Troubleshooting Catalyst® Switches—Part 1
Session CDC-301

Agenda

• Terminology
• The Layer 2 Basics
• Spanning Tree
• Layer 2 Quality of Service
• Layer 2 Access Control Lists
Trunk and EtherChannel—Terminology

- A trunk is a link between two devices that carries multiple VLANs simultaneously
  - ISL—Inter-Switch Link
  - IEEE 802.1q—Used on Gigabit and optionally Fast Ethernet ports
- EtherChannel is a method of grouping multiple physical links between two devices into a single logical link
ToS, CoS, and DSCP—Terminology

- Type of Service (ToS)—is a three bit value used in the IP header
- Class of Service (CoS)—is a three bit value used in a 802.1q, 802.1p or ISL Header
- Differentiated Services Code Point (DSCP)—is a six bit value used internally to the Catalyst switch, mapped to and from CoS values in packets

Policing and Shaping—Terminology

- Policing usually drops excessive traffic, but can change Quality of Service (QoS) marking as well
- Shaping typically delays excess traffic, using a buffer or queuing mechanism, to hold packets and shape the flow when the data rate exceeds expectations
Agenda

- Terminology
- The Layer 2 Basics
- Spanning Tree
- Layer 2 Quality of Service
- Layer 2 Access Control Lists

Port Startup Delays—Problem

- On Link-up it takes up to 45 seconds for packets to flow
- Three things contribute to delay in packet forwarding on link up
  - Spanning Tree
  - Trunking Auto-Negotiation
  - Ethernet Channeling Auto-Negotiation
Port Startup Delays—Solution

- To resolve all three causes of port startup delay, the following command is a macro that enables portfast, and disables channeling and trunking:

```plaintext
Switch> (enable) set port host 2/6-7
Port(s) 2/6-7 channel mode set to off.
Spantree ports 2/6-7 fast start enabled.
Port(s) 2/6-7 trunk mode set to off.
```

Trunk Fails to Form—Problem

- Default setting for trunking is auto mode, yet no trunk when adjacent switches connected

```plaintext
Switch> (enable) show cdp neighbors detail
Device-ID: 066505512
Device Addresses:
  IP Address: 10.6.1.234
  Holdtime: 152 sec
Capabilities: TRANSPARENT_BRIDGE SR_BRIDGE SWITCH
Version:
  WS-C5505 Software, Version McpSW: 3.2(6) NmpSW: 3.2(6)
  Copyright (c) 1995-1999 by Cisco Systems
Platform: WS-C5505
Port-ID (Port on Device): 1/1
Port (Our Port): 1/1
Switch> (enable) show trunk
No ports trunking.
```
# Trunk Fails to Form—Solution

<table>
<thead>
<tr>
<th>Uses DTP</th>
<th>Forms Trunk with Off</th>
<th>Forms Trunk with Auto</th>
<th>Forms Trunk with Desirable</th>
<th>Forms Trunk with On</th>
<th>Forms Trunk with Negotiate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Auto</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Desirable</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>On</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Negotiate</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Switch> (enable) sh trunk

* - indicates vtp domain mismatch

<table>
<thead>
<tr>
<th>Port</th>
<th>Mode</th>
<th>Encapsulation</th>
<th>Status</th>
<th>Native vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/1</td>
<td>auto</td>
<td>isl</td>
<td>trunking</td>
<td>1</td>
</tr>
</tbody>
</table>

Port Vlans allowed on trunk

<table>
<thead>
<tr>
<th>Port</th>
<th>1-1005</th>
</tr>
</thead>
</table>

Port Vlans allowed and active in management domain

<table>
<thead>
<tr>
<th>Port</th>
<th>2/1</th>
</tr>
</thead>
</table>

Port Vlans in spanning tree forwarding state and not pruned

<table>
<thead>
<tr>
<th>Port</th>
<th>2/1</th>
</tr>
</thead>
</table>

## Trunking—Commands

- **Show Trunk** tells the state of the trunk

Switch> (enable) sh trunk

* - indicates vtp domain mismatch

<table>
<thead>
<tr>
<th>Port</th>
<th>Mode</th>
<th>Encapsulation</th>
<th>Status</th>
<th>Native vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/1</td>
<td>auto</td>
<td>isl</td>
<td>trunking</td>
<td>1</td>
</tr>
</tbody>
</table>

