Deploying Campus-Based Protocols
Session 2803
Agenda

- Recipe for a Campus Network
- Intelligent Network Agents
- Cisco’s Intelligent Switch Protocols
- Q & A

Part I
Recipe for a Campus Network
Familiar Design?

Network protocols are just one piece of the puzzle . . .

So...What Makes a Solid Campus?

Three simple ingredients . . .

1. Well thought out network design
2. Complimentary suite of protocols
3. Strategic application of protocols

Strategic application of protocols and features requires detailed knowledge
Part II

Intelligent Network Agents

Four Key Areas to Maximize

Security
Availability
Manageability
Scalability
Campus Design

Cisco’s Protocols Maximize these Four Areas

Copyright © 1998, Cisco Systems, Inc. All rights reserved. Printed in USA.
Presentation_ID.scr
Intelligent Agent Technologies

- Industry standards
  - SNMP: Device get and sets
  - RMON1/2: Traffic monitoring

- Cisco extensions
  - Cisco Discovery Protocol (CDP)
  - ISL/802.1Q VLAN trunking
  - Dynamic Trunk Protocol (DTP)
  - CGMP/IGMP snooping
  - Broadcast suppression
  - EtherChannel®
  - Private VLANs
  - VLAN Access Lists (VACLs)
  - Spanning tree extensions

Cisco’s Key Linkages in Cisco IOS

Just some of Cisco’s network services . . .
Part III
Cisco’s Intelligent Switch Protocols

Embedded Switch Protocols

- Cisco Discovery Protocol (CDP)
- ISL/802.1Q VLAN Trunking
- Dynamic Trunk Protocol (DTP)
- CGMP/IGMP Snooping
- Broadcast Suppression
- EtherChannel
- Private VLANs
- Unidirectional Link Detection (UDLD)
- Spanning Tree Extensions
Lack of Layer 2 and Layer 3 View

- NMS topology views are extremely IP-centric
- NMS views don’t reflect Layer 2 topology
- NMS views unable to provide visibility in switched environments

Cisco Discovery Protocol (CDP)

- What is CDP?
  - Advertisement protocol
  - Media independent
  - Protocol independent
  - Visibility into adjacencies
  - On all major devices
Cisco Discovery Protocol

- CDP agent listens to neighboring devices
- Device parameters periodically exchanged
- Each device maintains “CDP” cache table and populates a CDP MIB
- Tables can be read by management application

Discovery Exchange
- IP Address
- Device Type

Software Revision
- VTP Domain Name
- Device ID/Name
- Native VLAN
- Capabilities
- Port ID

Uses multicast address 01-00-0C-CC-CC-CC-CC
- Enabled by default
- Selectively tuned by device/interface/sub-interface
- Default advertisement interval is 60 seconds
- Default time-to-live is 180 seconds
- CDP TTL set to zero for interface down or disable
- CDP packets redirected to supervisor, not flooded
- IETF activity – Physical Topology Mib Topology
(http://www.ietf.org/html.charters/ptopomib-charter.html)
CDP on Routers

```
hercules#show cdp neighbor
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                   S - Switch, H - Host, I - IGMP, r - Repeater
Device ID  Local Intrfce  Holdtme  Capability  Platform  Port ID
003166185(apollo)  Fddi0   136  T S  WS-C5000 2/1-2
062015145(zeus)    Fddi0   172  R S  WS-C1202 1
003292590(cronus)  Fas 0   179  T S  WS-C5000 2/3
003270690(rhea)    Fas 1   171  T S  WS-C5000 3/3
```

CDP on Switches

```
apollo# (enable) show cdp neighbor
Port   Device-ID  Port-ID
       * - indicates vlan mismatch.
       # - indicates duplex mismatch.
2/1-2  062015145(zeus)  1  WS-C1202
       2/1-2  003292590(cronus)  Fas 0  WS-C5000
       3/1-2  jupiter  ATM200/0/1  cisco ASP
```
CDP Details

