Security Best Practices in Catalyst Campus Switches

Mike Peeters
SE Toronto
Agenda

• Security Myths
• Management Channels
• VLAN Isolation
• Known Attacks
• Secure Switch Configuration
Security Myths

- MAC addresses cannot be spoofed
- A Switch protects against sniffers
- VLANs are completely isolated
Agenda

• Security Myths
• Management Channels
• VLAN Isolation
• Known Attacks
• Secure Switch Configuration
Management Channels

- Telnet: for command line interface
- SNMP: to read/write data from/to the switch
- VTP: VLAN Trunking Protocol
- VQP for VMPS Virtual Membership Policy Server
- CDP: Cisco Discovery Protocol
Using a Out of Band Management

• Cat 4000 has a dedicated physical Ethernet port for management
  can be put in a separate VLAN or even to another physical LAN

• Cat 5k & Cat 6K have a logical Ethernet port for management
  MUST be put in a VLAN
  this should be a dedicated VLAN
Out of Band Management (Cont.)

- Use topological ACL to prevent IP spoofing for the management VLAN or LAN.
- IPSec tunnel can provide authentication & confidentiality on the WAN.

Network Management

- Inbound ACL:
  - deny nms any
  - permit any any

- Outbound ACL:
  - permit nms any
  - deny any any

WAN
Management Channels: Telnet

- Telnet can give access to the command line from remote (passwords are sent in clear text)

- Two passwords:
  - login password
  - enable password
Management Channel: SSH

• On Cat 4K, 6K with CatOS 6.1 (or IOS 12.1(6)E) SSH can be used to replace Telnet

• On Cat 2950 EI and 3550 SSH is available on 12.1(11)EA1

• SSH is using 3DES to provide confidentiality to the Telnet session
Passwords

- Enable password should be different than login password
- *Physical access to console port means no password needed upon reboot*
- Passwords are stored in clear text on TFTP servers
- Passwords should be more creative than:
  - Router, switch, sanfran, cisco, enable.....
Using Radius/TACACS+

Can use one time token for login/enable authentication

```sh
CATALYST>
sel authentication login tacacs+ enable
set authentication enable tacacs+ enable
set tacacs key mysecret
set tacacs server 1.1.1.1
set tacacs server 2.2.2.2
```
Management Channels: SNMP

- SNMP is used to:
  - send traps
  - get information from switch
  - set information to switch
- three community strings (RO, RW, RW-all). Defaults *public*, *private*
- use SNMPv1 => everything in clear including community string
- Catalyst switches support SNMP V3 (DES Encryption)
Restricting Telnet/SNMP Access

- Telnet and SNMP access can be restricted to 10 IP addresses

```cisco
CATALYST>
set ip permit 192.168.1.0 255.255.255.0
set ip permit 192.168.100.1
set ip permit enable
```
VLAN Trunking Protocol (VTP)

- Used to distribute VLAN configuration among switches
- VTP is used over trunk ports
- VTP can cause more problems than it solves, consider if it is needed
- If needed, VTP can (and should) be authenticated:

```
CatOS> (enable) set vtp [domain domain_name] [mode {client | server | transparent | off}] [passwd passwd][pruning {enable | disable}] [v2 {enable | disable}]
IOS(config)#vtp password password-value
```
Potential VTP Attacks

- Most VTP attacks fall into the “nuisance” category of attacks
- DoS is possible by changing around the VLANs on multiple switches
- Disabling VTP:

  CatOS> (enable) set vtp mode transparent | off
  IOS(config)#vtp mode transparent
Management Channels: VMPS

- VLAN Membership Policy Server is used to assign a VLAN to a port based on:
  - MAC address
  - NT or Novell usernames (with URT)
VMPS Architecture

All VMPS traffic:
- clear text
- non authentication
- UDP based (spoofing trivial)
Risks with VQP

• DoS: preventing people to join the right VLAN

• impersonation: joining a desirable but forbidden VLAN
Adding Security to VMPS

Use an out of band management channel

Note: MAC addresses can be forged...
Management Channels: CDP

- Can be used to learn sensible information about the CDP sender (IP address, software version, …)
- Be sure to disable CDP on ALL non trunk ports

```
CATALYST>
set cdp disable all
set cdp enable 1/1
```
Agenda

