SAFE LAYER 2 SECURITY IN-DEPTH—VERSION 2

This document is an addendum for the SAFE Enterprise white paper describing Layer 2 network attacks as well as best practices for securing virtual LANs.

AUTHORS

Ido Dubrawsky is the author of this white paper. Ido is a network security architect and a member of the SAFE Architecture team in Cisco Systems, Inc.'s VPN and Security business unit. Additionally Sean Convery (CCIE #4232) provided significant input in the development of this white paper.

INTRODUCTION

The SAFE Enterprise white paper published by Cisco Systems® discusses various network attacks on a large-scale enterprise network. These network attacks are based on the premise that each device on the network is a potential target. During the time since the original publication date of the SAFE Enterprise white paper, significant research on network attacks has been conducted, focusing on Layer 2 of the OSI reference model. This research has prompted the need for an update to the white paper focusing on more specific requirements to protect Layer 2 in the network infrastructure.

GENERAL SWITCH OPERATION

Unlike hubs, switches are able to regulate the flow of data between their ports by creating almost "instant" networks that contain only the two end devices communicating with each other at that moment in time. Data frames are sent by end systems and their source and destination addresses are not changed throughout the switched domain. Switches maintain Content-Addressable Memory (CAM) lookup tables to track the source addresses located on the switch ports. These lookup tables are populated by an address-learning process on the switch. If the destination address of a frame is not known or if the frame received by the switch is destined for a broadcast or multicast address, the switch forwards the frame out all ports. With their ability to isolate traffic and create the "instant" networks, switches can be used to divide a physical network into multiple logical, or virtual LANs (VLANs) through the use of Layer 2 traffic segmentation.

VLANs

VLANs allow network administrators to divide their physical networks into a set of smaller logical networks. Like their physical counterparts, each VLAN consists of a single broadcast domain that is isolated from other VLANs. VLANs work by tagging packets with an identification header and then restricting the ports that the tagged packets can be received on to those that are part of the VLAN. The two most prevalent VLAN tagging techniques are the IEEE 802.1q tag and the Cisco® Inter-Switch Link (ISL) tag.

The ISL header format is shown in Figure 1 and the 802.1q VLAN header format is shown in Figure 2. The VLAN header is inserted at Layer 2 and the information contained within the tags is used to identify which VLAN the traffic belongs to. Only those ports that belong to the VLAN specified in the header are capable of receiving the traffic. The destination address then further specifies the particular port within the VLAN where the traffic is destined.

Figure 1
ISL Tag Header Structure

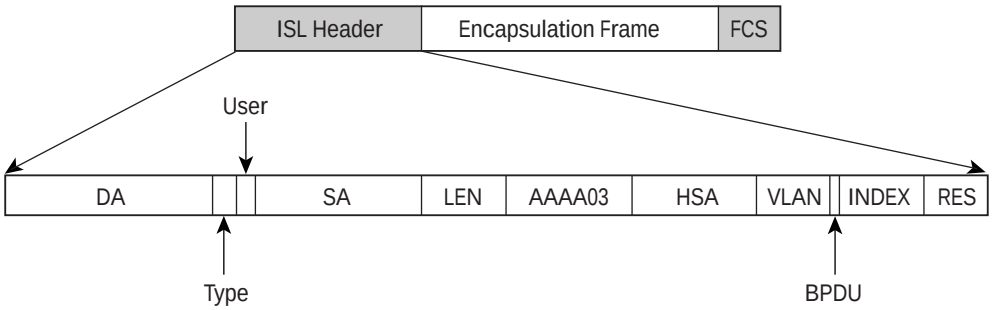
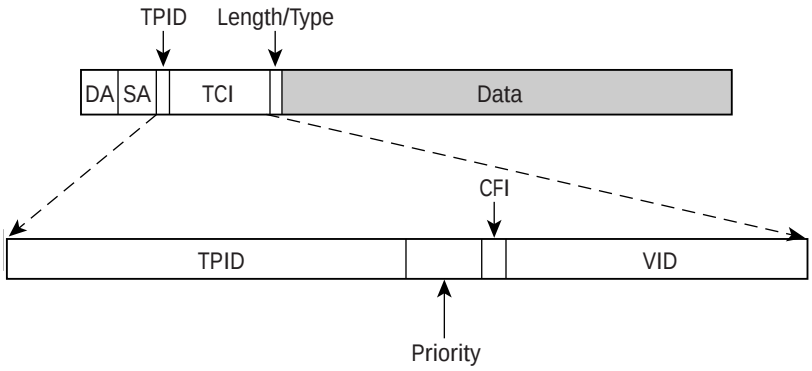


Figure 2
802.1q Header Structure



SWITCHES ARE TARGETS

Like routers, both Layer 2 and Layer 3 switches have their own sets of network security requirements. But not as much public information is available about the network security risks in switches and what can be done to mitigate those risks. Switches are susceptible to many of the same Layer 3 attacks as routers. Most of the network-security techniques detailed in the section of the SAFE Enterprise white paper titled "Routers Are Targets" also apply to switches. However, switches, and Layer 2 of the OSI reference model in general, are subject to network attacks in unique ways. These include:

- CAM table overflow
- VLAN hopping
- Spanning-Tree Protocol manipulation
- Media Access Control (MAC) Address spoofing
- Private VLAN
- DHCP "starvation"

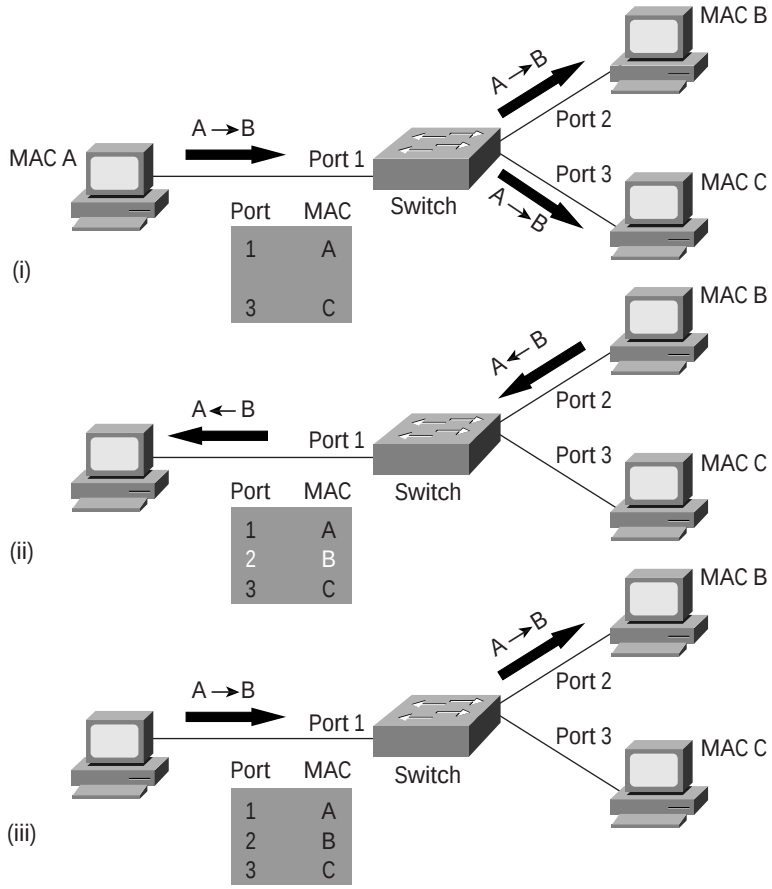
This paper explores each of these types of network attacks as well as provides recommendations for how to mitigate or reduce the effects of these attacks. Finally, risks involved with using Cisco Discovery Protocol and VLAN Trunking Protocol are discussed.