Device-ID: 062015145(zeus)
Device Addresses:
  IP Address: 192.10.10.6
  Holdtime: 151 sec
Capabilities: ROUTER SWITCH
Version: WS-C1202 Software, Ver Dmp SW: 4.21
  Nmp SW: 4.21
  Copyright (c) 1994,1995 by Cisco Systems
  DMP S/W Compiled on Aug 9 1996 10:54:03
  NMP S/W Compiled on Aug 9 1996 10:19:13
  Platform: WS-C1202
Port-ID (Port on Device): 1
Port (Our Port): 2/1-2

Embedded Switch Protocols

- Cisco Discovery Protocol (CDP)
- ISL/802.1Q VLAN Trunking
- Dynamic Trunk Protocol (DTP)
- CGMP/IGMP Snooping
- Broadcast Suppression
- EtherChannel
- Private VLANs
- Unidirectional Link Detection (UDLD)
- Spanning Tree Extensions
VLAN Trunking

- Many tagging methods
- Understanding 802.1Q standard
- Understanding solved problem

VLAN Tagging Protocols

- 802.10 (FDDI)
- ISL
- 802.1Q
- LANE (ATM)
What Is a VLAN in 802.1Q?

Two possible models

- **Access VLANs (typically untagged)**
  These VLANs are a way to specify filters to limit endstation-to-endstation connectivity on a single, bridged LAN

- **Independent VLANs (typically tagged)**
  These VLANs are a way to utilize one physical plant to carry multiple, independent bridged LANs

Access VLANs in 802.1Q

- It is a single bridged LAN, with filters
- Access VLANs mandate a single spanning tree for entire network
- One filtering database for all VLANs in each bridge
Access VLANs in 802.1Q Example

- One-way VLANs based on access lists
  Half-duplex conversations within different VLANs
  Switch 1 never sees F’s source on yellow or blue, nor X’s or Y’s sources on red
  Filtering database must ignore “color”

Independent VLANs in 802.1Q

- Better scaling for larger networks...
  Scope of each VLAN is not global
  Routers/Layer 3 switches terminate VLANs
- Separate filtering database per VLAN
- Able to work with:
  A single spanning tree
  One spanning tree per VLAN
  Multiple spanning trees for multiple VLANs
An Independent VLAN Advantage

- They support duplicate MAC addresses
  
  Eg. DECNet phase IV routers
  Multi-NIC configurations in Sun workstations
  Bridged protocols between VLANs

Number of “Filtering Databases”

- **MFD/SE**
  
  Multiple filtering database—single entry
  Natural solution for independent VLANs
  Compatible with multiple spanning trees

- **SFD/ME**
  
  Single filtering database—multiple entry
  Access VLAN method
  Difficult to solve duplicate MAC problem
  Requires a single spanning tree
IEEE 802 LMSC

- 802 LAN/MAN standards committee
- 802.1: Higher layer interfaces
  - 802.1D (transparent bridging)
- 802.1D Reaffirmation
- 802.1p Priorities/GARP/GMRP
- 802.1Q VLANs/GVRP
- 802.3: CSMA/CD (Ethernet)
  - 802.3ac Extended frame size (1522 bytes)

Frame Tagging

- Contains VLAN membership information
- Implicit tagging
  - No tag is added to the frame
  - Easy in connection-oriented approaches
  - Difficult for multicast/broadcast frames
- Explicit tagging
  - A tag is added to each frame
  - The tag carries the VLAN membership information
  - The tag may carry additional information
Explicit Tagging

• Where to position the tag in the frame?
• Two possibilities:
  - One level tagging
    Also called “internal tagging”
  - Two level tagging
    Also called “external tagging”
• Both must be implemented in ASICs for wire speed performance