Port Vlans allowed on trunk

<table>
<thead>
<tr>
<th>Port</th>
<th>1-1005</th>
</tr>
</thead>
</table>

Port Vlans allowed and active in management domain

<table>
<thead>
<tr>
<th>Port</th>
<th>2/1</th>
</tr>
</thead>
</table>

Port Vlans in spanning tree forwarding state and not pruned

<table>
<thead>
<tr>
<th>Port</th>
<th>2/1</th>
</tr>
</thead>
</table>
EtherChannel Fails to Form—Problem

- Default setting for EtherChannel is auto mode, yet no EtherChannel forms when adjacent switches are connected

```
lc5505-11a (enable) show cdp neighbor
* - indicates vlan mismatch.
# - indicates duplex mismatch.
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Device-ID</th>
<th>Port-ID</th>
<th>Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/1</td>
<td>066512851</td>
<td>2/1</td>
<td>WS-C5505</td>
</tr>
<tr>
<td>2/2</td>
<td>066512851</td>
<td>2/2</td>
<td>WS-C5505</td>
</tr>
</tbody>
</table>

Switch> (enable) show channel

Channel Id Ports

Switch> (enable)

EtherChannel Fails to Form—Solution

<table>
<thead>
<tr>
<th>Uses PAgP</th>
<th>Forms Channel with Off</th>
<th>Forms Channel with Auto</th>
<th>Forms Channel with Desirable</th>
<th>Forms Channel with On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Auto</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Desirable</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>On</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
EtherChannel—Commands

• Show channel tells what is going on with FEC

Switch> (enable) show channel
Channel Id Ports
----------- -----------------------------------------------
801 2/1-4

EtherChannel—Disable vs. Disabled

• If port is in DISABLE state then PAgP elected to shut the port because it detected a loop
• If port is in DISABLED state then the port has been administratively shutdown
• DISABLE is a clue that something is configured wrong
Agenda

- Terminology
- The Layer 2 Basics
- Spanning Tree
- Layer 2 Quality of Service
- Layer 2 Access Control Lists

Spanning Tree—Problem

- Bridge loops in the layer 2 redundant network causes attached routers to have high CPU, and other links in the network to be filled with traffic
- Effectively makes the network unusable
Spanning Tree—How It Works

Root Ports: Port with Least Cost Path to the Root Bridge
Nondesignated Ports: Ports in Blocking
Designated Ports: Ports Selected for Forwarding
Direction of BPDU Flow

Spanning Tree—How It Works Parameters

- Network parameters
  - Hello interval
  - Forward delay
  - Max age
  - Bridge priority (per bridge)
- Port-specific parameters
  - Port cost
  - Port priority
Spanning Tree—Commands

```
Switch> (enable) sh spantree 1
VLAN 1
Spanning tree mode          PVST+
Spanning tree type          ieee
Spanning tree enabled

Designated Root             00-60-83-55-7b-00
Designated Root Priority    100
Designated Root Cost        100
Designated Root Port        3/1
Root Max Age               20 sec
Hello Time                 2 sec
Forward Delay              15 sec

Bridge ID MAC ADDR          00-d0-06-24-6c-00
Bridge ID Priority         32768
Bridge Max Age             20 sec
Hello Time                 2 sec
Forward Delay              15 sec

