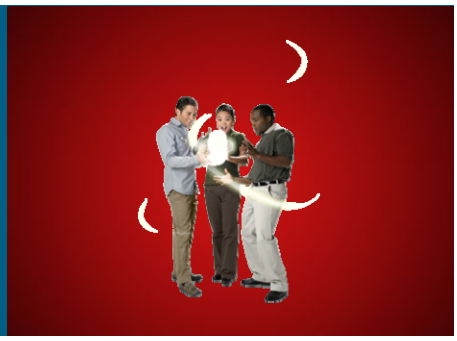
```
WS-6500#show vtp status
VTP Version                     : 2
Configuration Revision          : 4
Maximum VLANs supported locally : 4094
Number of existing VLANs        : 20
VTP Operating Mode              : Server
VTP Domain Name                 : Networkers
.
WS-6500(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.

WS-6500(config)#vtp mode server
Setting device to VTP SERVER mode
WS-6500#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 20
VTP Operating Mode              : Server
VTP Domain Name                 : Networkers
```

Zero-ize When change mode from server to transparent and back to server

Agenda

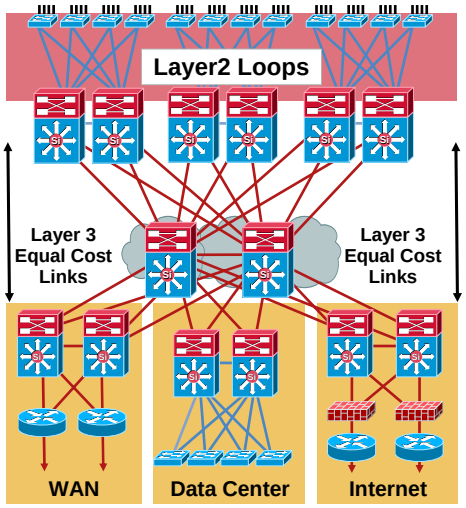
- Session Overview
- Troubleshooting Layer 1, Layer 2, and Layer 3 Connectivity Issues
- Troubleshooting Spanning Tree Protocol
- Security
- Common Issues for High CPU Utilization

Troubleshooting Spanning Tree Protocol

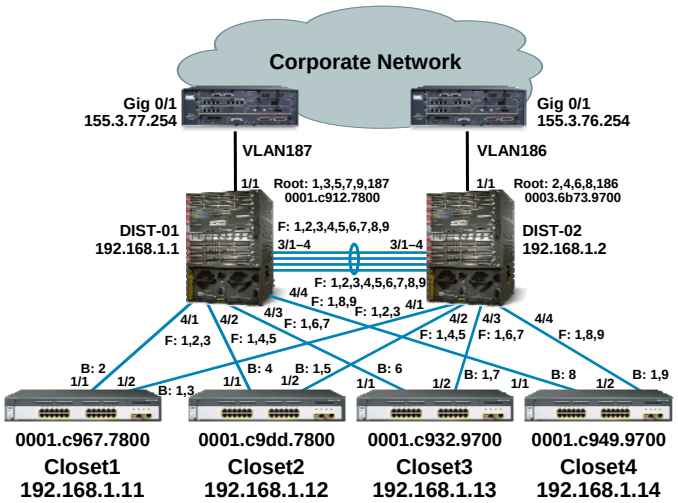


Spanning Tree Protocol Troubleshooting Methodology

- Start now—be proactive
- Divide and conquer
- Document Spanning Tree topology
- Implement Spanning Tree enhancement features
- Develop recovery plan to include data collection for root cause analysis



Spanning Tree Protocol Documenting Spanning Tree Topology



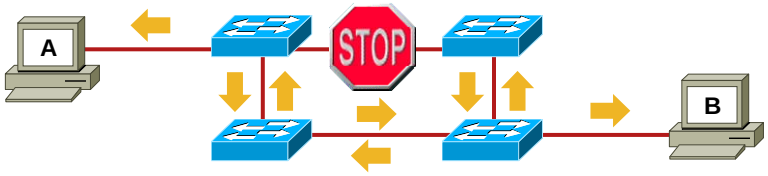
Spanning Tree Best Practice

"How Can I Have a Spanning Tree Loop? I Don't Have Spanning Tree Enabled?"

- Cisco recommends leaving STP-enabled for the following reasons:
  - If there is a loop (induced by mispatching, bad cable, and so on), STP will prevent detrimental effects to the network caused by multicast and broadcast data
  - Protection against an EtherChannel breaking down
  - Most networks are configured with STP, giving it maximum field exposure; more exposure generally equates to stable code
  - Protection against dual attached NICs misbehaving (or bridging enabled on servers)
  - Bridging between wired and wireless
  - The software for many protocols (such as PAgP, IGMP snooping, and trunking) is closely related to STP; running without STP may lead to undesirable results

Spanning Tree Standards and Features

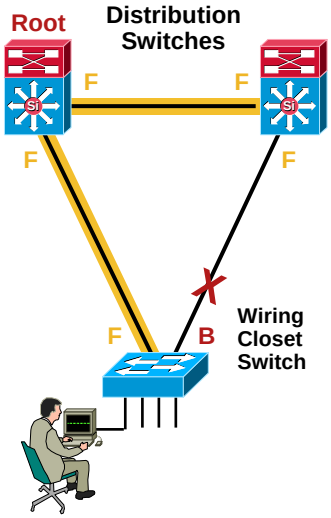
Spanning Tree Toolkit, 802.1D, 802.1s, 802.1w



- 802.1D/1998: legacy standard for bridging and Spanning Tree (STP)
- 802.1D/2004: updated bridging and STP standard; includes 802.1s, 802.1t, and 802.1w
- 802.1s: Multiple Spanning Tree Protocol (MSTP)—maps multiple VLANs into the same Spanning Tree instance
- 802.1t: MAC address reduction/extended system ID—moves some BPDU bits to high-numbered VLANs from the priority field, which constrains the possible values for bridge priority; unique "MAC" per chassis not port
- 802.1w: Rapid Spanning Tree Protocol (RSTP)—improved convergence over 1998 STP by adding roles to ports and enhancing BPDU exchanges
- Cisco Features: Per VLAN Spanning Tree (PVST), PVST+, Rapid PVST, Rapid-PVST+, UplinkFast, BackboneFast, BPDU Guard, RootGuard, LoopGuard, UDLD