One Level Tagging

• Tag added inside of original frame
• Valid format for “VLAN unaware” devices
  - MAC SA and DA are unchanged
• Addition 4 byte tag creates “Baby Giants”
  - 802.1 has persuaded 802.3 to increase the maximum frame size from 1518 to 1522 (four extra bytes)—802.3ac
Example of One Level Tagging

Tagging Ethernet—IEEE 802.3

**Ethernet v2.0**

- PREAM.  |  SFD  |  DA  |  SA  |  TAG  |  PT  |  DATA  |  FCS
- Octets  |  7   |  1   |  6   |  6   |  4   |  2     |  4 From 46 to 1500

**IEEE 802.3**

- MAC Length/Type
- MAC Data
- PAD
- FCS

802.1Q Tagging Scheme

- Destination Address 6
- Source Address 6
- EtherType = TPID 2
- Tag Control Information 2
- MAC Length/Type 2
- MAC DATA 42
- PAD 1500
- FCS 4

3 1

- User Priority
- CFI

VID (VLAN ID) — 12 Bits

Used in:
- IEEE 802.3ac
- IEEE 802.1Q
- IEEE 802.1p
Two-Level Tagging

- Original frame is left unchanged
- New header is added onto original frame
  - New SA, DA, (RIF), EtherType, and VLAN-ID
  - It is possible to support giant frames
- The RIF works better
  - Two-level tagging is a tunneling mechanism
- FCS fix-up in new header allows original frame FCS to be retained

Inter-Switch Link (ISL)

- Two-level tagging scheme
- Original frame is encapsulated with ISL header and FCS, i.e. two level tagging
- Initial support of up to 1,024 VLANs
- Implemented in ASICs provides wire speed performance
**ISL Header Format**

<table>
<thead>
<tr>
<th>Destination MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>DA</td>
</tr>
</tbody>
</table>

- The higher 40 bit—multicast destination address
- Lowest 8 bits used by type and user field

**ISL—Multiple Spanning Trees**

- All links in the network are simultaneously used by modifying spanning tree parameters

- S1
- S2
- S3

Red STP
Green STP
Spanning Tree Issues

- 802.1Q specifies one spanning tree (STP) per bridge cloud, but it does not preclude multiple spanning trees in later revisions of the specification.
- Cisco uses ‘n’ STPs per ‘m’ VLANs
  - 802.1Q is the special case $n = 1$
  - Current Cisco solution is $n = m$
- One spanning tree doesn’t allow for load-sharing

802.1Q and ISL

- ISL capabilities are superset of 802.1Q
  - ISL also has the user priority field
- Interoperability between SFD and MFD:
  - Yes in simple topologies (PVST+)
  - No in corner cases
- Current Catalyst switch VLAN support:
  - Hardware supports 4096 VLANs (802.1Q)
  - Software supports 1024 VLANs (802.1Q/ISL)
  - Future software support for 4096 VLANs
VLAN Trunk Types

- In Cisco’s VLAN architecture 802.1Q is just another trunk type:
  - ISL, LANE, IEEE 802.1Q, IEEE 802.10
  - Any mix of these in one VLAN is allowed
- Line cards support ISL, 802.1Q, or both
- DISL is extended (DTP) to negotiate ISL or IEEE 802.1Q

The Native VLAN in 802.1Q

- Single unencapsulated VLAN
- Commonly used for management protocols
- Defined and mandatory in 802.1Q spec
- Does not exist in Cisco’s ISL
- Not to interfere with trunked VLAN numbering
Problem: VLAN Trunk Endpoint Mismatch

- IEEE 802.1Q standard approved
- Need to automate ISL/802.1Q trunk configuration
- Possible loss in network connectivity due to configuration inconsistencies
Dynamic Trunk Protocol (DTP)

What is DTP?