NETWORK ATTACKS

CAM Table Overflow

The CAM table in a switch contains information such as the MAC addresses available on a given physical port of a switch, as well as the associated VLAN parameters. When a Layer 2 switch receives a frame, the switch looks in the CAM table for the destination MAC address. If an entry exists for the MAC address in the CAM table, the switch forwards the frame to the port designated in the CAM table for that MAC address. If the MAC address does not exist in the CAM table, the switch forwards the frame out every port on the switch, effectively acting like a hub. If a response is seen, the switch updates the CAM table. Figure 3 shows this operation. In this figure host A sends traffic to host B. The switch receives the frames and looks up the destination MAC address in its CAM table. If the switch cannot find the destination MAC in the CAM table it then copies the frame and broadcasts it out all of the switch ports (i). Host B receives the frame and sends back a reply to host A. The switch then sees that the MAC address for host B is located on port 2 and writes that information into the CAM table (ii). Now, any frame sent by host A (or any other host) to host B will simply be forwarded to port 2 of the switch and not broadcast out every port as was done earlier (iii).

Figure 3
MAC CAM Table Operation

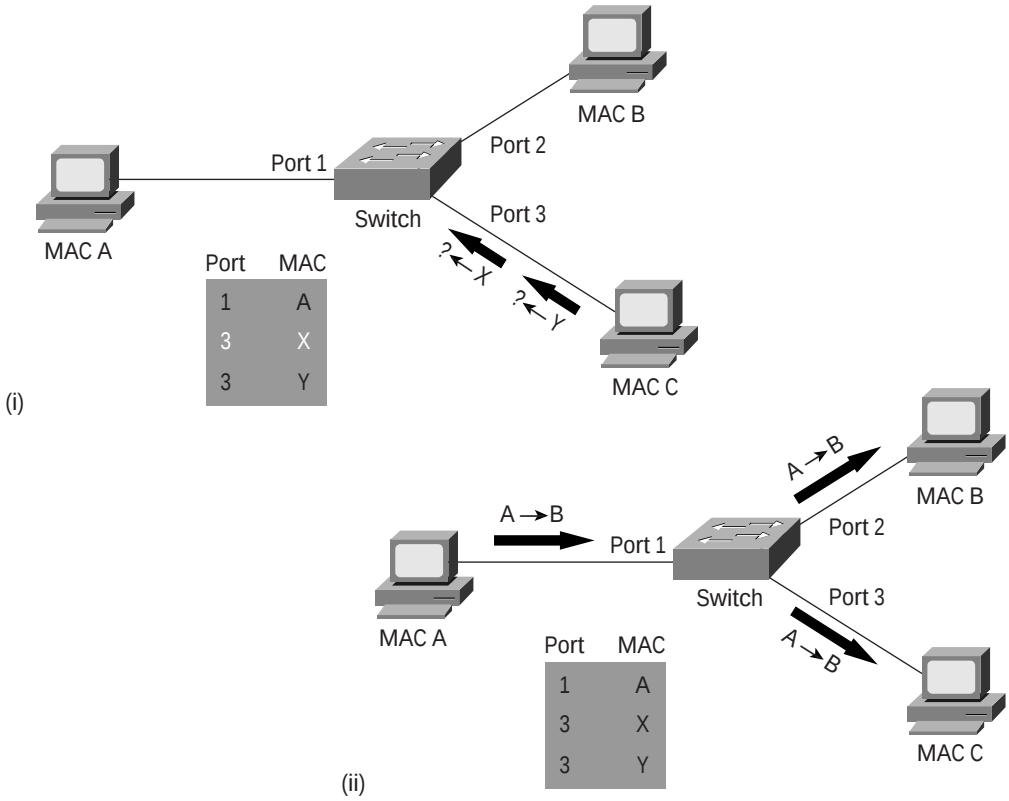


CAM tables are limited in size. If enough entries are entered into the CAM table before other entries are expired, the CAM table fills up to the point that no new entries can be accepted. Typically a network intruder will flood the switch with a large number of invalid-source MAC addresses until the CAM table fills up. When that occurs the switch will flood all ports with incoming traffic because it cannot find the port number for a particular MAC address in the CAM table. The switch, in essence, acts like a hub. If the intruder does not maintain the flood of invalid-source MAC addresses, the switch will eventually time out older MAC address entries from the CAM table and begin to act like a switch again. CAM table overflow only floods traffic within the local VLAN so the intruder will see only traffic within the local VLAN to which he or she is connected.

In May of 1999 the tool *macof* was released. It was written in approximately 100 lines of PERL code and was later ported to C language code and incorporated into the *dsniff* package. This tool floods a switch with packets containing randomly generated source and destination MAC and IP addresses. When the switch's CAM table fills up with these addresses, the switch begins to forward all frames it receives to every port. Figure 4 illustrates a CAM table-overflow attack. In this figure the host with MAC address C in the bottom right of each frame is sending out multiple packets with various source MAC addresses. Over a short period of time the CAM table in the switch fills

up until it cannot accept new entries. As long as macof is left running, the CAM table on the switch will remain full. When this happens the switch begins to broadcast all packets which it receives out of every port so that packets sent from host A to host B are also broadcast out of port 3 on the switch.

Figure 4
CAM Table-Overflow Attack



Network Attack Mitigation

The CAM table-overflow attack can be mitigated by configuring port security on the switch. This option provides for either the specification of the MAC addresses on a particular switch port or the specification of the number of MAC addresses that can be learned by a switch port. When an invalid MAC address is detected on the port, the switch can either block the offending MAC address or shut down the port.

Specifying MAC addresses on switch ports is far too unmanageable a solution for a production environment. Limiting the number of MAC addresses on a switch port is manageable. A more administratively scalable solution would be the implementation of dynamic port security at the switch. To implement dynamic port security, specify a maximum number of MAC addresses that will be learned as shown in the second example below.

Command Samples to Mitigate CAM Table-Overflow Attacks

CatOS> (enable) **set port security** *mod_num/port_num* **enable** *[mac_addr]*
CatOS> (enable) **set port security** *mod_num/port_range* **enable maximum** *[max_mac_addr]*
CatOS> (enable) **set port security** *mod_num/port_num mac_addr*
CatOS> (enable) **show port** *[mod_num[/port_num]*

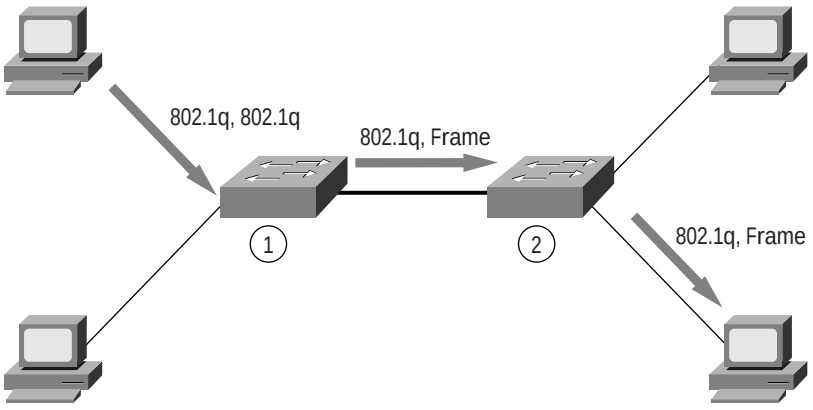
VLAN Hopping

VLAN hopping is a network attack whereby an end system sends out packets destined for a system on a different VLAN that cannot normally be reached by the end system. This traffic is tagged with a different VLAN ID to which the end system belongs. Or, the attacking system may be trying to behave like a switch and negotiate trunking so that the attacker can send and receive traffic between other VLANs.