Spanning Tree Features

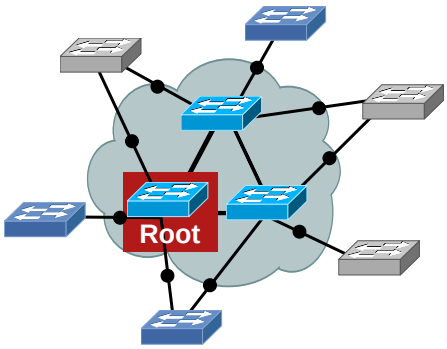
- PortFast*: bypass listening-learning phase for access port
- UplinkFast: three to five seconds convergence after link failure
- BackboneFast: cuts convergence time by Max_Age for indirect failure
- LoopGuard*: prevents alternate or root port from becoming designated in absence of BPDUs
- RootGuard*: prevents external switches from becoming root
- BPDUGuard*: disable PortFast enabled port if a BPDU is received
- BPDUFilter*: do not send or receive BPDUs on PortFast-enabled ports



*Also Supported with MST and Rapid PVST+

What Is Root Guard?

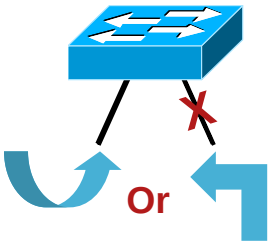
- Root guard forces a Layer 2 LAN interface to be a designated port, and if any device accessible through the interface becomes the root bridge, root guard puts the interface into the root-inconsistent (blocked) state




```
Router(config-if)# switchport
Router(config-if)# spanning-tree guard root

%SPANTREE-2-ROOTGUARDBLOCK: Port 3/3 tried to become non-designated in VLAN 800.
Moved to root-inconsistent state
```

What Is BPDU Guard?

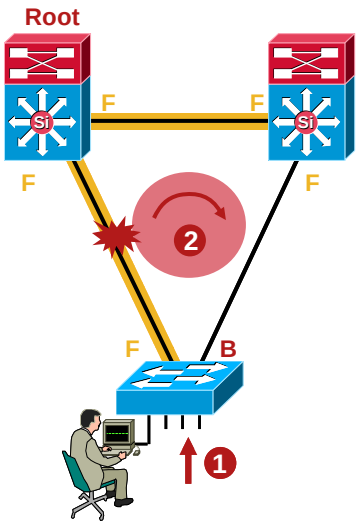
- PortFast BPDU guard can prevent loops by moving PortFast-configured interfaces that receive BPDUs to errdisable, rather than running Spanning Tree across that port
- This keeps ports configured with PortFast from being incorrectly connected to another switch




```
Router(config-if)#spanning-tree portfast
Router(config-if)#spanning-tree bpduguard enable

1w2d: %SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port FastEthernet3/1 with BPDU Guard
enabled. Disabling port.
1w2d: %PM-4-ERR_DISABLE: bpduguard error detected on Fa3/1, putting Fa3/1 in err-disable state
```

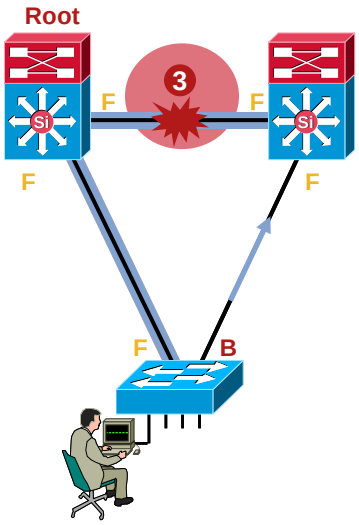

UplinkFast

- Spanning Tree enhancement to reduce failover convergence time
- Used when recovery path is known and predictable
- Enabled on access switch
- Bypasses ‘listening’ and ‘learning’ stages of STP
- Reduces failover time to 2–3 seconds from 30 seconds
- Auto-populates upstream address tables (dummy mcast)
- Default in RSTP



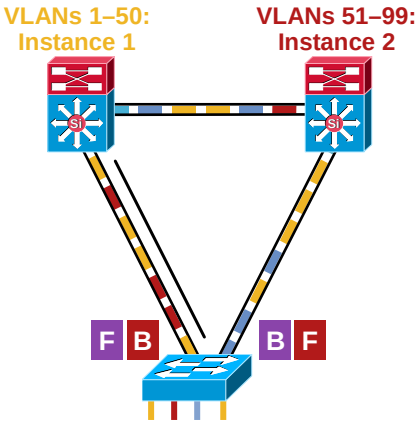
BackboneFast

- Spanning Tree enhancement to reduce failover convergence time
- Targeted at indirect failures
- Enabled on all switches
- Bypasses ‘max-age’
- Reduces failover time to 30 seconds from 50 seconds
- Default in RSTP



802.1s(MST) Overview

- Two active topologies
- All VLANs mapped to one of two topologies
- Lower BPDU counts
- Much less CPU utilization
- Very high scalability
- 802.1s: 12.1(11)EX
- Reduces complexity of numerous topologies



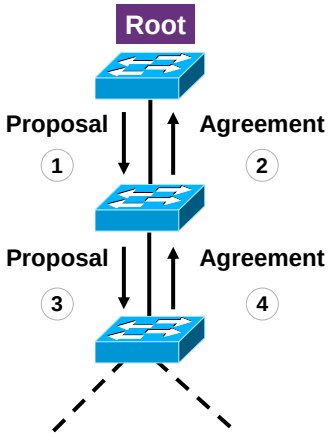
The Problem with Running a Single Instance of STP Is That Any Blocked Link Is Unable to Actively Participate in the Forwarding of Data—thus It Becomes a Wasted Resource—