Port Vlan Port-State Cost Prio Portfast Channel_id
---- ---- ---------------------- ---- -------- ----------
1/1 1    not-connected 4 32    disabled 0
3/1 1    forwarding 100 32    enabled 0
```

Spanning Tree—Solution

Root Bridge

I’m the Root!
Spanning Tree—Solution

Root Bridge

- The root of the tree should be in the very core of the network; typically server farm
- Use the set spantree root macro on the root switch

Spanning Tree—Commands

- A macro that sets the bridge priority parameter to 8192 for the specified VLANs, 16384 for secondary roots
- Root bridge dictates hello interval for entire network

Switch> (enable) set spantree root 1 dia 2 hello 2
VLAN 1 bridge priority set to 8192.
VLAN 1 bridge max aging time set to 10.
VLAN 1 bridge hello time set to 2.
VLAN 1 bridge forward delay set to 7.
Switch is now the root switch for active VLAN 1.
Spanning Tree—Solution
UDLD

- Fiber links can become Uni-Directional for many reasons, and UDLD will provide protection for most of those reasons

- For the best protection use UDLD Aggressive Mode

Switch> (enable) set udld enable
UDLD enabled globally
Switch> (enable) set udld aggressive-mode enable 1/1
Aggressive UDLD enabled on port 1/1.
Switch> (enable) sh udld port

<table>
<thead>
<tr>
<th>Port</th>
<th>Admin Status</th>
<th>Aggressive Mode</th>
<th>Link State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>enabled</td>
<td>enabled</td>
<td>undetermined</td>
</tr>
<tr>
<td>1/2</td>
<td>enabled</td>
<td>disabled</td>
<td>undetermined</td>
</tr>
</tbody>
</table>

Spanning Tree—Commands
UDLD

- UDLD is a global configuration, but Aggressive Mode is configured per port
Spanning Tree—Solution
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

Spanning Tree—Feature
Uplinkfast

- A feature that when enabled ONLY on an “Access Layer” switch tunes Spanning Tree such that the blocking redundant uplink is activated immediately upon failure of the primary root port
Spanning Tree—Feature
Uplinkfast

• A 4.1(x) and higher feature which can bypass waiting for Max Age timer to expire
• Uses a Remote Link Query (RLQ) PDU to test path to the root upon receipt of an inferior BPDU

Spanning Tree—Feature
Backbonefast
Spanning Tree—Commands
Uplinkfast and Backbonefast

- Notice how uplinkfast changes STP parameters to try and keep the switch from being root

Switch> (enable) set spantree uplinkfast enable
VLANs 1-4094 bridge priority set to 49152.
The port cost and portviancost of all ports set to above 3000.
Station update rate set to 15 packets/100ms.
uplinkfast all-protocols field set to off.
uplinkfast enabled for bridge.

Switch> (enable) set spantree backbonefast enable
Backbonefast enabled for all VLANs.

Spanning Tree—Commands
Show Spantree Summary

Switch> (enable) sh spantree summary
MAC address reduction: disabled
Root switch for vlans: none.
Portfast bpdu-guard enabled for bridge.
Uplinkfast enabled for bridge.
Backbonefast enabled for bridge.

Summary of connected spanning tree ports by vlan

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Blocking</th>
<th>Listening</th>
<th>Learning</th>
<th>Forwarding</th>
<th>STP Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

Blocking Listening Learning Forwarding STP Active

Total 0 0 0 3 3
Spanning Tree—Be Proactive

- Know your network before trouble begins
- Know where the root of each tree is
- Know where all the blocked ports are
- Don’t do any tuning you don’t understand

Spanning Tree—Recovery

- DO NOT POWER OFF SWITCHES
- Check and physically remove the connections to the ports that should be blocking—this will get your network functional again
- Set up remote access to your network and call the TAC
Spanning Tree—Be Careful

- Spanning Tree is rather complex
- Do not “tune” Spanning Tree parameters manually unless you fully understand, have a plan, and have a reason
- Abide by recommended guidelines for number of Spanning Tree instances

Spanning Tree—Instances

\[ \text{Max Recommended Instances} = (\# \text{ of non-ATM trunks} \times \# \text{ of vlans on trunk}) + (\# \text{ of ATM trunks} \times \text{vlans on trunk} \times 2) + \# \text{ of non-trunking ports} \]

<table>
<thead>
<tr>
<th>Model</th>
<th>Max Recommended Instances</th>
</tr>
</thead>
<tbody>
<tr>
<td>5000 Sup I</td>
<td>400</td>
</tr>
<tr>
<td>5000 Sup II</td>
<td>1,500</td>
</tr>
<tr>
<td>5000 Sup II G</td>
<td>1,800</td>
</tr>
<tr>
<td>5000 Sup III</td>
<td>4,000</td>
</tr>
<tr>
<td>5000 Sup II G</td>
<td>1,800</td>
</tr>
<tr>
<td>4000 Sup I</td>
<td>1,500</td>
</tr>
<tr>
<td>4000 Sup II</td>
<td>1,500</td>
</tr>
<tr>
<td>6000 Sup I</td>
<td>4,000</td>
</tr>
<tr>
<td>6000 Sup II</td>
<td>20,000</td>
</tr>
</tbody>
</table>
Agenda

- Terminology
- The Layer 2 Basics
- Spanning Tree
- Layer 2 Quality of Service
- Layer 2 Access Control Lists

Quality of Service—Theory
Weighted Random Early Discard

WRED addresses:
In the event packets need to be dropped, what class of packets should be dropped