Switch Spoofing—In a VLAN hopping attack, the network attacker configures a system to spoof itself as a switch. This requires that the network attacker be capable of emulating either ISL or 802.1q signaling along with Dynamic Trunk Protocol (DTP) signaling. Using this method a network attacker can make a system appear to be a switch with a trunk port. If successful, the attacking system then becomes a member of all VLANs.

Double Tagging—Another version of this network attack involves tagging the transmitted frames with two 802.1q headers in order to forward the frames to the wrong VLAN (Figure 5). The first switch to encounter the double-tagged frame (1) strips the first tag off the frame and forwards the frame. The result is that the frame is forwarded with the inner 802.1q tag out all the switch ports (2) including trunk ports configured with the native VLAN of the network attacker. The second switch then forwards the packet to the destination based on the VLAN identifier in the second 802.1q header.

Figure 5
VLAN Hopping with Double-Encapsulated 802.1q Traffic



Network Attack Mitigation

Mitigating VLAN hopping attacks requires several modifications to the VLAN configuration. One of the more important elements is to use dedicated VLAN IDs for all trunk ports. Also, disable all unused switch ports and place them in an unused VLAN. Set all user ports to nontrunking mode by explicitly turning off DTP on those ports.

Command Samples to Disable Auto-Trunking (CatOS)

CatOS> (enable) set trunk *mod_num/port_num* off

or

CatOS> (enable) set port host *mod_num/port_range*

Command Samples to Disable Auto-Trunking (IOS)

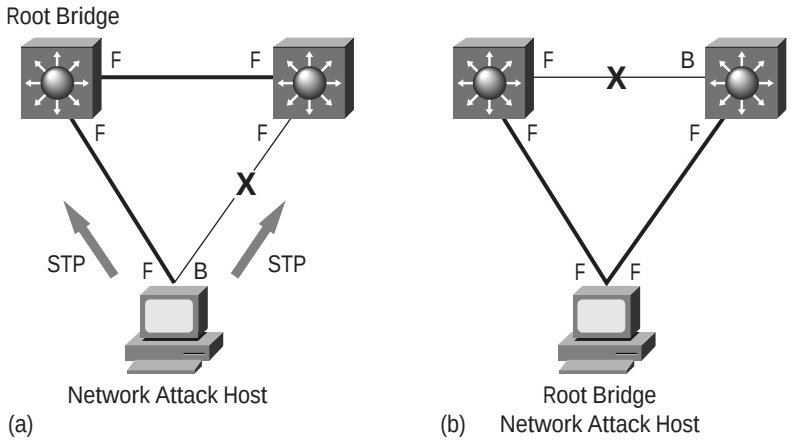
IOS# (config-if) switchport mode access

Spanning-Tree Protocol Manipulation

Another attack against switches involves intercepting traffic by attacking the Spanning-Tree Protocol. This protocol is used in switched networks to prevent the creation of bridging loops in an Ethernet network topology. Upon bootup the switches begin a process of determining a loop-free topology. The switches identify one switch as a root bridge and block all other redundant data paths.

By attacking the Spanning-Tree Protocol, the network attacker hopes to spoof his or her system as the root bridge in the topology. To do this the network attacker broadcasts out Spanning-Tree Protocol Configuration/Topology Change Bridge Protocol Data Units (BPDUs) in an attempt to force spanning-tree recalculations. The BPDUs sent out by the network attacker's system announce that the attacking system has a lower bridge priority. If successful, the network attacker can see a variety of frames. Figure 6 illustrates how a network attacker can use Spanning-Tree Protocol to change the topology of a network so that it appears that the network attacker's host is a root bridge with a higher priority. By transmitting spoofed Spanning-Tree Protocol packets, the network attacker causes the switches to initiate spanning-tree recalculations that then result in the two connections to the network attacker's system to forward packets.

Figure 6
Traffic Interception Using Spanning-Tree Protocol



Network Attack Mitigation

To mitigate Spanning-Tree Protocol manipulation use the root guard and the BPDU guard enhancement commands to enforce the placement of the root bridge in the network as well as enforce the Spanning-Tree Protocol domain borders. The root guard feature is designed to provide a way to enforce the root-bridge placement in the network. The Spanning-Tree Protocol BPDU guard is designed to allow network designers to keep the active network topology predictable. While BPDU guard may seem unnecessary given that the administrator can set the bridge priority to zero, there is still no guarantee that it will be elected as the root bridge because there might be a bridge with priority zero and a lower bridge ID. BPDU guard is best deployed towards user-facing ports to prevent rogue switch network extensions by an attacker.

Command Samples to Mitigate Spanning-Tree Protocol Manipulation Attacks

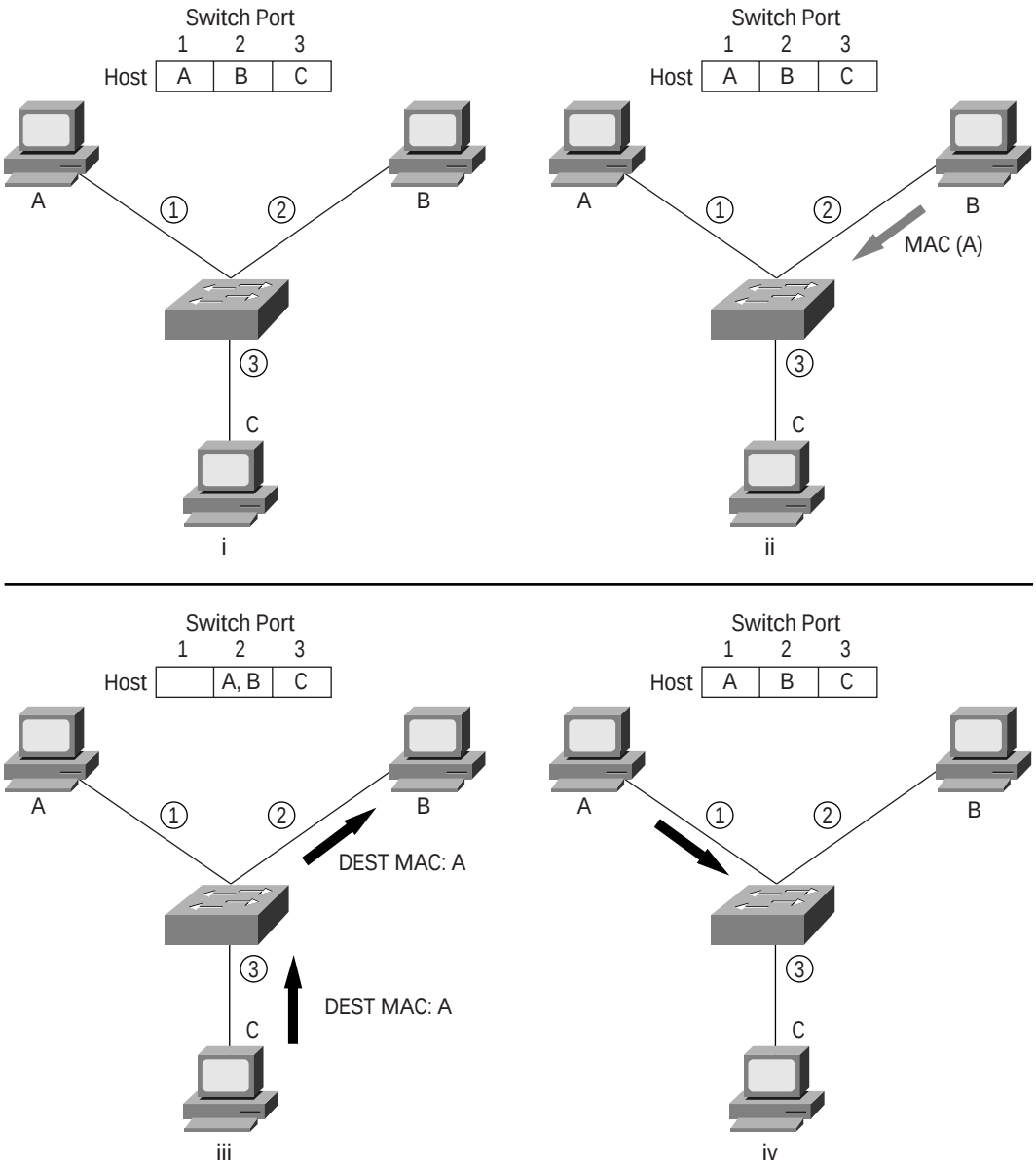
CatOS> set spantree portfast bpdu guard enable
CatOS> set spantree guard root *mod_num/port_num*