Spanning Tree Issues

- 802.1D-based Spanning Tree implementations don't converge fast (2 x Fwd_Delay + Max_Age)
- Traditional Spanning Tree is based on network-wide timers
- Cisco's PortFast, UplinkFast, and BackboneFast help, but standardization would be better
- IEEE work resulted in new standard: Rapid Spanning Tree Protocol (RSTP), defined in 802.1w

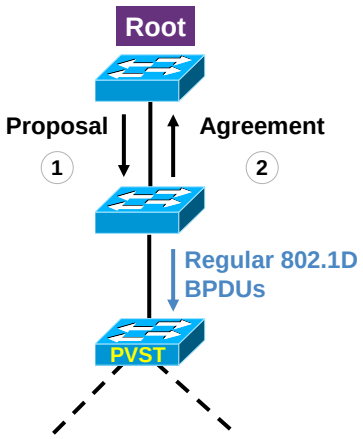
RSTP(802.1w) Overview

- Takes advantage of today's topologies (full-duplex point-to-point links)
- No more network-wide timers when all switches run 802.1w
- Handshake mechanism between bridges
- Proposal-agreement messaging ("I want to become designated—do you agree?")
- Can achieve subsecond convergence



RSTP Overview (Cont.)

- Incorporates mechanisms similar to UplinkFast/ BackboneFast extensions
- Decouples port status/role (i.e., forwarding designated)
- No need to tune timers
- Backwards compatible with 802.1d/PVST+ on a per-port basis



Spanning Tree Protocol

Troubleshooting Commands

```
IOS#show spanning-tree vlan 1 brief

VLAN0001
 Spanning tree enabled protocol ieee
 Root ID          Priority 1
                  Address  0060.8355.7b00
                  Cost     23
                  Port     1 (GigabitEthernet1/1)
                  Hello Time 2 sec Max Age 20 sec   Forward Delay 15 sec

 Bridge ID        Priority 32769 (priority 32768 sys-id-ext 1)
                  Address  0007.0e8f.0880
                  Hello Time 2 sec Max Age 20 sec   Forward Delay 15 sec
                  Aging Time 300

Interface                                          Designated
Name     Port ID  Prio     Cost Sts    Cost  Bridge ID       Port ID
--------------------------         ----------- ------  ------- -------
GigabitEthernet1/1 128.1  128  4 FWD        67 32768 0005.5f33.dc01  128.1
FastEthernet3/48  128.176 128  19 FWD  48 32768 0030.7bdd.5080      128.16
```


Spanning Tree Protocol

Troubleshooting Commands

```
IOS#show spanning-tree vlan 1

VLAN0001
 Spanning tree enabled protocol rstp
 Root ID  Priority  32768
       Address   0030.7b4e.4801
       This bridge is the root
       Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec

 Bridge ID Priority  32768
       Address   0030.7b4e.4801
       Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
       Aging Time 300

Interface    Role Sts Cost   Prio.Nbr Type
---------------- ---- --- --------- -------- ------------------------
Fa2/1      Desg FWD 19    128.129 P2p Peer(STP)
```


Spanning Tree Protocol

Troubleshooting Commands

```
IOS#show spanning-tree summary
Root bridge for: VLAN0010.
Extended system ID is enabled
PortFast BPDU Guard is enabled
EtherChannel misconfiguration guard is disabled
UplinkFast is disabled
BackboneFast is enabled
Default pathcost method used is short

Name      Blocking  Listening  Learning          Forwarding          STP Active
------------------------------------ ------------- ------------- ---------------- --------
VLAN0001      0        0        0                      2          2
VLAN0010      0        0        0                      1          1
VLAN1002      0        0        0                      1          1
VLAN1003      0        0        0                      1          1
VLAN1004      0        0        0                      1          1
VLAN1005      0        0        0                      1          1
----------------------      ------------- ------------- ------------- ----------------

6 VLANs       0        0        0                       7          7
```

Root for Listed VLANs

Spanning Tree Protocol

Logical Ports and STP Instances

- =(Number of non-ATM trunks * number of VLANs on trunk)
- +(Number of ATM trunks * VLANs on trunk *2)
- +Number of nontrunking ports
- [(Number of active VLANs x number of trunks)+ number of access ports]
- *VTP pruning does not remove STP from trunks

	Max Recommended Instances
2950	64 VLANs
3550	128 VLANs
3750-E	128 VLANs
3560	128 VLANs
4000 Sup I or II	1,500 VLANs
4500 Sup II+,IV,V	3,000 VLANs
6000 Sup I	4000 VLANs
6500 Sup II	14,000 VLANs
6500 Sup 32	11,000 VLANs
6500 Sup 720	14,000 VLANs

See Respective Platform Release Notes for More Details

Spanning Tree Protocol

Troubleshooting Commands

```
IOS# show proc cpu
CPU utilization for five seconds: 1%/0%; one minute: 2%; five minutes: 2%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           0         1          0  0.00%  0.00%  0.00%   0 Chunk Manager
  <…some output removed…>
  79           0       256          0  0.00%  0.00%  0.00%   0 mls-msc Process
  80       30508    461976         66  0.40%  0.43%  0.44%   0 Spanning Tree
  81         108     27024          3  0.00%  0.00%  0.00%   0 Ethchnl
  <…some output removed…>
 162          12        41        292  0.00%  0.01%  0.00%   1 Virtual Exec
```

```
IOS# show spanning-tree summary
<…some output removed…>

Name                     Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                       1         0        0          1          2
<…some output removed…>
VLAN1005                       0         0        0          1          1
---------------------- -------- --------- -------- ---------- ----------
282 vlans                      1         0        0        282        283
```