Queue

Packets Classified as Blue Start Dropping at a 50% Queue Depth. Drop Rate Is Increased as Queue Depth Is Increased

Packets Classified as Gold Are Dropped at 90% Queue Depth
Quality of Service—Theory

Weighted Round Robin

Weighted Round Robin Used to Schedule Between Queues

WRR Queue Scheduler

Output Port

Weighted Round Robin

Used To Schedule between Queues

Quality of Service—Theory

Dual Queues—Dual Thresholds
Quality of Service—Problem
CoS Not Set Properly

- The Class of Service is set by a different switch or a client, but another switch does not see the previous set CoS
- This will cause packets to be misclassified and possibly dropped
Quality of Service—Solution
CoS Not Set Properly

- Some form of tagging is necessary to pass CoS between devices

---

Quality of Service—Solution
CoS Not Set Properly

- On trusted ports, ingress port assigns CoS only to untagged packets
- On untrusted ports, the ingress port assigns a default CoS to all packets, tagged or not
- CoS assigned by an ingress port is independent of the VLAN
- Software routed packets lose CoS
Quality of Service—Trusted vs. Untrusted

- Cisco’s QoS model assumes that the CoS carried in a packet can be both “trusted” and “untrusted”
- Ports are “untrusted” by default
- Servers may be reliable enough to correctly tag the packets
- End stations generally are not trusted to tag a packet’s priority correctly
- 10/100 ports can only be “untrusted”

Quality of Service—Example Setting CoS with an ACL

- Example: Classify frames using ACLs;
  All traffic from vlan 200 to 1.1.1.1 gets CoS 4 (internal default DSCP 32); IP phones are on module 3 and get a DSCP of 40 (CoS=5)
  
c6k#set qos enable
c6k#set port qos 2/1-12 vlan-based
c6k#set qos acl ip mission_critical dscp 32 ip any host 1.1.1.1
c6k#commit qos acl mission_critical
c6k#set qos acl map mission_critical 200
c6k#set port qos 3/1-48 port-based
c6k#set qos acl ip voip dscp 40 ip any any
c6k#set qos acl map voip 3/1-48
Quality of Service—Problem
Unexpected Policing

• The Catalyst is configured to police traffic at a certain rate, but when traffic flows at that rate some of it is getting policed
• Obviously this is packet loss, that is BAD for any network

Quality of Service—Solution
Unexpected Policing

• There are a couple of common issues for this problem
  Incorrectly configured policer
  Not all applications send data in a steady stream...
Quality of Service—Policing
Policing Bucket

- Start with a bucket without data
- Data is added at a bursty rate
- Data is leaked at a specified constant rate
- If the bucket overflows, the packet gets policed

Quality of Service—Example

Rate: 16000 kbps, burst size: X kbits

Means: each leaking interval we will leak 16000 kbps * 0.00025 s = 4000 bits

If X=1 and the input rate is 16 Mbps, the output rate will only be 4 Mbps: this is because between leaking intervals, we attempt to put 16000 kbps * 0.00025 s = 4000 bits into the bucket; Since the bucket is already full after 1000 bits, 3/4 of the traffic will get policed
Quality of Service—Example (Cont.)

• If X=4 and the packet size is 1518 bytes, the output rate will be 0 Mbps: this is because between leaking intervals, we attempt to put at least one 1518 byte packet into the bucket; Since the bucket can only hold the first 4000 bits of the 12144 bit frame the frame will be policed.

Quality of Service—Example (Cont.)

• For a rate of 16 Mbps with 1518 byte packets, the minimum burst size is 13 (12144 bits rounded up)
• This will work great for UDP, but with TCP this will give you the “sawtooth” effect, so for TCP traffic multiply the calculated burst by 2
Quality of Service—Example Policing

- Example: policing of all http traffic in general and to web server 2.2.2.2 in particular
  
c6k#set qos policer aggregate Policer_http rate 10000 burst 26 drop  
c6k#set qos policer microflow Policer_2.2.2.2 rate 1000 burst 26 drop  
c6k#set qos acl ip police_acl trust-dscp microflow Policer_2.2.2.2 tcp any host 2.2.2.2 eq port 80  
c6k#set qos acl ip police_acl trust-dscp aggregate Policer_http tcp any eq port 80

Quality of Service—Problem Out of Order Packets

- Using QoS to police flows and mark down the CoS instead of dropping the packet; <reword> out of order packets on the network  
  
  - This problem can cause connections to drop or cause slowness in many applications (e.g. SNA, IPX, TFTP)
Quality of Service—Solution
Out of Order Packets

• When packets are marked down in CoS it is possible that they will be put into a different output queue for the egress port, if that queue is not as full, the marked down packet might leave the switch before a previous non-marked down packet

• When marking down packets make sure that they still go to the same output queue

Quality of Service—Example
Output Queuing

• Example: output scheduling using 1p2q2t ports; VOIP has CoS=5, Critical Data has CoS=6, policed to 10Mbps and marked down to CoS=4