- DTP is a point-to-point protocol
- Automates ISL/.1Q trunk configuration
- Operates between switches
- Does not operate on routers

DTP Function

- DTP synchronizes the trunking mode on link ends
- DTP prevents the need for management intervention on both sides
- DTP state on ISL/1Q trunking port can be set to “Auto”, “On”, “Off”, “Desirable”, or “Non-negotiate”
DTP Trunk States

• Valid states for switch trunk ports
  
  NEGOTIATE—Negotiate for ISL or 1Q
  
  NATIVE—Non trunk
  
  ISL—All frames transmitted and received are ISL tagged. DTP packets are sent out both tagged and untagged
  
  802.1Q—All frames transmitted and received are 802.1Q tagged except those on the native VLAN. DTP packets are transmitted untagged on native VLAN

DTP Admin States

• Administrator configurable trunk states
  
  ON I want to be a trunk and I don’t care what you think!  
  (Used when the other end does not understand DTP)
  
  OFF I don’t want to be a trunk and I don’t care what you think!  
  (Used when the other end cannot do ISL or 1Q)
  
  Desirable I’m willing to become a VLAN trunk. Are you interested?  
  (Used when you are interested in being a trunk)
  
  Auto I’m willing to go with whatever you want!  
  (Used as the default mode for plug-and-play)
  
  Nonegotiate I want to trunk, and this is what kind of trunk I will be!  
  (Used when you want a specific type of trunk ISL or 1Q)
DTP Specifics

- Uses destination multicast 01-00-0C-CC-CC-CC
- HDLC protocol 0x2004
- DTP default “Auto” state
- DTP passes through ports in STP blocked state
- During DTP negotiations the port does not participate in STP
- DTP Packets not flooded, but redirected to NMP

DTP Configuration

- DTP management messages from another VTP domain are ignored
- DTP packets sent out every 30 seconds except in the “OFF” state
- DTP syntax
  
  ```
  set trunk <mod/port> [on|off|desirable|auto|nongotiate] [vlans] [trunk_type]
  ```
- DTP available on Catalyst® switches supporting ISL and/or 802.1Q
DTP on Catalyst Switches

cronus> (enable) set trunk
Usage: set trunk <mod_num/port_num> [on/off/desirable/auto] [vlans] [trunk_type]
   (vlans = 1..1000  An example of vlans is 2-10,1000)
cronus> (enable) set trunk 2/3 on 1-1000
   Port 2/3 allowed vlans modified to 1-1000.  Port 2/3 mode set to on.
cronus> (enable) show trunk 2
* - indicates vtp domain mismatch
<table>
<thead>
<tr>
<th>Port</th>
<th>Mode</th>
<th>Encap</th>
<th>Status</th>
<th>Native-VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/1</td>
<td>auto</td>
<td>negotiate</td>
<td>not-trunking</td>
<td>1</td>
</tr>
<tr>
<td>2/2</td>
<td>on</td>
<td>negotiate</td>
<td>not-trunking</td>
<td>1</td>
</tr>
<tr>
<td>2/3</td>
<td>on</td>
<td>ISL</td>
<td>trunking</td>
<td>1</td>
</tr>
</tbody>
</table>
Port VLANs allowed on trunk
- 2/1 1-1000
- 2/2 1-1000
- 2/3 1-1000
Port VLANs allowed and active
- 2/1 1
- 2/2 1
- 2/3 1-4

Embedded Switch Protocols

- Cisco Discovery Protocol (CDP)
- ISL/802.1Q VLAN Trunking
- Dynamic Trunk Protocol (DTP)
- CGMP/IGMP Snooping
- Broadcast Suppression
- EtherChannel
- Private VLANs
- Unidirectional Link Detection (UDLD)
- Spanning Tree Extensions
Problem: Preventing IP Multicast Flooding

- Packets not sourced from multicast address—switch can’t learn
- Switches treat multicasts as broadcasts unless entered in the CAM tables
- Need to administer multicast flood entries
- Multicasting becoming more prevalent in the campus
- Scalability of multicasting in the campus an issue

Cisco Group Management Protocol (CGMP)

- What is CGMP?
  - CGMP is a derivative of IGMP
  - Enables intelligent setup of multicast trees
  - Runs in conjunction with Cisco routers running multicast routing protocols
IP Multicast Elements

Network DA 224.1.1.1
MAC DA 01-00-5E-0101-01

Multicast Server

IGMP Join Request

Layer 2 Switch

Multicast Client

Layer 2 Switch

Keep Quiet or Everybody Gets it!