Number of Spanning Tree Instances

Spanning Tree Protocol

Troubleshooting Topology Change

```
IOS#show spanning-tree vlan 1 detail

 VLAN0001 is executing the ieee compatible Spanning Tree protocol
 Bridge Identifier has priority 32768, address 0005.7495.9101
 Configured hello time 2, max age 20, forward delay 15
 Current root has priority 32768, address 0001.c912.7800
 Root port is 70 (GigabitEthernet2/6), cost of root path is 4
 Topology change flag not set, detected flag not set
 Number of topology changes 4 last change occurred 02:17:20 ago
     from Port-channel1
 Times: hold 1, topology change 35, notification 2
     hello 2, max age 20, forward delay 15
 Timers: hello 0, topology change 0, notification 0, aging 300

 Port 70 (GigabitEthernet2/6) of VLAN0001 is forwarding
  Port path cost 4, Port priority 128, Port Identifier 128.70.
  Designated root has priority 32768, address 0001.c912.7800
  Designated bridge has priority 32768, address 0001.c912.7800
  Designated port id is 128.70, designated path cost 0
  Timers: message age 2, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  Link type is point-to-point by default
  BPDU: sent 7, received 4162

 Port 833 (Port-channel1) of VLAN0001 is blocking
  Port path cost 4, Port priority 128, Port Identifier 128.833.
  Designated root has priority 32768, address 0001.c912.7800
  Designated bridge has priority 32768, address 0001.c912.7800
  Designated port id is 128.769, designated path cost 0
  Timers: message age 1, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  Link type is point-to-point by default
  BPDU: sent 4, received 134836
```

Don't Forget PortFast

Spanning Tree Protocol

Troubleshooting Commands

- Track down source of changes

  TCN, logs, network management

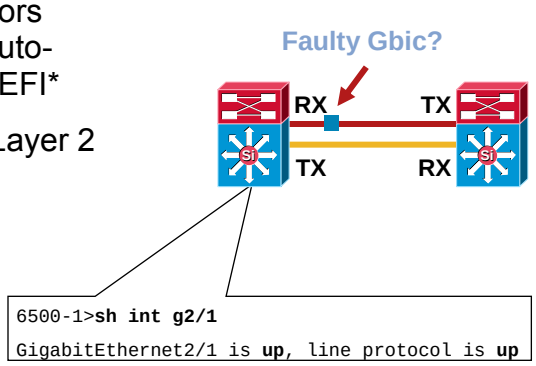
- Protect against the changes

  UDLD, PortFast, network management

Can Unidirectional Link Detection (UDLD) Help to Avoid Spanning Tree Loop?

What Is UDLD?

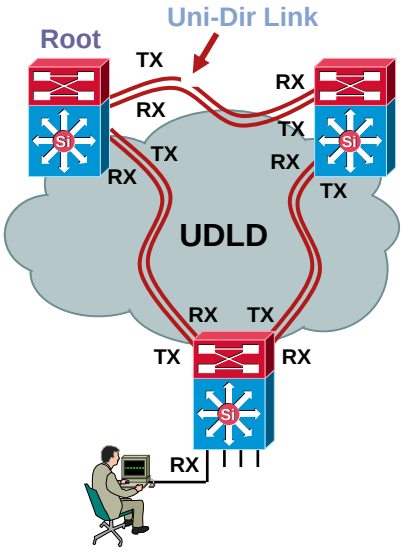
- Detects one-way logical connectivity
- Physical-layer errors are detected by auto-negotiation and FEFI*
- Detects faults at Layer 2



*FEFI: Far-End Fault Indication

Why Are Uni-Dir Links a Bad Thing?

- Root xmits BPDUs
- Neighbor doesn't receive them and thinks the root is dead ▷now claims it's the new root
- Bottom switch opens up its blocked port ▶loop in the network
- Network goes down, troubleshooting very difficult



Show UDLD

```
IOS# show udld gigabitEthernet 1/1
Interface Gi1/1
---
Port enable administrative configuration setting: Enabled / in aggressive mode
Port enable operational state: Enabled / in aggressive mode
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single neighbor detected
Message interval: 15
Time out interval: 5

  Entry 1
  ---
  Expiration time: 35
  Device ID: 1
  Current neighbor state: Bidirectional
  Device name: SAL06090FCJ
  Port ID: Gi1/1
  Neighbor echo 1 device: SAD044204Y8
  Neighbor echo 1 port: Gi1/1

  Message interval: 5
  CDP Device name: ls-7603-16a
```

%PM-4-ERR_DISABLE: **udld error detected on Gi1/0/25, putting Gi1/0/25 in err-disable state**

Spanning Tree: Commands

UDLD Enable/Aggressive

- Native can have standard or aggressive configured globally and per port exceptions

```
IOS(config)#udld enable
IOS(config)#interface gigabitEthernet 1/1
IOS(config-if)#udld aggressive
```


Spanning Tree Protocol

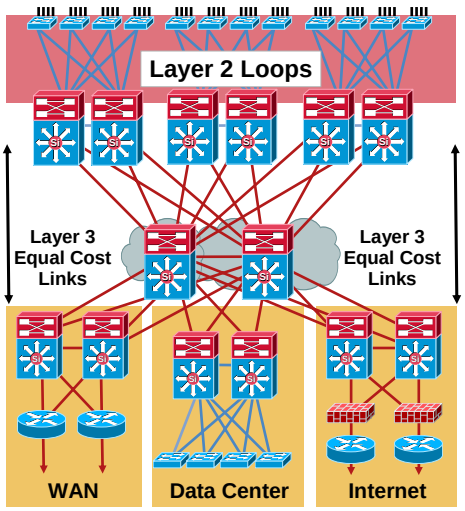
STP Loop Recovery

- Do not power off switches—pull/shut redundant links
- If possible, initially disable ports that should be blocking
- Check and physically remove the connections to the ports that should be blocking
- Set up remote access to your network and call TAC