```
c6k#set qos policer aggregate Policer_data rate 10000 burst 3 policed-dscp
c6k#set qos policed-dscp-map 48:32
c6k#set qos map 1p2q2t tx queue 3 1 cos 5
c6k#set qos map 1p2q2t tx queue 2 1 cos 4
c6k#set qos map 1p2q2t tx queue 2 2 cos 6,7
c6k#set qos wred 1p2q2t tx queue 2 80 100
c6k#set qos wrr 1p2q2t 30 70
c6k#set qos txq-ratio 1p2q2t 70 15 15
```
### Quality of Service—Commands

#### Show Port QoS

```plaintext
Cat6000> (enable) show port qos 4/1
QoS is enabled for the switch.
QoS policy source for the switch set to local.

<table>
<thead>
<tr>
<th>Port</th>
<th>Interface Type</th>
<th>Policy Source</th>
<th>Policy Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/1</td>
<td>config</td>
<td>config</td>
<td>runtime</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Interface Type</th>
<th>Trust Type</th>
<th>Def CoS</th>
<th>Def CoS</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/1</td>
<td>1p2q2t</td>
<td>untrusted</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

(*)Runtime trust type set to untrusted.

**Config:**

<table>
<thead>
<tr>
<th>Port</th>
<th>ACL name</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

No ACL is mapped to port 4/1.

**Runtime:**

<table>
<thead>
<tr>
<th>Port</th>
<th>ACL name</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

No ACL is mapped to port 4/1.
```

### Quality of Service—Commands

#### Show Port Capabilities