IP Multicast Elements

CGMP Details

- Runs on switches and routers
- IGMP packets forwarded only to the router port and the NMP
- Router sends CGMP multicast packets to switches at known address of: 01-00-0c-dd-dd-dd
- CGMP packet contains:
  Type field—Join or leave
  MAC address of the IGMP client
  Multicast address of the group
- Switch uses CGMP packet info to add or remove CAM entry for particular multicast address
Join a Group with CGMP

- Host sends IGMP request for group they wish to join
- Catalyst forwards request to router
- Router builds CGMP Join message and multicasts it to switch
- Switch searches MAC entries in CAM table to identify port where MAC is resident
- Switch places port into the required multicast group

Leaving a Group with CGMP

- Router periodically sends general query
- IGMP version 1 hosts signal active multicast groups
- If router detects no members left in a multicast group, sends a CGMP-remove to all switches
- IGMP version 2 hosts send a specific leave message to 224.0.0.2 for groups they wish to leave
- Routers handle version 2 host leaves by sending group specific query
- Router queries for ports with more than one host present within that group
CGMP—Router Commands

- `ip cgmp`  
  Enables cgmp for IP Multicast on LANs

- `debug ip cgmp`  
  Logs cgmp packets and activity

- `show ip cgmp interface`  
  Displays on what interfaces cgmp is enabled

- `clear ip cgmp [interface]`  
  Clears all switch group entries

CGMP—Switch Commands

- `set cgmp enable, disable`  
  Enables cgmp processing

- `set multicast router 3/1`  
  Sets ports that have CGMP capable routers

- `show multicast router 3/1`  
  Shows the ports enabled for CGMP capable routers

- `show multicast router cgmp 5`  
  Shows the router ports on VLAN 5

- `show multicast group cgmp 5`  
  Shows all multicast groups/members within a VLAN
IGMP Snooping

- Switch “watches” IGMP communications on the VLANs to do constrained L2 multicast forwarding
- Will also dynamically learn about various multicast routers and multicast sources
- Done in hardware on the Catalyst series
  Snooping operations performed in hardware

IGMP-Snooping Switch Commands

- set igmp enable, disable
  Enables igmp-snooping processing
- set multicast router 3/1
  Sets ports that have IGMP-enabled routers
- show multicast router 3/1
  Shows the ports that have IGMP-enabled routers
- show multicast router igmp 5
  Shows the IGMP router ports on VLAN 5
- show multicast group 5
  Shows all multicast groups/members within a VLAN
Catalyst Switch Support

• CGMP is supported on following switch series
  Catalyst 1900, 2800, 2900G, 2900XL, 3500XL, 4000, 5000, 5500, 6000, 6500

• IGMP-snooping is supported on following switch series:
  Catalyst 2926G, 5000/5500 with Sup-III/NFFCI/I1, Catalyst 6000

Embedded Switch Protocols

• Cisco Discovery Protocol (CDP)
• ISL/802.1Q VLAN Trunking
• Dynamic Trunk Protocol (DTP)
• CGMP/IGMP Snooping
• Broadcast Suppression
• EtherChannel
• Private VLANs
• Unidirectional Link Detection (UDLD)
• Spanning Tree Extensions
The Broadcast Storm

- Problem:
  Broadcasts generated at extreme rates by a misbehaving workstation or STP looping state
  - Malfunctioning STP process
  - Malfunctioning learning process
  - Corrupted BPDU reception
  - Faulty hardware
  - Broadcast-intensive application
  - Faulty NIC or workstation

Broadcast Suppression

What is broadcast suppression?
- Reduces effects of broadcast storm
- Filtering mechanism to reduce traffic
- Measures broadcast/multicasts activity over time
- Suppresses broadcasts and multicasts
- Can be implemented in hardware or software
- Disabled by default
How Does it Work?