Spanning Tree Protocol

Troubleshooting Summary

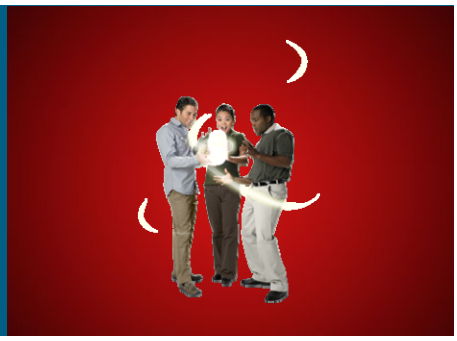
- **Be proactive!**
- Use the diagram of the network
- Know where the root is
- Know where redundancy is
- Minimize the number of blocked ports
- Keep STP even if it is unnecessary
- Have modem access to key devices, call TAC



Agenda

- Session Overview
- Troubleshooting Layer 1, Layer 2, and Layer 3 Connectivity Issues
- Troubleshooting Spanning Tree Protocol
- Troubleshooting Security
- Troubleshooting High CPU Utilization

Troubleshooting Security



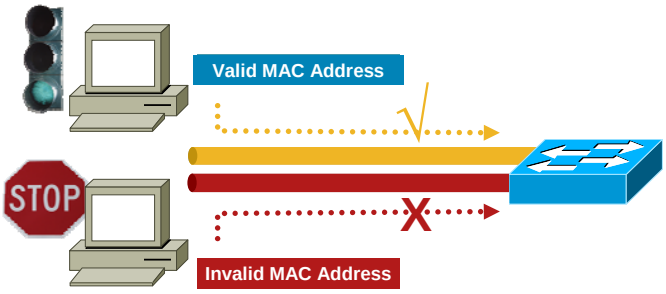
Port Security

- What it does:

  Limits the number of MAC addresses that are able to connect to a switch and ensures only approved MAC addresses are able to access the switch

- Benefit:

  Ensures only approved users can log on to the network



Port Security Details

- Configuration options

```
Interface FastEthernet1/1
switchport port-security
switchport port-security maximum 3
switchport port-security aging time 1
switchport port-security violation restrict
switchport port-security aging type inactivity
```

- Default action—shutdown

```
1w2d: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa3/1, putting Fa3/1 in err-disable state
1w2d: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred,
caused by MAC address 0005.dccb.c941 on port FastEthernet3/1.
```


Port Security Details

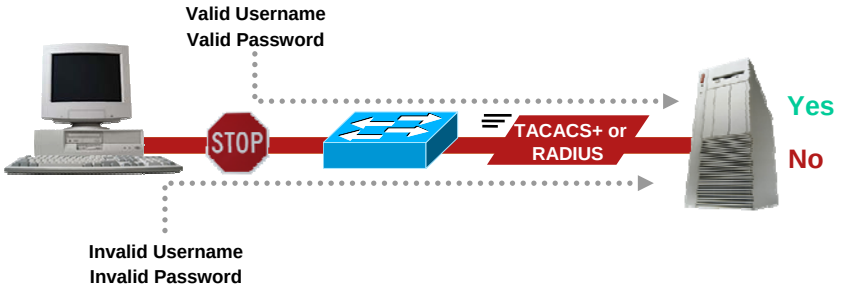
```
Switch_B#sh port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)
--------------------------------------------------------------------------
      Fa3/5          3072         3072                  0         Restrict
     Fa3/10            10            2              19172         Restrict
--------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 3072
Max Addresses limit in System (excluding one mac per port) : 3072
Switch_B#
```


```
Switch_B#sh port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)
--------------------------------------------------------------------------
      Fa3/5          3072         3072                  0         Restrict
     Fa3/10            10            2              19172         Restrict
--------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 3072
Max Addresses limit in System (excluding one mac per port) : 3072
Switch_B#
```


Understanding 802.1x

How It Works

- Each person trying to enter the network must receive authorization based on their personal username and password



Client Accessing Switch

TACACS+ or RADIUS Server

Understanding 802.1x

```
! enable AAA
aaa new-model
! use AAA for 802.1x only (optional)
aaa authentication login default none
aaa authentication dot1x default group radius
! set IP address of radius server
radius-server host 10.48.66.102
! radius server key
radius-server key Cisco
! enable 802.1x
dot1x system-auth-control
! L3 interface for accessing RADIUS server
interface Vlan1
 ip address 10.48.72.177 255.255.254.0
! RADUIS server is behind this L2 port
interface gi2/1
 switchport
 switchport mode access
 switchport access vlan 1
! enable 802.1x on the interface
interface gi2/16
 switchport
 switchport mode access
 dot1x port-control auto
end
```

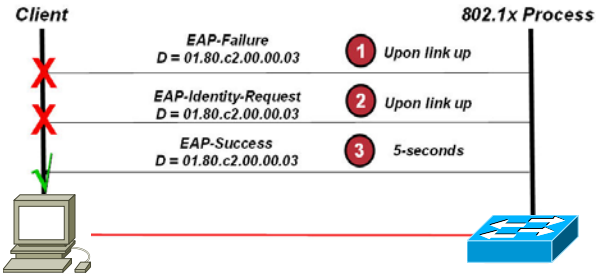
```
Switch#sh dot1x
Sysauthcontrol = Enabled
Dot1x Protocol Version = 1
Dot1x Oper Controlled Directions =
Both
Dot1x Admin Controlled Directions =
Both
```

```
Switch#sh dot1x interface g2/16
AuthSM State    = HELD
BendSM State    = IDLE
PortStatus     = UNAUTHORIZED
MaxReq       = 2
MultiHosts     = Disabled
Port Control    = Auto
QuietPeriod     = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod    = 3600 Seconds
ServerTimeout    = 30 Seconds
SuppTimeout     = 30 Seconds
TxPeriod      = 30 Seconds
```

- Debugging commands:
  - debug dot1x event
  - debug radius

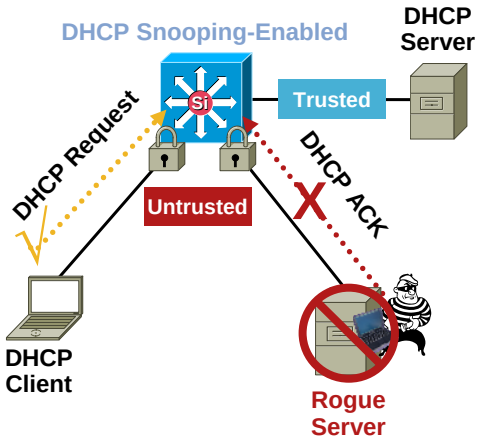
PC Is Authenticated in Correct Vlan but Have IP Address from DHCP in Guest Vlan