- security myths
- management channels
- VLAN isolation
- known attacks
- secure switch configuration
VLAN Isolation

MYTH: VLAN $a$ is completely isolated from VLAN $b$

I.e. without layer 3 device, no station on one VLAN can send data to another station on another VLAN
Trunk Port Refresher

- Trunk ports have access to all VLANs by default
- Used to route traffic for multiple VLANs across the same physical link (generally used between switches)
- Encapsulation can be 802.1Q or ISL
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

• 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 Administrative States**

- Administrator configurable trunk states

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ON</td>
<td>I want to be a trunk and I don’t care what you think! (Used when the other end does not understand DTP)</td>
</tr>
<tr>
<td>OFF</td>
<td>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)</td>
</tr>
<tr>
<td>Desirable</td>
<td>I’m willing to become a VLAN trunk; are you interested? (Used when you are interested in being a trunk)</td>
</tr>
<tr>
<td>Auto</td>
<td>I’m willing to go with whatever you want! (This is the default on many switches!)</td>
</tr>
<tr>
<td>Non-Negotiate</td>
<td>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)</td>
</tr>
</tbody>
</table>
Basic VLAN Hopping Attack

- A station can spoof as a switch with ISL or 802.1Q signaling (DTP signaling is usually required as well)
- The station is then member of all VLANs
- Requires a trunking favorable setting on the port (the SANS paper is three years old)

http://www.sans.org/newlook/resources/IDFAQ/vlan.htm
Double Encapsulated 802.1Q VLAN Hopping Attack

- Send double encapsulated 802.1Q frames
- Switch performs only one level of decapsulation
- Unidirectional traffic only
- Works even if trunk ports are set to off

Note: Only Works if Trunk Has the Same Native VLAN as the Attacker (then the trunk will not append a new tag)
Disabling Auto-Trunking

- Defaults change depending on switch; always check:

  From the Cisco docs: “The default mode is dependent on the platform…”

  To check from the CLI:

  ```
  CatOS> (enable) set trunk <mod/port> off
  IOS(config-if)#switchport mode access
  ```

  ```
  CatOS> (enable) show trunk [mod|mod/port]
  IOS(config-if)#show interface type number switchport
  ```
Security Best Practices for VLANs and Trunking

- **Always** use a dedicated VLAN ID (native VLAN) for all trunk ports that is not defined as an access port on the switch.
- Disable unused ports and put them in an unused VLAN.
- Be paranoid: Do not use VLAN 1 for anything.
- Set all user ports to non-trunking (DTP Off).
Agenda

- security myths
- management channels
- VLAN isolation
- known attacks
- secure switch configuration
Spanning Tree Attacks
Spanning Tree

- Purpose: To maintain loop-free topologies in a redundant Layer 2 infrastructure
- Provides path recovery services
- Hackers are just starting to play around with STP; the “dsniff” of STP attacks has yet to be released
Spanning Tree Basics

A Switch Is Elected as Root

A ‘Tree-Like’ Loop-Free Topology Is Established

Loop-Free Connectivity
Spanning Tree Attack Example 1/2

- Send BPDU messages from attacker to force spanning tree recalculations
  Impact likely to be DoS
- Send BPDU messages to become root bridge
Spanning Tree Attack Example 2/2

- Send BPDU messages from attacker to force spanning tree recalculations
  Impact likely to be DoS

- Send BPDU messages to become root bridge
  The hacker then sees frames he shouldn’t
  MITM, DoS, etc. all possible
  Any attack is very sensitive to the original topology, trunking, PVST, etc.
  Requires attacker to be dual homed to two different switches
Spanning Tree DoS Example

• Attacker sends BPDU advertising itself with a bridge priority of zero
  - Attacker becomes root bridge
  - Spanning Tree recalculates
  - GE backbone becomes FE 🙄
  - If attack is combined with macof, it could yield more packets available to sniff
STP Attack Mitigation

- **Disable STP** (It is not needed in loop free topologies)
- **BPDU Guard**
  Disables ports using portfast upon detection of a BPDU message on the port
  Globally enabled on all ports running portfast
  Available in CatOS 5.4.1 for Cat 2K, 4K, 5K, and 6K; 12.0XE for native IOS 6K; 12.1(8a)EW for 4K Sup III; 12.1(4)EA1 for 3550; 12.1(6)EA2 for 2950

```
CatOS> (enable) set spantree portfast bpdu-guard enable

IOS(config)#spanning-tree portfast bpduguard
```