Two Methods for Measurement

- **Packet-based**—measures number of broadcasts/multicasts received over 1st period, implemented in software
- **Bandwidth-based**—measures amount of bandwidth for broadcasts/multicasts over 1st period, implemented in hardware
- Filtering mechanism to reduce traffic
- Suppresses broadcasts **and** multicasts
- Disabled by default

Broadcast Suppression Example

- Example of packet-based measurement
- Filtering occurs at T1-T2 and T4-T5
- Bandwidth-based over packet-based
Broadcast Suppression Commands

- set port broadcast 3/1 70%
  Enables broadcast suppression (bandwidth-based)
- set port broadcast 3/1 10000
  Enables broadcast suppression (packet-based)
- show port broadcast 3/1
  Shows the broadcast statistics for port 3/1
- clear port broadcast 3/1
  Disable broadcast suppression for port 3/1

Broadcast Suppression Availability

- Available on:
  - Catalyst 6000 family
  - Catalyst 5000 and 5500 families with Sup-III and NFFC-I/II
  - Catalyst 3500XL series
  - Catalyst 2926G
Embedded Switch Protocols

- Cisco Discovery Protocol (CDP)
- ISL/802.1Q VLAN Trunking
- Dynamic Trunk Protocol (DTP)
- CGMP/IGMP Snooping
- Broadcast Suppression
- EtherChannel
- Private VLANs
- Unidirectional Link Detection (UDLD)
- Spanning Tree Extensions

EtherChannel Protocol

What is EtherChannel?
- A logical aggregation of common links
- Works for 10/100/1000 Mbps
- Operates between switches, routers, and certain server NICs
- Channel created between same two devices
- Similar to the new 802.3ad
EtherChannel

Load sharing and redundancy provided
Valid link aggregations include 2 and 4 links
Catalyst 6000 Family supports 2–8 links

EtherChannel Bandwidth Options
Routers and Non-6X00 Switches

• Smooth migration to higher bandwidths
• Gain resiliency at same time
• Considered as one link to STP and routing protocols
• Featured on Catalyst family and Cisco IOS
EtherChannel Bandwidth Options
Catalyst 6X00 Switches

- Bundle formed with 2–8 links considered valid
- Bundle members can exist on different cards
- Maximum bandwidth of 16 Gbps (FDX) possible
- Considered as one link to STP and Routing Protocols

EtherChannel Load Balancing

How does it load share?
- Layer 2 devices
  Source/destination MAC
- Layer 3 devices
  Source/destination IP
- Server NICs
  Source/destination MAC
- Catalyst 6000 family can be switched between MAC/IP
Caution With EtherChannel Servers

- Algorithm based on source/destination MAC address
- Layer 3 interface only one MAC address
- Only one link in channel will ever be used
- FEC a good solution for workgroup servers

EtherChannel Admin States

- Administrator configurable channel states
  - **ON**: I want to be a channel and I don’t care what you think! (Used when the other end does not understand PAgP)
  - **OFF**: I don’t want to be a channel and I don’t care what you think! (Used when the other end cannot support EtherChannel)
  - **Desirable**: I’m willing to become a channel. Are you interested? (Used when you are interested in being a channel)
  - **Auto**: I’m willing to go with whatever you want! (Used as the default mode for plug-and-play)

- **EtherChannel syntax**
  - `set port channel <mod/port> [admin_group]`
    Associate ports to same channel instance
  - `set port channel <mod/port> mode <on|off|auto|desirable> [silent|nonsilent]`
    Set the administrative state of the channel
  - `set port channel all distribution <ip|mac> <source|destination|both>`
    Set the load balancing mode – Catalyst 6000 Family only
Embedded Switch Protocols

- Cisco Discovery Protocol (CDP)
- ISL/802.1Q VLAN Trunking
- Dynamic Trunk Protocol (DTP)
- CGMP/IGMP Snooping
- Broadcast Suppression
- EtherChannel
- Private VLANs
- Unidirectional Link Detection (UDLD)
- Spanning Tree Extensions

What Is a Private VLAN?