- Tx-period: Default is 30 sec; switch expects response from client before retransmitting EAP-Identity-Request frame again
- Max-reauth-req: Default is 2
- Configuring the minimum values, a switch port can be deployed into the guest VLAN in 5 seconds if our timers are very aggressive
- DHCP and the 802.1x processes are completely asynchronous



DHCP Snooping

- What it does:
  - Switch forwards only DHCP requests from untrusted access ports, drops all other types of DHCP traffic; allows only designated DHCP ports or uplink ports trusted to relay DHCP messages
  - Builds a DHCP binding table containing client IP address, client MAC address, port, VLAN number
- Benefit:
  - Eliminates rogue devices from behaving as the DHCP server



DHCP Snooping

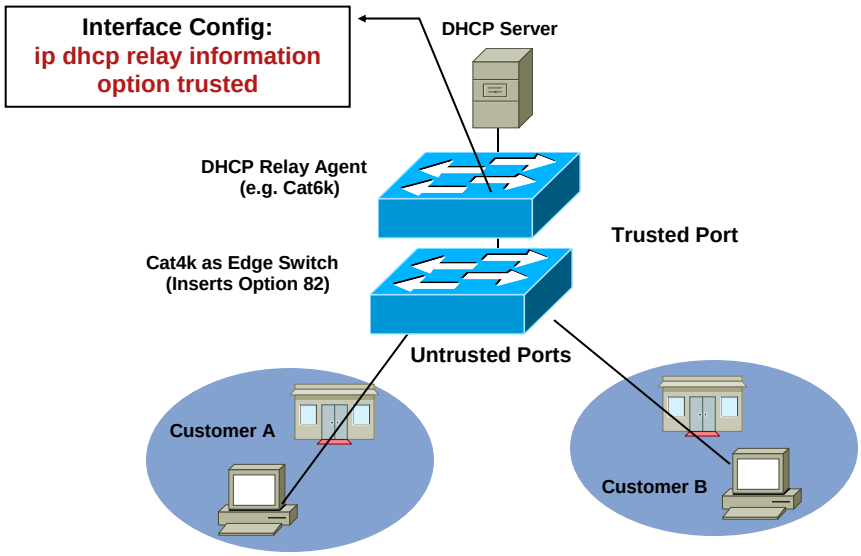
```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10 100
Switch(config)# int f6/1
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)# ip dhcp snooping limit rate <rate>
```

```
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:1
Insertion of option 82 is enabled
Interface        Trusted   Rate limit (pps)
-------------------   -------   ----------------
FastEthernet2/1     yes     100

Switch# show ip dhcp snooping binding
MacAddress   IpAddress Lease(sec) Type   VLAN Interface
------------------   --------------- ----------     -------     ---- ----------------
0000.0100.0201 10.0.0.1    1600     dynamic  100 Fa2/1
```

What We Should Know Before We Start Troubleshooting?

- Configured to rate-limit the incoming DHCP packets
- Points to note:
  - DHCP request broadcasted to only trusted ports in that vlan
  - DHCP responses unicasted to the client port only
  - DHCP responses on untrusted port is dropped
- Option 82 enabled by default, when dhcp snooping is enabled
- Option 82 DHCP pkt is dropped when rcvd on untrusted port

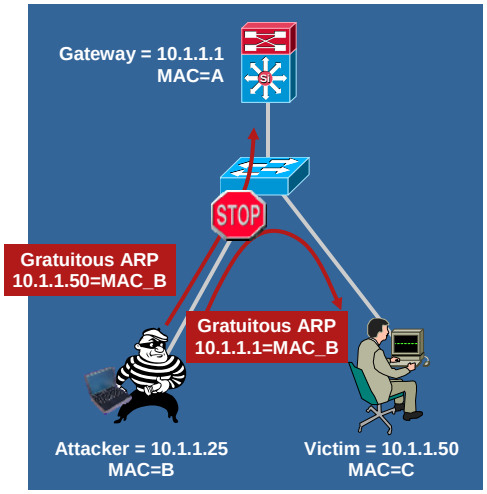
When Upstream Switch Is a Relay Agent:



Dynamic ARP Inspection

Dynamic ARP Inspection Protects Against ARP Poisoning

- Uses the DHCP-snooping binding table
- Tracks MAC to IP from DHCP transactions
- Rate-limits ARP requests from client ports; stop port scanning
- Drop BOGUS ARPs; prevents ARP poisoning/ MIM attacks



Dynamic ARP Inspection

```
Switch(config)#ip arp inspection vlan 1
Switch(config)#ip arp inspection filter static-hosts vlan 1

Switch(config)#arp access-list static-hosts
Switch(config-arp-nacl)#permit ip host 10.1.1.5 mac any
```

```
Switch#show ip arp inspection vlan 1

Source Mac Validation   : Disabled
Destination Mac Validation : Disabled
IP Address Validation   : Disabled

 Vlan   Configuration  Operation  ACL Match    Static ACL
 ----   -------------  ---------  ---------    -----------
 1      Enabled        Active     static-hosts  No

 Vlan   ACL Logging   DHCP Logging
 ----   -----------   -------------
 1      Deny          None
```