MAC Spoofing Attack

MAC spoofing attacks involve the use of a known MAC address of another host to attempt to make the target switch forward frames destined for the remote host to the network attacker. By sending a single frame with the other host's source Ethernet address, the network attacker overwrites the CAM table entry so that the switch forwards packets destined for the host to the network attacker. Until the host sends traffic it will not receive any traffic. When the host sends out traffic, the CAM table entry is rewritten once more so that it moves back to the original port.

Figure 7 shows how MAC spoofing works. In frame (i) the switch has learned that Host A is on port 1, Host B is on port 2, and Host C is on port 3. Host B sends out a packet identifying itself as Host B's IP address but with Host A's MAC address or another packet with the same IP address and MAC address combination (ii). This traffic causes the frame to move the location of Host A in its CAM table from port 1 to port 2. Traffic from Host C destined to Host A is now visible to Host B (iii). To correct this situation, Host A must send out traffic on the switch port for the switch to "relearn" the location of Host A's MAC address (iv).

Figure 7
MAC Spoofing Attack



Address Resolution Protocol Spoofing—ARP or Address Resolution Protocol is used to map IP addressing to MAC addresses in a local area network segment where hosts of the same subnet reside. Normally, a host will send out a broadcast ARP request to find the MAC address of another host with a particular IP address and an ARP response will come from the host whose address matches the request. The requesting host will then cache this ARP response. Within the ARP protocol another provision is made for hosts to perform unsolicited ARP replies. The unsolicited ARP replies are called gratuitous ARPs (GARP). GARP can be exploited maliciously by an attacker to spoof the identity of an IP address on a LAN segment. Typically, this is used to spoof the identity between two hosts or all traffic to and from a default gateway in a Man in the Middle attack.

By crafting an ARP reply, a network attacker can make his or her system appear to be the destination host sought by the sender. The ARP reply causes the sender to store the MAC address of the network attacker's system in the ARP cache. This MAC address is also stored by the switch in its CAM table. In this way the network attacker has inserted the MAC address of his or her system into both the switch's CAM table and the sender's ARP cache. This allows the network attacker to intercept frames destined for the host that he or she is spoofing.

Network Attack Mitigation

Use the port security commands to mitigate MAC-spoofing attacks. The port security command provides the capability to specify the MAC address of the system connected to a particular port. The command also provides the ability to specify an action to take if a port-security violation occurs. However, as with the CAM table-overflow attack mitigation, specifying a MAC address on every port is an unmanageable solution. Hold-down timers in the interface configuration menu can be used to mitigate ARP spoofing attacks by setting the length of time an entry will stay in the ARP cache. However, hold-down timers by themselves are insufficient. Modification of the ARP cache expiration time on all end systems would be required as well as static ARP entries. Even in a small network this approach does not scale well. One solution would be to use private VLANs to help mitigate these network attacks.

Command Samples to Mitigate MAC Spoofing (Cisco Catalyst® Operating System [Catalyst OS])

CatOS> **set port security** *mod_num/port_num* **enable** *[mac_addr]*
CatOS> **set port security** mod_num/port_num mac_addr
CatOS> **set port security** mod_num/port_num **violation** {shutdown | restrict}
CatOS> **show port** *[mod_num[/port_num]*

Command Samples to Mitigate MAC Spoofing (Cisco IOS® Software)

IOS(config-if)# **port security max-mac-count** {1-132}
IOS(config-if)# **port security action** {**shutdown**|**trap**}
IOS(config-if)# **arp timeout** *seconds*

Another solution that can be used to mitigate various ARP-based network exploits is the use of DHCP snooping along with Dynamic ARP Inspection (DAI). These Catalyst feature validate ARP packets in a network and permit the interception, logging, and discarding of ARP packets with invalid MAC address to IP address bindings.

DHCP Snooping provides security by filtering trusted DHCP messages and then using these messages to build and maintain a DHCP snooping binding table. DHCP Snooping considers DHCP messages originating from any user facing port that is not a DHCP server port or an upling to a DHCP server as untrusted. From a DHCP Snooping perspective these untrusted, user-facing ports should not send DHCP server type responses such as DHCPOffer, DHCPAck, or DHCPNak. Untrusted DHCP messages are messages received from outside the network or firewall. The DHCP snooping binding table contains the MAC address, IP address, lease time, binding type, VLAN number, and interface information corresponding to the local untrusted interfaces of a switch; it does not contain information regarding hosts interconnected with a trusted interface. An untrusted interface is an interface configured to receive messages from outside the network or firewall. A trusted interface is an interface that is configured to receive only messages from within the network. The DHCP snooping binding table can contain both dynamic as well as static MAC address to IP address bindings.

DAI determines the validity of an ARP packet based on the valid MAC address to IP address bindings stored in a DHCP snooping database. Additionally, DAI can validate ARP packets based on user-configurable ACLs. This allows for the inspection of ARP packets for hosts using statically configured IP addresses. DAI allows for the use of per-port and VLAN Access Control Lists (PACLs) to limit ARP packets for specific IP addresses to specific MAC addresses.

Command Samples to Mitigate MAC Spoofing Using Dynamic ARP Inspection

Configuring DHCP Snooping (Cisco IOS Software)

switch(config)# ip dhcp snooping
switch(config)# ip dhcp snooping vlan *vlan_id [,vlan_id]*
switch(config-if)# ip dhcp snooping trust
Switch(config-if)# ip dhcp snooping limit rate *rate*

Configuring ARP Inspection with Static ACLs (Cisco Catalyst Operating System [Catalyst OS])

CatOS> (enable) set security acl ip VLAN03 permit arp-inspection host 10.16.17.1 00-d0-b7-11-13-14
CatOS> (enable) set security acl ip VLAN03 deny arp-inspection host 10.16.17.1 any log
CatOS> (enable) set security acl ip VLAN03 permit arp-inspection host 10.16.17.2 00-d0-00-ea-43-fc
CatOS> (enable) set security acl ip VLAN03 deny arp-inspection host 10.0.2.2 any log
CatOS> (enable) set security acl ip VLAN03 permit arp-inspection any any
CatOS> (enable) set security acl ip VLAN03 permit ip any any
CatOS> (enable) commit security acl VLAN03

Configuring Dynamic ARP Inspection with DHCP Snooping (Cisco IOS Software)

Switch(config)# ip arp inspection vlan *vlan_id[,vlan_id]*
Switch(config)# ip arp inspection validate src-mac dst-mac ip
Switch(config-if)# ip arp inspection trust