- A Private VLAN:
  - A Layer 2 structure with three port classifications
  - **Isolated ports**: can only communicate with **Promiscuous Ports**
  - **Promiscuous ports**: can communicate with all other ports
  - **Community ports**: can communicate with other members of community and all promiscuous ports
  - All within the same VLAN (subnet)
**Private VLAN Details**

- ‘Private VLANs’ and normal VLANs can exist simultaneously in same switch
- ‘Private VLANs’ currently exist on Catalyst 6000 family switches
- Provides for protected connections
- No ARP discovery possible by neighbors
- ‘Private VLAN Edge’ exists on Catalyst 3500XL

**Private VLAN Structure**

Only one Subnet!

- Primary VLAN
- Community VLAN
- Community VLAN
- Isolated VLAN
- Isolated VLAN

1 Private VLAN
Private VLAN Community Uses

Fault-tolerant server NIC arrangements
Server clustering
Front-end content replication
Network management reasons

Private VLAN Community allows for front-end connectivity while maintaining Private VLAN security functionality

Normal VLAN Structure
Router Application

Catalyst 6500 with MSFC

Catalyst 6500 without Private VLAN Support

Three IP Subnets!
6 Broadcast Addresses
9 HSRP Addresses
15 Unusable Addresses
**Private VLAN Structure**

**Router Application**

Catalyst 6500 with MSFC
Private VLAN Support

Catalyst 6500
with Private VLAN Support

One IP Subnet!

2 Broadcast Addresses
3 HSRP Addresses

-----------------------------------
5 Unusable Addresses only!

**Private VLAN Structure**

Extending a Private VLAN

Only trunk those VLANs which are required to be propagated

ie. If community doesn’t exist on other switches, don’t trunk its VLAN.
Private VLAN Advantages

- Conserves IP addressing
- Easier IP addressing IP allocation
- Provides same security as separate VLANs
- Reduces VLAN usage (without communities)
- Completely 802.1Q compatible
Embedded Switch Protocols

- Cisco Discovery Protocol (CDP)
- ISL/802.1Q VLAN Trunking
- Dynamic Trunk Protocol (DTP)
- CGMP/IGMP Snooping
- Broadcast Suppression
- EtherChannel
- Private VLANs
- VLAN Access Lists
- Unidirectional Link Detection (UDLD)
- Spanning Tree Extensions

Unidirectional Link Detection (UDLD)

- What is UDLD?
  - Detects one-way connectivity
  - Independent of auto-negotiation
  - Similar to FEFI in 100Fx
  - Supports 10/100Tx, 1000X
  - Detects faults above physical layer
Unidirectional Link Detection Protocol

- UDLD agent listens to neighboring devices
- Device parameters periodically exchanged
- Each device maintains “UDLD” cache table
- UDLD MIB is populated to be used in NMS app

<table>
<thead>
<tr>
<th>Discovery Exchange</th>
<th>Echo</th>
<th>Device Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device ID</td>
<td>Message Interval</td>
<td>Sequence Number</td>
</tr>
<tr>
<td>Port ID</td>
<td>Timeout Interval</td>
<td>Reserved fields</td>
</tr>
</tbody>
</table>