Dynamic ARP Troubleshooting

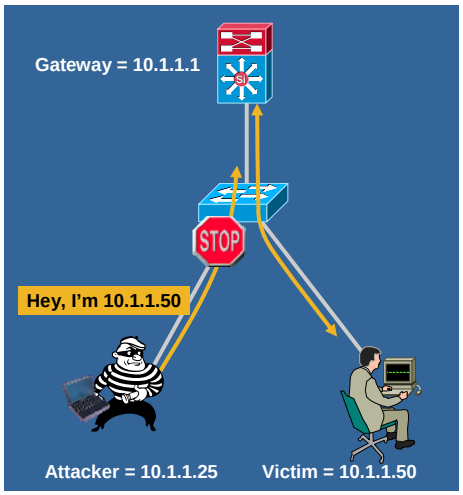
```
Switch_A# sh ip arp inspection statistics
Vlan     Forwarded      Dropped    DHCP Drops     ACL Drops
----     ---------      -------    ----------     ---------
  5        200            10          5              5

Vlan   DHCP Permits   ACL Permits   Source MAC Failures
----   ------------   -----------   -------------------
  5        125           75                0

Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
----   -----------------   ----------------------   ---------------------
  5          0                     0                        0
Switch_A#
```


IP Source Guard

Protection Against Spoofed IP Addresses

IP Source Guard Protects Against Spoofed IP Addresses

- Uses the DHCP-snooping binding table
- Tracks IP address to port associations
- Dynamically programs port ACL to drop traffic not originating from IP address assigned via DHCP



IP Source Guard

```
Switch(config)# ip dhcp snooping vlan 10 20
Switch(config)# interface fa6/1
Switch(config-
if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 10
Switch(config-if)# switchport trunk allowed vlan 11-20
Switch(config-if)# no ip dhcp snooping trust
Switch(config-if)# ip verify source vlan dhcp-snooping

Switch# sh ip verify source interface f6/1
Interface Filter-type Filter-mode IP-address    Mac-
address    Vlan
--------- ----------- ----------- --------------- ----
------------- ----------
Fa6/1          ip-mac    active          10.1.1.3
00:04:9A:49:E5:FF       10
Fa6/1          ip-mac    active         deny-all
11-20
```


Troubleshooting Commands: IPSG in IP Mode

```
Switch_A# sh ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
10.1.1.3         0063.6973.636f.2d30.    Mar 30 2007 02:50 AM    Automatic
                 3030.342e.3961.3439.
                 2e65.3566.662d.566c.
                 35
Switch_A# sh ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  ----------
----------
00:04:9A:49:E5:FF   10.1.1.3         82522       dhcp-snooping  10     FastEthernet6/1
Total number of bindings: 1

Switch_A# sh ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  -------
---
Fa6/1       ip           active       10.1.1.3                            10
```


Access Control Lists

- What it does:
  - Allows or denies access based on the source or destination address
  - Restricts users to designated areas of the network, blocking unauthorized access to all other applications and information
- Benefit:
  - Prevents unauthorized access to servers and applications
  - Allows designated users to access specified servers

Types of ACLs

- Router ACL (RACL)
- VLAN ACL (VACL)
- Port-based ACL (PACL)

Applying a RACL/PACL

```
interface Vlan4
 ip address 4.4.4.1 255.255.255.0
end
```

```
Switch#show ip access-lists
Extended IP access list 101
deny tcp host 200.200.200.1 any neq 80 (5 matches)
permit ip any any (11915 matches)
```

```
Switch(config)#interface vlan 4
Switch(config-if)#ip access-group 101 in
Switch(config-if)#
```

```
Switch(config)#interface fa 4/23
Switch(config-if)#swichport access vlan 4
Switch(config-if)#ip access-group 101 in
```

Counters

RACL

PACL

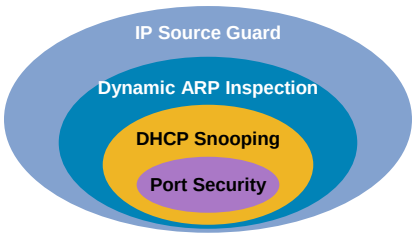
VLAN ACL Map (VACL)

```
mac access-list extended drop-appletalk
 permit any any protocol-family
appletalk

ip access-list extended ip2
 permit ip any any

vlan access-map vacl-100 15
action drop
match mac address drop-appletalk
vlan access-map vacl-100 20
 action forward
 match ip address ip2
!
vlan filter vacl-100 vlan-list 201
```

- VACLs match all packets on the VLAN
- VACLs may have IP-based and MAC-based ACLs, with implicit deny all at the end
- This example will permit IP and drop all AppleTalk frames on VLAN 201

Catalyst Integrated Security Features

Summary Cisco IOS



- Port security prevents MAC flooding attacks
- DHCP snooping prevents client attack on the switch and server
- Dynamic ARP inspection adds security to ARP using DHCP snooping table
- IP source guard adds security to IP source address using DHCP snooping table
- All features work on switchports

```
ip dhcp snooping
ip dhcp snooping vlan 2-10
ip arp inspection vlan 2-10
!
interface fa3/1
switchport port-security
switchport port-security max 3
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
ip arp inspection limit rate 100
ip dhcp snooping limit rate 100
no ip dhcp snooping trust
ip verify source vlan dhcp-snooping
Interface gigabit1/1
ip dhcp snooping trust
ip arp inspection trust
```

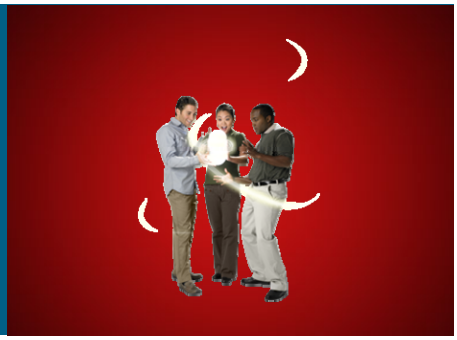

NAC Sessions

- SEC-2041: Deploying Cisco NAC Appliance for Diverse Access Methods
- SEC-3040: Troubleshooting NAC
- SEC-3041: Troubleshooting Cisco NAC Appliance
- SEC-2030: Deploying Network-Based Intrusion Prevention Systems
- SEC-2031: Deploying Host-Based Intrusion Prevention Technology
- SEC-3030: Troubleshooting Intrusion Detection Systems