- **Root Guard**
  Disables ports who would become the root bridge due to their BPDU advertisement
  Configured on a per port basis
  Available in CatOS 6.1.1 for Cat 29XX, 4K, 5K, and 6K; 12.0(7) XE for native IOS 6K, 12.1(8a)EW for 4K Sup III; 29/3500XL in 12.0(5)XU; 2950 in 12.0(5)WC(1); 3550 in 12.1(4)EA1; 2950 in 12.1(6)EA2

```
CatOS> (enable) set spantree guard root 1/1

IOS(config)#spanning-tree guard root (or rootguard)
```
VLAN Isolation
ARP Refresher

- An ARP request message should be placed in a hardware frame and broadcast to all computers on the network.
- Each computer receives the request and examines the IP address.
- The computer mentioned in the request sends a response; all other computers process and discard the request without sending a response.
Gratuitous ARP

- Gratuitous ARP is used by hosts to "announce" their IP address to the local network and avoid duplicate IP addresses on the network. Routers and other network hardware may use cache information gained from gratuitous ARPs.
- Gratuitous ARP is a broadcast packet (like an ARP request)

- HOST W: Hey everyone I’m host W and my IP Address is 1.2.3.4 and my MAC address is 12:34:56:78:9A:BC
Misuse of gratuitous ARP

- ARP has no security or ownership of IP or MAC addresses
- What if we did the following?

- Host W broadcasts I’m 1.2.3.1 with MAC 12:34:56:78:9A:BC
- (wait 5 seconds)
- Host W broadcasts I’m 1.2.3.1 with MAC 12:34:56:78:9A:BC
A Test in the Lab

- Host X and Y will likely ignore the message unless they currently have an ARP table entry for 1.2.3.1

When host Y requests the MAC of 1.2.3.1 the real router will reply and communications will work until the timer on the gratuitous ARP kicks off

- Even a static ARP entry for 1.2.3.1 on Y will get overwritten by the gARP on some OSs (NT4, WIN2K for sure)
Dsniff – a collection of tools to do:

- ARP spoofing
- MAC flooding
- Selective sniffing
- SSH / SSL Interception

Dug Song, Author of dsniff

www.monkey.org/~dugsong/dsniff
Arpspoof in Action

C:\>test
C:\>arp -d 15.1.1.1
C:\>ping -n 1 15.1.1.1
Pinging 15.1.1.1 with 32 bytes of data:
Reply from 15.1.1.1: bytes=32 time<10ms TTL=255
C:\>arp -a
Interface: 15.1.1.26 on Interface 2
    Internet Address  Physical Address  Type
    15.1.1.1          00-04-4e-f2-d8-01  dynamic
    15.1.1.25         00-10-83-34-29-72  dynamic
C:\>arp -a
Interface: 15.1.1.26 on Interface 2
    Internet Address  Physical Address  Type
    15.1.1.1          00-10-83-34-29-72  dynamic
    15.1.1.25         00-10-83-34-29-72  dynamic

[root@hacker-lnx dsniff-2.3]# ./arpspoof 15.1.1.1
0:4:43:f2:d8:1 ff:ff:ff:ff:ff:ff 0806 42: arp reply
    15.1.1.1 is-at 0:4:4e:f2:d8:1
0:4:43:f2:d8:1 ff:ff:ff:ff:ff:ff 0806 42: arp reply
    15.1.1.1 is-at 0:4:4e:f2:d8:1
0:4:43:f2:d8:1 ff:ff:ff:ff:ff:ff 0806 42: arp reply
    15.1.1.1 is-at 0:4:4e:f2:d8:1
More on Arpspoof

- All Traffic now flows through machine running dsniff in a half-duplex manner
  
  Not quite a sniffer but fairly close

- Port security doesn’t help

- Note that attack could be generated in the opposite direction by spoofing the destination host when the router sends its ARP request (more difficult because of race condition)
ARP Spoof Mitigation: Private VLANs

• What is a ‘Private’ VLAN?