UDLD Exchange Parameters

- Device ID—MAC address of sending device
- Port ID—#mod/#port of sending device
- Echo—valid #mod/#port pairs known by sending device
- Message Interval—transmit interval of sending device
- Timeout Interval—timeout interval of sending device
- Device Name—CDP device ID string of sending device
- Sequence Number—used to validate discovery packets
- Reserved Fields—reserved for future use
UDLD Specifics

- Uses destination multicast 01-00-0C-CC-CC-CC
- HDLC protocol 0x2111
- UDLD disabled by default
- UDLD is a link layer protocol
- Both ends must run UDLD
- Update/timeout configurable
- Configurable per switch port

Risks of One-Way Connections
Routing Black Holes

- One-way connection created due to broken fiber
- One end is ‘up’, other is ‘down’
- ½ of the traffic is lost

Routes still advertised
Traffic still forwarded
Risks of One-Way Connections
STP Black Hole

- One-way connection created due to broken fiber
- One end is ‘up’, other is ‘down’
- STP keeps link in ‘forwarding’
- Access switch cut-off

Other Detectable Configurations

- More problems than just a broken fiber
- One-way connections can also cause STP loops
- All interfaces look ‘UP’ without UDLD!
- UDLD resolves these
UDLD Advantages

- Detects more than physical problems
- Totally transparent to the user
- Enhances overall network availability
- Detects link breakages and wrong connections
- Available on most Catalyst switch platforms

Embedded Switch Protocols

- Cisco Discovery Protocol (CDP)
- ISL/802.1Q VLAN Trunking
- Dynamic Trunk Protocol (DTP)
- CGMP/IGMP Snooping
- Broadcast Suppression
- EtherChannel
- Private VLANs
- Unidirectional Link Detection (UDLD)
- Spanning Tree Extensions
End-to-End Network Resilience

**Problem** Providing Resilience across Campus

**Solution** Path and Device Resilience

- **Wiring closet resilience:**
  - Multiple links—load-sharing
  - STP-per-VLAN
  - UplinkFast
  - EtherChannel

- **Data center resilience:**
  - HSRP router resilience
  - Routing protocol tuning

---

Spanning Tree Port Types

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

Diagram illustrates core, distribution, and peer devices with Port Types.
Distributing VLANs Using STP

With Default Settings all VLAN Traffic Goes Down One Path

By Administering PortVlanPriority Settings on Equal Cost Paths to Root VLAN Traffic now has Redundancy as Well as Distribution

Port Priority Reduced from Default of 32 to 16 to Make this Preferred for the RED VLAN

Distributing VLANs Using STP

Backup Root — VLAN Green
Root — VLAN Red

Backup Root — VLAN Red
Root — VLAN Green

Blocking Ensured at the Access by Letting the Roots and Backup Roots be at the Distribution Switches (A and B)
Spanning Tree Protocol Timer

- Hello
  2 seconds (min 1)
- Forward delay
  15 seconds (min 4)
- Max age
  20 seconds (min 6)

Fast Convergence Using UplinkFast

- Enable on access switches
- Fast cutover (~2 seconds)
- Faster re-learning process
- Use your available bandwidth!
- Uplinks can be EtherChannel®
- Available across Catalyst Line
**Uplinkfast Protocol Timers**

- Link failure detection (2–3 seconds)
- Transition from blocking to forwarding (1 second)
- Re-learning (1–2 seconds)

---

**STP Designs—General Rules (1)**

- Use default timer values for most networks
- Reducing STP values to bare minimum can cause lots of data forwarding issues
- Reduce hops to root
- Keep network diameter small for tuning
- Take advantage of UplinkFast for fast convergence on wiring closet switches
STP Designs—General Rules (2)

- Root switch for VLAN dictates STP timers; set similar values at backup root device
- Minimize blocking at a single switch in the distribution or core
- Setting `portvlanpri` on Catalyst only on ports with equal cost paths to the root and connected to the same switch

Part III

Q&A
Deploying Campus-Based Protocols
Session 2803

Please Complete Your Evaluation Form
Session 2803