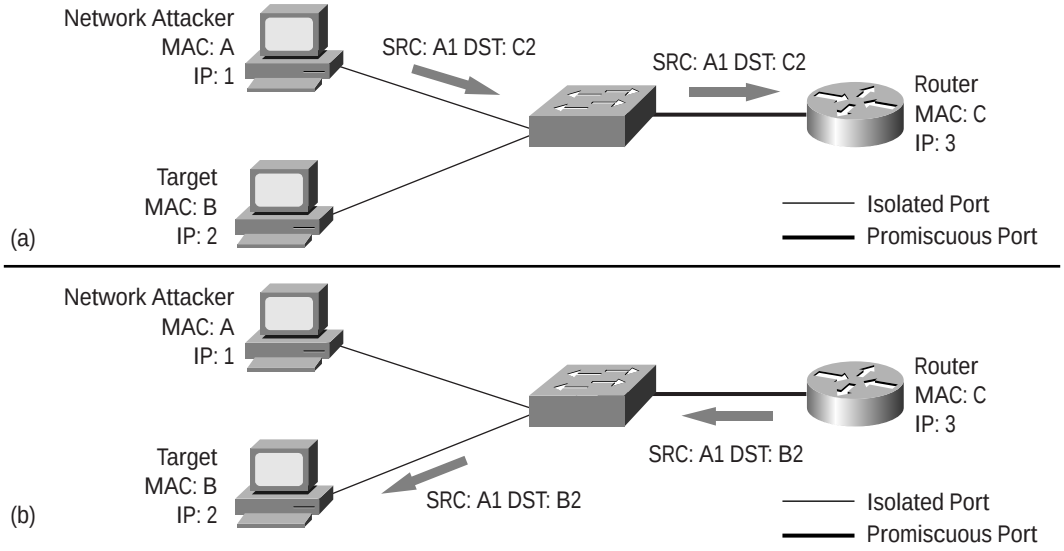
Private VLAN Attacks

While private VLANs are a common mechanism to restrict communications between systems on the same logical IP subnet, they are not a full-proof mechanism. Private VLANs work by limiting the ports within a VLAN that can communicate with other ports in the same VLAN. Isolated ports within a VLAN can communicate only with promiscuous ports. Community ports can communicate only with other members of the same community and promiscuous ports. Promiscuous ports can communicate with any port. One network attack capable of bypassing the network security of private VLANs involves the use of a proxy to bypass access restrictions to a private VLAN.

Proxy Attack—In this network attack against private VLANs, frames are forwarded to a host on the network connected to a promiscuous port such as a router. In Figure 8 the network attacker sends a packet with the source-IP and MAC address of his or her device, a destination IP address of the target system, but a destination MAC address of the router. The switch forwards the frame to the router's switch port. The router routes the traffic, rewrites the destination MAC address as that of the target, and sends the packet back out. Now the packet has the proper format as shown in Figure 8 and is forwarded to the target system. This network attack allows only for unidirectional traffic

because any attempt by the target to send traffic back will be blocked by the private VLAN configuration. If both hosts are compromised, static ARP entries could be used to allow bidirectional traffic. This scenario is not a private VLAN vulnerability because all the rules of private VLANs were enforced; however, the network security was bypassed.

Figure 8
Private VLAN Proxy Attack



Network Attack Mitigation

Configure access control lists (ACLs) on the router port to mitigate private VLAN attacks. Virtual ACLs can also be used to help mitigate the effects of private VLAN attacks. An example of using ACLs on the router port is if a server-farm segment were 172.16.34.0/24, then configuring the following ACLs on the default gateway would mitigate the private VLAN proxy attack.

Command Samples to Mitigate Private VLAN Proxy Attack

```
IOS(config)# access-list 101 deny ip 172.16.34.0 0.0.0.255 172.16.34.0 0.0.0.255 log
IOS(config)# access-list 101 permit ip any any
IOS(config-if)# ip access-group 101 in
```

DHCP Starvation

A DHCP starvation attack works by broadcasting DHCP requests with spoofed MAC addresses. This is easily achieved with attack tools such as gobbler. If enough requests are sent, the network attacker can exhaust the address space available to the DHCP servers for a period of time. This is a simple resource starvation attack just like a SYN flood is a starvation attack. The network attacker can then set up a rogue DHCP server on his or her system and respond to new DHCP requests from clients on the network. Exhausting all of the DHCP addresses is not *required* to introduce a rogue DHCP server, though. As stated in RFC 2131:

"The client collects DHCPOFFER messages over a period of time, selects one DHCPOFFER message from the (possibly many) incoming DHCPOFFER messages (for example, the first DHCPOFFER message or the DHCPOFFER message from the previously used server) and extracts the server address from the 'server identifier' option in the DHCPOFFER message. The time over which the client collects messages and the mechanism used to select one DHCPOFFER are implementation dependent."

By placing a rogue DHCP server on the network, a network attacker can provide clients with addresses and other network information. Since DHCP responses typically include default gateway and DNS server information, the network attacker can supply his or her own system as the default gateway and DNS server resulting in a "man-in-the-middle" attack.

Network Attack Mitigation

The techniques that mitigate CAM table flooding also mitigate DHCP starvation by limiting the number of MAC addresses on a switch port. As implementation of RFC 3118, Authentication for DHCP Messages, increases, DHCP starvation attacks will become more difficult.

Additional features in the Catalyst family of switches, such as the DHCP snooping command, can be used to help guard against a DHCP starvation attack. DHCP snooping is a security feature that filters untrusted DHCP messages and builds and maintains a DHCP snooping binding table. The binding table contains information such as the MAC address, IP address, lease time, binding type, VLAN number and the interface information corresponding to the local untrusted interfaces of a switch. Untrusted messages are those received from outside the network or firewall and untrusted switch interfaces are ones that are configured to receive such messages from outside the network or firewall.