Agenda

- Session Overview
- Troubleshooting Layer 1, Layer 2, and Layer 3 Connectivity Issues
- Troubleshooting Spanning Tree Protocol
- Security
- Common Issues for High CPU Utilization

Troubleshooting High CPU Utilization



Common Reasons for High CPU Utilization

- Packets are process switched
- If switch cannot forward packet in hardware because fragmentation issue
- Packets coming with IP options
- Expired TTL
- ACL configured with log keyword
- ACL failed to get programmed in hardware
- IP routes failed to get programmed in hardware

Issues Encountered with High CPU Utilization

- Degrade performance of network
- On router HSRP status may flap from active to standby
- Router will lose its routing neighbors
- May fail to access the switch via SSH or Telnet and many more

Basic Commands to Understand CPU Utilization: Know the CPU Baseline

```
CAT6K-STATIC#show processes cpu sorted

CPU utilization for five seconds: 71%/70%; one minute: 0%; five minutes: 0%
  PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
  239         32        59        542  0.15%  0.01%  0.00%   1 Virtual Exec
118      388712   1264243        307  0.07%  0.01%  0.00%   0 QOS Stats Export
                    ------------- Snip------------
```

71% Is the average total utilization during the last 5 seconds (interrupts + processes)

70% Is the average utilization due to interrupts, during the last 5 seconds
Use show proc cpu history cmd to view a more detailed history of CPU utilization "history"

```
CAT6K-STATIC#show interface vlan 1
Vlan1 is up, line protocol is up
Hardware is EtherSVI, address is 000c.cf2b.9c00 (bia 000c.cf2b.9c00)
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
Input queue: 0/2000/9986/890(size/max/drops/flushes); Total output drops: 0
        ------------- Snip------------
5 minute input rate 7890000 bits/sec, 4560 packets/sec
5 minute output rate 7500 bits/sec, 10 packets/sec
```


Basic Commands to Understand CPU Utilization

```
CAT6K-STATIC#show interface switching
Vlan1
        Throttle count        0
      Drops        RP        0        SP        0
  SPD Flushes    Fast        0        SSE       0
  SPD Aggress    Fast        0
 SPD Priority    Inputs     63     Drops        0
    Protocol      Path    Pkts In   Chars In   Pkts Out    Chars Out
         Other    Process       6       462          0            0
           Cache misses         0
                   Fast         0         0          0            0
              Auton/SSE         0         0          0            0
           IP    Process       652     57635        603         8654
           Cache misses         0
                   Fast       905     66904        902        53982
              Auton/SSE         0         0        905        70484
           ARP    Process     30608   1836480        111        12432
             Cache misses        0
                   Fast         0         0          0            0
              Auton/SSE         0         0          0            0
```


What Should Be Our Approach

- A local span session can be configured to capture the traffic for analysis
- Check log for any error messages which tell us about resource issues
- Make sure Spanning Tree is stable
- We can capture traffic going to CPU with help of TAC on Cat6500/Cat4500

Storm Control Can Help to Protect CPU

- Configuring traffic storm control to avoid packets flood the LAN, creating excessive traffic and degrading network performance
- `Router(config-if)# storm-control broadcast level level[.level]`

```
WS-C3750-24TC-L-A(config)#storm-control
broadcast level pps 1000 500
```

- `Router(config-if)# storm-control multicast level level[.level]`

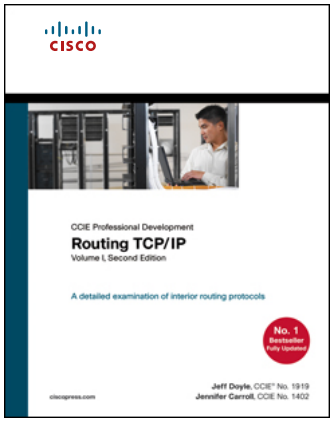
```
WS-C3750-24TC-L-A(config-if)#storm-control
multicast level bps 100000 1000
```


Best Practices

- Following building codes results in solid well constructed homes and buildings
- Following LAN switching “building code” results in resilient well-constructed and stable switched networks
- Practices for Cisco Catalyst® 4500/4000, 5500/5000, and 6500/6000 Series Switches, Running Cisco CatOS/IOS Configuration and Management
- http://www.cisco.com/warp/customer/473/103.html
- http://www.cisco.com/warp/customer/473/185.html

Recommended Reading

- Continue your Cisco Live learning experience with further reading from Cisco Press
- Check the Recommended Reading flyer for suggested books



Available Onsite at the Cisco Company Store

Complete Your Online Session Evaluation

- Give us your feedback and you could win fabulous prizes. Winners announced daily.
- Receive 20 Passport points for each session evaluation you complete.
- Complete your session evaluation online now (open a browser through our wireless network to access our portal) or visit one of the Internet stations throughout the Convention Center.

Don't forget to activate your Cisco Live virtual account for access to all session material on-demand and return for our live virtual event in October 2008.

Go to the Collaboration Zone in World of Solutions or visit www.cisco-live.com.

References

http://www.cisco.com

- Catalyst 4000 Troubleshooting TechNotes

  http://www.cisco.com/en/US/products/hw/switches/ps663/prod_tech_notes_list.html
- High CPU Utilization on Cisco IOS Software-Based Catalyst 4500 Switches

  Document ID: 65591
- Best Practices for Catalyst 6500/6000 Series and Catalyst 4500/4000 Series Switches Running Cisco IOS Software

  Document ID: 24330
- Catalyst 4500 System Message Guide
- DOM Compatibility Matrix

  http://www.cisco.com/en/US/docs/interfaces_modules/transceiver_modules/compatibility/matrix/OL_8031.html

  http://www.cisco.com/en/US/docs/interfaces_modules/transceiver_modules/compatibility/matrix/OL_6974.html

  http://www.cisco.com/en/US/docs/interfaces_modules/transceiver_modules/compatibility/matrix/OL_6981.html
- Cisco Transceiver Data Sheets

  http://www.cisco.com/en/US/products/hw/modules/ps5455/products_data_sheets_list.html