A specific kind of VLAN (useful for DMZ, …)

Isolated ports *(usually hosts)* cannot talk to each other but only to designated promiscuous ports *(usually routers or firewalls)*

‘Private’ VLANs and normal VLANs can exist simultaneously in the same switch
ARP Spoof Mitigation: Private VLANs

Only One Subnet!

Primary VLAN
Community VLAN
Community VLAN
Isolated VLAN

Consider Local Proxy ARP as an option for host to host communication without broadcasts
Normal CAM Behaviour 1/3

MAC A

MAC B

MAC C

Port 1

Port 2

Port 3

MAC | port
---|---
A | 1
C | 3

A->B

I see traffic to B!

B unknown… flood the frame

A->B
Normal CAM Behaviour 2/3

MAC A

MAC B

MAC C

Port 1

Port 2

Port 3

MAC  | port
---|---
A  | 1
B  | 2
C  | 3

A is on port 1
learn:
B is on port 2
Normal CAM Behaviour 3/3

MAC A

MAC B

MAC C

Port 1

Port 2

Port 3

MAC | port
---|---
A | 1
B | 2
C | 3

A->B

A->B

B is on port 2

I do not see traffic to B!

B is on port 2

I do not see traffic to B!
CAM Overflow 1/3

- theoretical attack until May 1999
- *macof* cracker tool since May 1999 *(about 100 lines of perl)*
- based on the limited size of CAM
CAM Overflow 2/3

MAC A

MAC B

MAC C

Port 1

Port 2

Port 3

MAC port
X 3
Y 3
C 3

X is on port 3

Y is on port 3

X ->?

Y ->?
CAM Overflow 3/3

MAC Overflow Table:

<table>
<thead>
<tr>
<th>MAC</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>3</td>
</tr>
<tr>
<td>Y</td>
<td>3</td>
</tr>
<tr>
<td>C</td>
<td>3</td>
</tr>
</tbody>
</table>

- MAC A
- MAC B
- MAC C

Port 1:
- A -> B

Port 2:
- A -> B

I see traffic to B!

Port 3:
- A -> B

B unknown… flood the frame
MAC Flooding switches with Dsniff

[root@hacker-lnx dsniff-2.3]# ./macof
101.59.29.36 -> 60.171.137.91 TCP D=55934 S=322 Syn Seq=1210303300 Len=0 Win=512
145.123.46.9 -> 57.11.96.103 TCP D=44686 S=42409 Syn Seq=1106243396 Len=0 Win=52
109.40.136.24 -> 51.158.227.98 TCP D=59038 S=21289 Syn Seq=2039821840 Len=0 Win=2
126.121.183.80 -> 151.241.231.59 TCP D=7519 S=34044 Syn Seq=310542747 Len=0 Win=2
211.28.168.72 -> 91.247.223.23 TCP D=62807 S=53618 Syn Seq=2084851907 Len=0 Win=2
183.159.196.56 -> 133.10.138.7 TCP D=23929 S=51034 Syn Seq=1263121444 Len=0 Win=2
19.113.88.77 -> 16.189.146.61 TCP D=1478 S=56820 Syn Seq=609596358 Len=0 Win=512
237.162.172.114 -> 51.32.8.36 TCP D=38433 S=31784 Syn Seq=410116516 Len=0 Win=2
118.34.90.6 -> 61.169.58.50 TCP D=42232 S=31424 Syn Seq=1070019027 Len=0 Win=52
46.205.246.13 -> 72.165.185.7 TCP D=56224 S=34492 Syn Seq=937536798 Len=0 Win=52
105.109.246.116 -> 252.233.209.72 TCP D=23840 S=45783 Syn Seq=1072699351 Len=0 Win=2
60.244.56.84 -> 142.93.179.59 TCP D=3453 S=4112 Syn Seq=1964543236 Len=0 Win=512
151.126.212.86 -> 106.205.161.66 TCP D=12959 S=42911 Syn Seq=1028677526 Len=0 Win=2
9.121.248.84 -> 199.35.30.115 TCP D=3377 S=31735 Syn Seq=1395858847 Len=0 Win=2
226.216.132.20 -> 189.89.89.110 TCP D=26975 S=57485 Syn Seq=1783586857 Len=0 Win=2
124.54.134.104 -> 235.83.143.109 TCP D=23135 S=55908 Syn Seq=852982595 Len=0 Win=2
27.54.72.62 -> 207.73.65.108 TCP D=54512 S=25534 Syn Seq=1571701185 Len=0 Win=2
246.109.199.72 -> 1.131.122.89 TCP D=6131 S=43891 Syn Seq=1443011876 Len=0 Win=2
251.49.6.89 -> 18.168.34.97 TCP D=25959 S=956 Syn Seq=6153014 Len=0 Win=512
51.105.154.55 -> 225.89.20.119 TCP D=33931 S=1893 Syn Seq=116924142 Len=0 Win=52
82.2.236.125 -> 210.40.246.122 TCP D=43954 S=49355 Syn Seq=1263650806 Len=0 Win=2
70.63.102.43 -> 69.88.108.26 TCP D=61968 S=53055 Syn Seq=682544782 Len=0 Win=512
CAM Table Full!