Command Samples to Mitigate DHCP Starvation Attacks Using DHCP Snooping

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan vlan_number [vlan_number]
Switch(config)# ip dhcp snooping information option
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)# ip dhcp snooping limit rate rate
```

Other Catalyst switch features such as IP Source Guard can provide additional defense against attacks such as DHCP starvation and IP spoofing. Like DHCP snooping, IP source guard is enabled on untrusted Layer 2 ports. All IP traffic is initially blocked *except* for DHCP packets captured by the DHCP snooping process. Once a client receives a valid IP address from the DHCP server a per-port and VLAN access control list (PACL) is applied to the port. This restricts the client IP traffic to those source IP addresses configured in the binding. Any other IP traffic with a source address other than the addresses in the binding will be filtered.

Command Samples to Mitigate DHCP Starvation Attacks Using DHCP Snooping and IP Source Guard

Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan *vlan_number [vlan_number]*
Switch(config-if)# no ip dhcp snooping trust
Switch(config-if)# ip verify source vlan dhcp-snooping port-security
Switch(config-if)# switchport port-security limit rate invalid-source-mac rate
Switch(config-if)# ip source binding *ip-address mac-address* vlan *vlan-id* interface *interface*

One method of preventing a rogue DHCP server from responding to DHCP Requests utilizes VACLs. While the use of VACLs does not entirely eliminate the possibility of a rogue DHCP server since IP spoofed DHCP messages are still possible but more difficult to successfully implement. The VACLs can be used to limit DHCP replies to legitimate DHCP servers and deny these same replies from all others. A more effective method of defending against rogue DHCP servers is the application of DHCP snooping. This provides an excellent defense against potential rogue DHCP servers by placing all ports on the switch into an "untrusted" state and blocking any DHCP replies that servers make. Such replies would be DHCP OFFERs, ACK's or NAC's.

Rogue DHCP Server Mitigation Using VACLs (Cisco Catalyst Operating System [Catalyst OS])

CatOS> (enable) set security acl ip ROGUE-DHCP permit udp host 10.16.17.225 any eq 68
CatOS> (enable) set security acl ip ROGUE-DHCP deny udp any any eq 68
CatOS> (enable) set security acl ip ROGUE-DHCP permit ip any any

Cisco Discovery Protocol

The Cisco Discovery Protocol runs at Layer 2 and allows Cisco devices to identify themselves to other Cisco devices. However, the information sent through Cisco Discovery Protocol is transmitted in cleartext and unauthenticated. Cisco Discovery Protocol is necessary for management applications and cannot be disabled without impairing some network-management applications. However, Cisco Discovery Protocol can be selectively disabled on interfaces where management is not being performed.

Network Attack Mitigation

Use Cisco Discovery Protocol only where appropriate.

Command Samples for Controlling Cisco Discovery Protocol

Global configuration:
IOS# no cdp run
Interface configuration menu:
IOS(config-if) no cdp enable

VLAN Trunking Protocol

The VLAN Trunking Protocol (VTP) is a Layer 2 messaging protocol that allows network administrators to centrally manage the addition, deletion, and renaming of VLANs. VTP is typically configured as a domain (also called a VLAN management domain) composed of one or more interconnected switches. The switches share the VTP-management

domain name. Changes to the VTP domain can be made either through the command-line interface (CLI) or through Simple Network Management Protocol (SNMP) and are propagated to member switches through VTP advertisements. If a switch receives a VTP advertisement over a trunk link and it is not configured to be a transparent switch, it inherits the VTP domain name and configuration-revision number.

VTP security is provided through a password that is entered into the VTP database on all of the switches. This shared password is used to authenticate VTP advertisements.

At the present time no vulnerabilities have been identified or published with regard to VTP. It is theoretically possible to forge VTP packets and inject them into a VLAN management domain if the network attacker can configure his or her connection as a trunk link. In this way a network attacker could add or remove VLANs from the VTP domain as well as create Spanning-Tree Protocol loops. While the level of difficulty of such an attack remains high, the possibility is not inconceivable. VTP remains a valued method to centrally manage VLANs throughout an enterprise. It is recommended that a VTP password be set throughout the VTP domain to prevent the possibility of forging VTP advertisements.

Network Attack Mitigation

Assign a VTP password in the VTP management domain.

Command Samples for Assigning a VTP Domain Password

Global Configuration (CatOS):

CatOS> (enable) **set vtp passwd** *passwd*

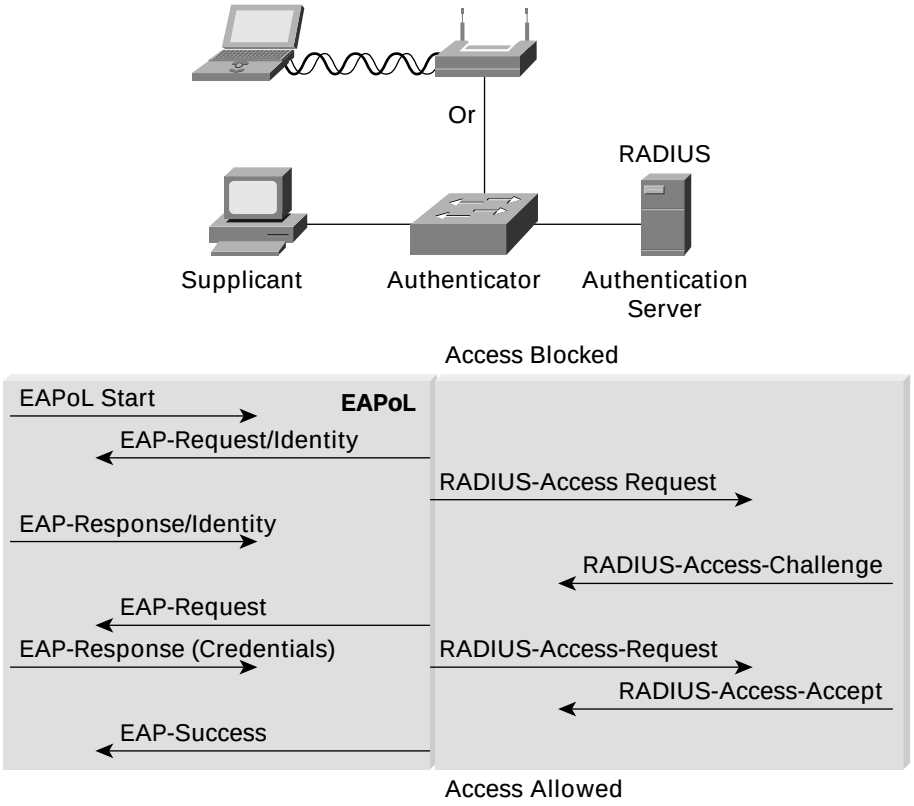
Global Configuration (IOS):

IOS# **vtp password** *passwd*

IEEE 802.1x

The IEEE 802.1x is a standard for passing the Extensible Authentication Protocol (EAP) framework over a wired or wireless network. Originally written to be used within the Point-to-Point Protocol (PPP) of dial-up and remote access networks, 802.1x allows for EAP to be used within the context of LANs. The IEEE 802.1x standard originally was written for use in wired networks but gained significant momentum when the vulnerabilities of WEP in the IEEE 802.11 standard were discovered and published. The basis of 802.1x is 802.1x works by requiring a supplicant (the client) to authenticate to an authentication server before access to the network is provided. The exchange of authentication information is facilitated by a device in-between the two, the authenticator. The 802.1x protocol is also known as “EAP encapsulation over LANs,” or EAPoL. Figure 9 below shows a typical authentication sequence between the supplicant and the authentication server.

Figure 9
EAPoL Authentication



The supplicant begins the exchange by sending an “EAPoL Start” message to the Authenticator who responds with an “EAP-Request/Identity” packet. The supplicant responds with an “EAP-Response/Identity” packet which it sends to the authenticator who then forwards it on to the authentication server. The authenticator (shown above as a RADIUS server) responds with an access challenge which it sends to the authenticator. The authenticator unpacks this challenge from the IP format and repackages it within the EAPoL framework and forwards it to the supplicant. EAP supports both client-only (EAP-MD5 and EAP-Cisco) as well as mutual authentication (EAP-TLS) of both the supplicant as well as the authentication server.

The supplicant responds to the challenge and passes the response to the authenticator who then forwards it to the authentication server. If the supplicant provides the proper credentials the authentication sends an “Access-Accept” message to the authenticator who then sends an “EAP-Success” message to the supplicant. Once this process has succeeded, network traffic can pass through the authenticator unimpeded. If the supplicant fails to successfully authenticate to the authentication server then the authenticator sends an “EAP-Failure” message to the supplicant and does not permit traffic to pass through to the network beyond.

In their published work *An Initial Security Analysis of the IEEE 802.1x Standard*, Arunesh Mishra and William Arbaugh of the University of Maryland’s Computer Science department detail two critical deficiencies in the 802.1x protocol which could be exploited by an attacker to gain access to a wireless network. One of the attacks is a Man-in-the-Middle (MITM) attack executed toward the end of the EAPoL authentication sequence. The attacker sends the supplicant an EAP-Success message that is forged so as to appear to come from the authenticator. The EAP-

Success message from the authenticator contains no integrity preserving information and causes both the authenticator and the supplicant state machines to transition to the *authenticated* state. This could theoretically allow the attacker to establish themselves in the network path between the supplicant and the authenticator.

The second vulnerability involves the capability of an attacker to hijack an existing session. After the supplicant has authenticated to the authentication server the authenticator and the supplicant state machines remain in an authenticated state. An attacker can send a *dissociate* management frame forged with the authenticator's MAC address to the supplicant. This causes the supplicant to dissociate from the wireless network but leaves the authenticator in an associated and open state. The attacker gains access to the network by forging their systems MAC address with the address of the system that was dissociated. The authenticator state machine is still in an authenticated and associated state.

The Protected EAP (PEAP) authentication protocol was developed to address these and other concerns about 802.1x, in particular its use in wireless network. PEAP's basic protocol structure is in two parts:

- The establishment of a TLS session between the supplicant and the PEAP authentication server and,
- The EAP exchange over the TLS session to authenticate the supplicant using a defined EAP authentication protocol

To date, no known vulnerabilities exist in PEAP.

Network Attack Mitigation

Deploy 802.1x on access switches and wireless access points to ensure that all access to the network infrastructure requires authentication. Consider deploying PEAP for use with wireless LANs.

Command Samples for Enabling 802.1x (Cisco IOS Software)