```plaintext
Cat6000> (enable) show port capabilities 4/1

<table>
<thead>
<tr>
<th>Model</th>
<th>WS-X6416-GE-MT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>4/1</td>
</tr>
<tr>
<td>Type</td>
<td>1000BaseSX</td>
</tr>
<tr>
<td>Speed</td>
<td>1000</td>
</tr>
<tr>
<td>Duplex</td>
<td>full</td>
</tr>
<tr>
<td>Trunk encap type</td>
<td>802.1Q,ISL</td>
</tr>
<tr>
<td>Trunk mode</td>
<td>on,off,desirable,auto,negotiate</td>
</tr>
<tr>
<td>Channel</td>
<td>yes</td>
</tr>
<tr>
<td>Broadcast suppression</td>
<td>percentage(0-100)</td>
</tr>
<tr>
<td>Flow control</td>
<td>receive-(off, on, desired), send-(off, on, desired)</td>
</tr>
<tr>
<td>Security</td>
<td>yes</td>
</tr>
<tr>
<td>Membership</td>
<td>static,dynamic</td>
</tr>
<tr>
<td>Fast start</td>
<td>yes</td>
</tr>
<tr>
<td>QoS scheduling</td>
<td>rx-(1p1q4t),tx-(1p2q2t)</td>
</tr>
<tr>
<td>CoS rewrite</td>
<td>yes</td>
</tr>
<tr>
<td>ToS rewrite</td>
<td>DSCP</td>
</tr>
<tr>
<td>ULD</td>
<td>yes</td>
</tr>
<tr>
<td>SPAN</td>
<td>source,destination</td>
</tr>
</tbody>
</table>
```

---

*Note: The images are not legible due to quality issues.*
Quality of Service—Commands
Show QoS Information

Cat6000> (enable) show qos info runtime 4/1
Run time setting of QoS:
QoS is enabled
Policy Source of port 4/1: Local
Tx port type of port 4/1: 1p2q2t
Rx port type of port 4/1: 1p1q4t
Interface type: port-based
ACL attached:
The qos trust type is set to untrusted.
Default CoS = 0
Queue and Threshold Mapping for 1p2q2t (tx):
Queue Threshold CoS
------------- ---------------
1 1 0 1
1 2 2 3
2 1 4 6
2 2 7
3 1 5
Queue and Threshold Mapping for 1p1q4t (rx):
All packets are mapped to a single queue.
Rx drop thresholds:
Rx drop thresholds are disabled.
Tx drop thresholds:
Tx drop-thresholds feature is not supported for this port type.

Quality of Service—Commands
Show QoS ACL Map

Cat6000> (enable) show qos acl map all
ACL name Vlan # Ports
---------- ----------------- -----------------------------
ACLdeny_http 1,4-7
ACLpermit_isp1 2 1/1

Cat6000> (enable) show qos acl map 1
Vlan ACL name
---- ----------------
1 ACLdeny_http

Cat6000> (enable) show qos acl map ACLpermit_isp1
ACL name Vlan # Ports
---------- ----------------
ACLpermit_isp1 2 1/1
Quality of Service—Commands
Show QoS ACL Map Runtime All

Cat6000> (enable) show qos acl map runtime all
ACL name     Type  Vlans
---------------------  -----  ------------
aciHTTP_LIMIT     IP    1
ACL name
---------------------  -----  ------------
aciHTTP_LIMIT     IP    Ports
ACL name
---------------------  -----  ------------
aciMB1            MAC  4/1
ACL name
---------------------  -----  ------------
Cat6509 (enable)

Quality of Service—Commands
Show QoS Policer Runtime All

Cat6000> (enable) show qos policer runtime all
QoS microflow policers:
Microflow name       Avg. rate (kbps)  Burst size (kb)  Exceed action
---------------------  ---------------  ---------------  ---------------
mpMB1                992              32              drop
ACL attached
---------------------  ---------------  ---------------  ---------------
aciHTTP_LIMIT

QoS aggregate policers:
Aggregate name       Avg. rate (kbps)  Burst size (kb)  Exceed action
---------------------  ---------------  ---------------  ---------------
apMB1                992              32              drop
ACL attached
---------------------  ---------------  ---------------  ---------------
aciMB1
Quality of Service—Commands
QoS ACL Statistics

```
Cat6000> (enable) show qos stat l3stats
Packets dropped due to policing:    189003
IP packets with ToS changed:        29843
IP packets with CoS changed:        4532
Non-IP packets with CoS changed:    17254
```

```
Cat6000> (enable) show qos acl resource-usage
ACL resource usage:
ACL storage (mask/value): 0.29%/0.7%
ACL to switch interface mapping table: 0.39%
ACL layer 4 port operators: 0.0%
```

Agenda

- Terminology
- The Layer 2 Basics
- Spanning Tree
- Layer 2 Quality of Service
- Layer 2 Access Control Lists
Access Lists—Problem
MAC ACL Not Blocking IP

• The following ACL has been configured and applied to Vlan 1
  
c6k#set security acl mac mac_acl deny host 00-00-0c-12-34-56 host 00-00-0c-98-76-54
c6k#set security acl map mac_acl 1

• In testing these two stations are still able to talk to each other with IP and IPX

Access Lists—Solution
MAC ACL Not Blocking IP

• This is a function of how the Catalyst 6000 works
  
  When a packet is accepted into the switch it is classified as a IP/IPX/MAC packet by the incoming port; So when the ACLs are applied the MAC ACL is only applied to the MAC frames, not to IP or IPX frames
Access Lists—Commands

Cat6000> (enable) show security acl info all
set security acl ip security

arp permit
1. deny ip host 10.118.2.21 host 10.118.2.56

set security acl mac mac_acl

1. deny host 00-00-0c-12-34-56 host 00-00-0c-98-76-54

Cat6000> (enable) show security acl map all
ACL Name       Type  Vlans
-------------------- --------
security        IP     1
mac_acl          MAC    1

Cat6000> (enable) show security acl resource-usage
Security ACL resource usage:
ACL storage (mask/value): 0.14%/0.1%
ACL to switch interface mapping table: 0.39%
ACL layer 4 port operators: 0.0%