- Dsniff (macof) can generate 155,000 MAC entries on a switch per minute
- Assuming a perfect hash function the CAM table will total out at 128,000 (16,000 x 8) 131,052 to be exact
  - Since hash isn’t perfect it actually takes 70 seconds to fill the cam table
- Once table is full, traffic without a CAM entry floods on the VLAN, existing traffic NOT

Snoop output on non-SPAN port

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Destination IP</th>
<th>Packet Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.1.22</td>
<td>(broadcast)</td>
<td>ARP C Who is 10.1.1.1, 10.1.1.1?</td>
</tr>
<tr>
<td>10.1.1.22</td>
<td>(broadcast)</td>
<td>ARP C Who is 10.1.1.19, 10.1.1.19?</td>
</tr>
<tr>
<td>15.1.1.26</td>
<td>15.1.1.25</td>
<td>ICMP Echo request (ID: 256 Sequence number: 7424) ← OOPS</td>
</tr>
<tr>
<td>15.1.1.25</td>
<td>15.1.1.26</td>
<td>ICMP Echo reply (ID: 256 Sequence number: 7424) ← OOPS</td>
</tr>
</tbody>
</table>
MAC flooding mitigation

- Port Security
  Beware management and performance hit

Lots of options besides just “ON/OFF”

1025 MAC entries into table + 1 per port

“Restrict” option will fail under dsniff load and disable the port

set port security 3/21 enable age 10 maximum 5 violation restrict

2001 Jul 03 15:40:32 %SECURITY-1-PORTSHUTDOWN:Port 3/21 shutdown due to no space
Selective Sniffing

• Once traffic is flooded through either of the previous two methods, Dsniff obtains passwords:

[root@hacker-lnx dsniff-2.3]# ./dsniff -c
dsniff: listening on eth0
-----------------
(http)
GET /SERVICE/Paging/page/ HTTP/1.1
Host: wwwin-apps.cisco.com
Authorization: Basic c2Nvd1gh39UNMRH4lejDmaA== [myuser:mypassword]

Supports more than 30 standardized / proprietary protocols: FTP, Telnet, SMTP, HTTP, POP, poppass, NNTP, IMAP, SNMP, LDAP, Rlogin, RIP, OSPF, PPTP MS-CAP, NFS, YP/NIS, SOCKS, X11, CVS, IRC, AIM, ICQ, Napster, PostgreSQL, Meeting Maker, Citrix ICA, Symantec pcAnywhere, NAI Sniffer, Microsoft SMB, Oracle SQL*Net, Sybase et Microsoft SQL.
SSL / SSH Interception

- Using dnsspoof, all web sites can resolve to the dsniff host IP address:

  C:\>ping www.amazon.com

  Pinging www.amazon.com [15.1.1.25] with 32 bytes of data:

  Reply from 15.1.1.25: bytes=32 time<10ms TTL=249
  Reply from 15.1.1.25: bytes=32 time<10ms TTL=249
  Reply from 15.1.1.25: bytes=32 time<10ms TTL=249
  Reply from 15.1.1.25: bytes=32 time<10ms TTL=249

- Once that happens you can proxy all web connections through the dsniff host
SSL / SSH Interception

- Using dsniff (webmitm) most SSL sessions can be intercepted and bogus certificate credentials can be presented.
SSL / SSH Interception

• Upon inspection they will look invalid but they would likely fool most users
Attack Summary

- Switches can be sniffed without SPAN
- ARP has no security
- Switches fail open under load
Private VLAN Attacks 1/2