```
Router(config)# aaa new-model
Router(config)# aaa authentication dot1x default group radius
Router(config)# dot1x system-auth-control
Router(config)# interface fastethernet 0/1
Router(config-if)# dot1x port-control auto
Router(config-if)# ^Z
Router# show dot1x all
```

Layer 2 Best Practices Scenarios

Much of the information covered in this document is applicable to many situations. The following cases are meant to highlight implementation of some of the Layer 2 mitigation techniques in specific situations. The various cases considered depend on three factors:

- The number of security zones in the network design
- The number of user groups in the network design
- The number of switch devices in the design

These scenarios can be broken down into eight total cases:

Case #	Security Zones	Number of User Groups	Number of Switch Devices
1	Single	Single	Single
2	Single	Single	Multiple
3	Single	Multiple	Single
4	Single	Multiple	Multiple
5	Multiple	Single	Single
6	Multiple	Single	Multiple
7	Multiple	Multiple	Single
8	Multiple	Multiple	Multiple

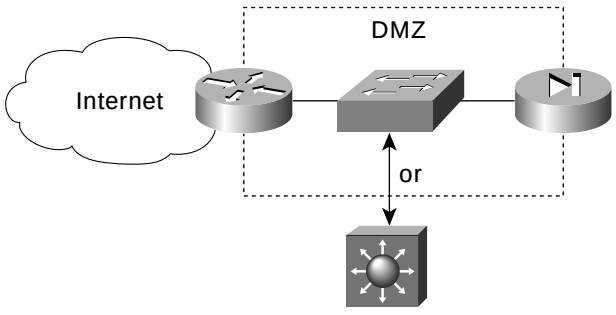
The above table can be read as follows: case #1 involves a network design where there is a single security zone of trust, used by a single user group, and only includes one physical switch. Case #8 involves a network design where there are multiple security zones of trust with multiple user groups and multiple physical switches in the design. An example of case #1 could be a small business network using a broadband connection behind a DSL router/firewall. An example of case #8 could be a large application service provider data center. The above cases are discussed in further detail below.

Case #1: Single Security Zone, One User Group, One Physical Switch

Description:

This design provides for a single physical switch existing within a zone of trust. Only one user group's traffic traverses the switch. An example of such a design would be a switch within a network DMZ created between an edge router and a corporate firewall as shown in Figure 10 below. In this design all systems within the security zone are on the same VLAN.

Figure 10
Single Security Zone, One User Group, One Switch Design



Vulnerabilities:

This designs primary Layer 2 vulnerabilities include the following:

1. MAC spoofing
2. CAM Table Overflow

Mitigation:

Use the mitigation techniques described in the "CAM Table Overflow" and "MAC Spoofing" sections to secure the Layer 2 environment in this design. Port security may well be administratively appropriate in this case because of the limited size of the design. The Layer 2 switches are a part of the security perimeter between the zones of trust and should be managed as securely as possible including the use of SSH for command line management, SNMPv3 for remote management, configuration audits and regular penetration testing of each VLAN using tools capable of exploiting Layer 2 vulnerabilities such as Dsniff. An equally effective and less administratively burdensome approach would be to use dynamic port security through the application of DHCP snooping and Dynamic ARP Inspection as discussed earlier.

Command Samples to Mitigate MAC Spoofing (Cisco Catalyst Operating System [Catalyst OS])

CatOS> set port security *mod_num/port_num* **enable** *[mac_addr]*
CatOS> set port security *mod_num/port_num mac_addr*
CatOS> set port security *mod_num/port_num* **violation** {shutdown | restrict}
CatOS> show port *[mod_num[/port_num]*

Command Samples to Mitigate MAC Spoofing (Cisco IOS Software)

IOS(config-if)# port security max-mac-count {1-132}
IOS(config-if)# port security action {shutdownltrap}
IOS(config-if)# arp timeout *seconds*

Configuring DHCP Snooping (Cisco IOS Software)

switch(config)# ip dhcp snooping
switch(config)# ip dhcp snooping vlan *vlan_id [,vlan_id]*
switch(config-if)# ip dhcp snooping trust
Switch(config-if)# ip dhcp snooping limit rate *rate*

Configuring Dynamic ARP Inspection with DHCP Snooping (Cisco IOS Software)

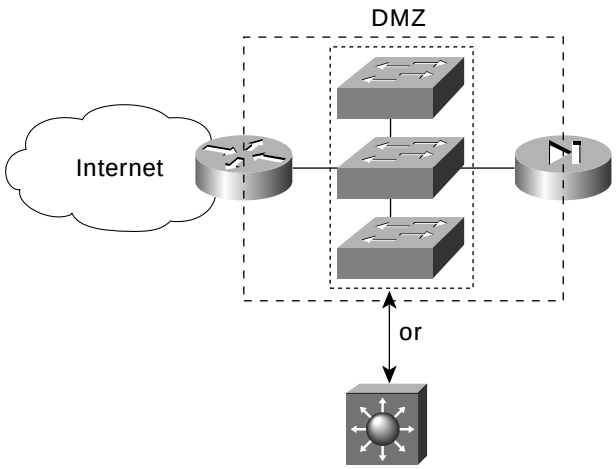
Switch(config)# ip arp inspection vlan *vlan_id[,vlan_id]*
Switch(config)# ip arp inspection validate src-mac dst-mac ip
Switch(config-if)# ip arp inspection trust

Case #2: Single Security Zone, One User Group, Multiple Physical Switches

Description:

This design provides for multiple physical switches existing within a single zone of trust. Only one user group's traffic traverses the switch and can be represented by a very large DMZ as shown in Figure 11 below or a DMZ with multiple VLANs all existing within a single security zone of trust. Additionally, this could also be represented as a Layer 3 switch within the DMZ to provide inter-VLAN routing.

Figure 11
Single Security Zone, One User Group, Multiple Physical Switches



Vulnerabilities:

This designs primary Layer 2 vulnerabilities include the following:

1. MAC spoofing
2. CAM Table Overflow
3. VLAN Hopping
4. Spanning Tree Attacks (for multiple switches)

In addition to the above vulnerabilities this scenario may also be vulnerable to a private VLAN proxy attack as described above in the section titled "Private VLAN Attacks".

Mitigation:

If the security zone is small enough use port security to help mitigate the CAM table overflow vulnerability as well as the MAC spoofing vulnerability. BPDU guard and root guard can be used to mitigate attacks against the Spanning Tree Protocol (STP).

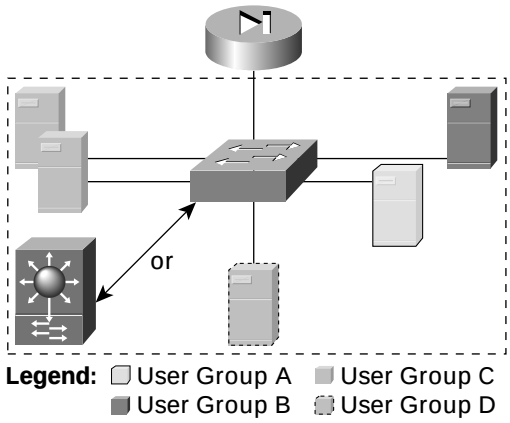