Attacker
Mac:A IP:1

Victim
Mac:B IP:2

Router
Mac:C IP:3

PVLANs Work Drop Packet

S:A1 D:B2

Promiscuous Port
Isolated Port
Private VLAN Attacks 2/2

- Only allows unidirectional traffic (Victim will ARP for A and fail)
- If both hosts were compromised, setting static ARP entries for each other via the router will allow bi-directional traffic
- Most firewalls will not forward the packet like a router
- Note: this is not a PVLAN vulnerability as it enforced the rules!
PVLAN Attack Mitigation

• Setup ACL on ingress router port:

```plaintext
IOS(config)#access-list 101 deny ip local-subnet 1 submask local-subnet 1 submask log
IOS(config)#access-list 101 permit ip any any
IOS(config-if)#ip access-group 101 in
```

• All known PVLAN exploits will now fail

• VLAN ACL (VACL) could also be used
Agenda

- Security Myths
- Management Channels
- VLAN Isolation
- Known Attacks
- Secure Switch Configuration
Secure Management Channels

- Set login/enable passwords
- use out of band management
- Use SSH instead of Telnet
- change SNMP community string
- use `set ip permit` to restrict telnet/SNMP access
- disable CDP on station ports
- disable trunking on station ports
- use password authentication for VTP
- do not rely on port security
Secure Management Channels

- Use TACACS+ and one time passwords
- do not use VTP
- do not use CDP at all
- do not use VMPS
- put all unused ports to a dummy VLAN without any layer 3 device
802.1x is a client-server-based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible ports.

1. User activates link (i.e. PC Powers on)
2. Switch requests Authentication Server if user authorised to access LAN
3. Authentication Server responds with authority access
4. Switch opens controlled port (if authorised) for user to access LAN
IEEE 802.1x (Terminology)

Supplicant PAE (Port Access Entity)

Authentication Server

Extensible Authentication Protocol over LAN

Authenticator PAE
IEEE 802.1x
(Switch Authentication)

For each 802.1x switch port, the switch creates TWO virtual access points at each port.

The controlled port is open only when the device connected to the port has been authorized by 802.1x.

Uncontrolled port provides a path for EAPOL (Extensible Authentication Protocol over LAN) traffic ONLY.
Layer 2 Security Best Practices 1/2

- Manage switches in as secure a manner as possible (SSH, OOB, permit lists, etc.)
- **Always** use a dedicated VLAN ID for all trunk ports
- Be paranoid: do not use VLAN 1 for anything
- Set all user ports to non trunking
- Deploy port-security where possible for user ports
- Selectively use SNMP and treat community strings like root passwords
- Have a plan for the ARP security issues in your network
Layer 2 Security Best Practices 2/2

- Enable STP attack mitigation (BPDU Guard, Root Guard)
- Use private VLANs where appropriate to further divide L2 networks
- Use MD5 authentication for VTP
- Use CDP only where necessary
- Disable all unused ports and put them in an unused VLAN
- Consider 802.1X for the future

All of the Preceding Features Are Dependant on Your Own Security Policy
## Catalyst Switch Feature Support

<table>
<thead>
<tr>
<th>Feature</th>
<th>Cat 2900 XL</th>
<th>Cat 3500 XL</th>
<th>Cat 2950</th>
<th>Cat 3550</th>
<th>Cat 29XX G</th>
<th>CatOS 4000</th>
<th>CatOS 6000</th>
<th>IOS 4000</th>
<th>IOS 6000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Security</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Private VLANs</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>STP BPDU Guard</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>STP Root Guard</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>SSH Support</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>VMPS Client</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>VMPS Server</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.1X Auth</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Wire Rate ACLs</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Further Reading

- SAFE Blueprints
  http://www.cisco.com/go/safe

- Improving Security on Cisco Routers

- Securing Networks with Private VLANs and VLAN Access Control Lists

- Links in this presentation:
  Port security:
  http://cisco.com/univercd/cc/td/doc/product/lan/cat5000/rel_5_4/config/sec_port.htm
  SANS VLAN paper (out of date):
  http://www.sans.org/newlook/resources/IDFAQ/vlan.htm
  PVLAN details:
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_7_1/conf_gd/vlans.htm#xtocid854519