The Layer 2 switches are a part of the security perimeter between zones of trust and should be managed as securely as possible including the use of SSH for command line management, SNMPv3 for remote management, configuration audits and regular penetration testing of each VLAN using tools capable of exploiting Layer 2 vulnerabilities such as Dsniff.

Case #3: Single Security Zone, Multiple User Groups, Single Physical Switch

Description:

In this design VLANs are used to logically separate the traffic of multiple user groups within a single physical network. A typical example of such a design would be an application service provider's data center or different departments within a single corporate enterprise who require data segregation. This case is depicted in Figure 12.

Figure 12
Single Security Zone, Multiple User Groups, Single Physical Switch



Vulnerabilities:

This designs primary layer 2 vulnerabilities include the following:

1. MAC spoofing
2. CAM Table Overflow
3. VLAN Hopping

In addition to the above vulnerabilities this scenario may also be vulnerable to a private VLAN proxy attack as described above in the section titled "Private VLAN Attacks".

Mitigation:

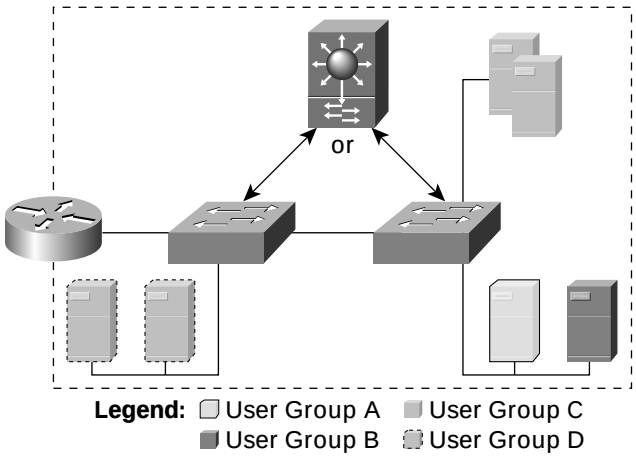
If the security zone is small enough use port security to help mitigate the CAM table overflow vulnerability as well as the MAC spoofing vulnerability. Additionally, mitigation of VLAN hopping can be accomplished by following the VLAN best practices outlined within this paper. As with the previous cases, the switches must be managed as securely as possible and tested on a regular basis.

Case #4: Single Security Zone, Multiple User Groups, Multiple Physical Switches

Description:

This scenario represents a slightly more complex case than case #3 above. This design, shown in Figure 13 below, represents one where high-availability is a factor as well as the need to trunk information between the switch devices. In addition the direction of travel for the network traffic as determined through the Spanning Tree Protocol (STP) requires additional considerations when determining some of the more specific mitigation techniques. VLANs are used to provide traffic segmentation between the various user groups.

Figure 13
Single Security Zone, Multiple User Groups, Multiple Physical Switches



Vulnerabilities:

This designs primary Layer 2 vulnerabilities include the following:

1. MAC spoofing
2. CAM Table Overflow
3. VLAN Hopping
4. Spanning Tree Protocol Attacks

In addition to the above vulnerabilities this scenario may also be vulnerable to a private VLAN proxy attack as described above in the section titled “Private VLAN Attacks”.

Mitigation:

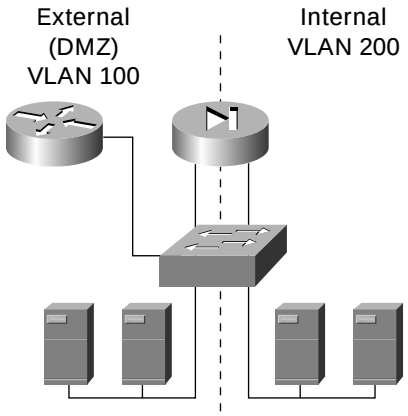
If the security zone is small enough use port security to help mitigate the CAM table overflow vulnerability as well as the MAC spoofing vulnerability. Additionally, mitigation of VLAN hopping can be accomplished by following the VLAN best practices outlined within this paper. If necessary deploy 802.1x authentication to prevent unauthorized access to the security zone from an attacker who may physically connect to a switch in the design. As with the previous cases, the switches must be managed as securely as possible and tested on a regular basis.

Case #5: Multiple Security Zone, One User Group, Single Physical Switch

Description:

This design provides for a single physical switch existing two security zones of trust. Only one user group’s traffic traverses the switch. An example of such a design would be a switch which is configured for “double-duty” on a firewall’s DMZ or internal interfaces. VLANs separate traffic on a single physical LAN into multiple logical LANs through the use of VLAN tags. The use of VLANs can be considered as a possible way of segmenting multiple interfaces of a firewall on a single switch as shown in Figure 14 below. In this example both the external network, the DMZ, and the internal network utilize the same switch for Layer 2 connectivity. The external network traffic is tagged as VLAN ID 100 while the internal network traffic is tagged with VLAN ID 200. While it is technically feasible to make this design secure there are significant ramifications should the switch be compromised.

Figure 14
Single Switch Network



Vulnerabilities:

This designs primary Layer 2 vulnerabilities include the following:

1. MAC spoofing (within VLANs)
2. CAM Table Overflow (per VLAN traffic flooding)
3. VLAN Hopping

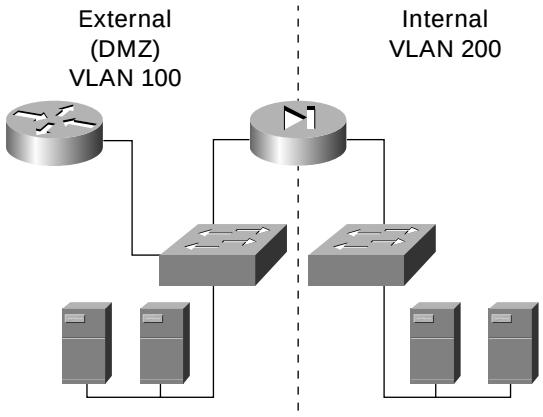
If private VLANs are implemented within each VLAN this design may also be vulnerable to a private VLAN proxy attack described earlier. Additionally, if one of the VLANs is large and DHCP is used for address management then this design may be vulnerable to the DHCP starvation attacks described above.

Mitigation:

If the security zones are small enough use port security to help mitigate the CAM table overflow vulnerability as well as the MAC spoofing vulnerability. Additionally, mitigation of VLAN hopping can be accomplished by following the VLAN best practices outlined within this paper. As with the previous cases, the switches must be managed as securely as possible and tested on a regular basis.

In this design another mitigation approach would be to split the Layer 2 functionality of the switch to two separate physical switches. This design, shown in Figure 15 below, would then simply as a case #1 scenario (Single Security Zone, Single user group, Single Switch) as described above. If this is done then the mitigation techniques described in case #1 would apply to both distinct security zones.

Figure 15
Multiple Switch Network Separation



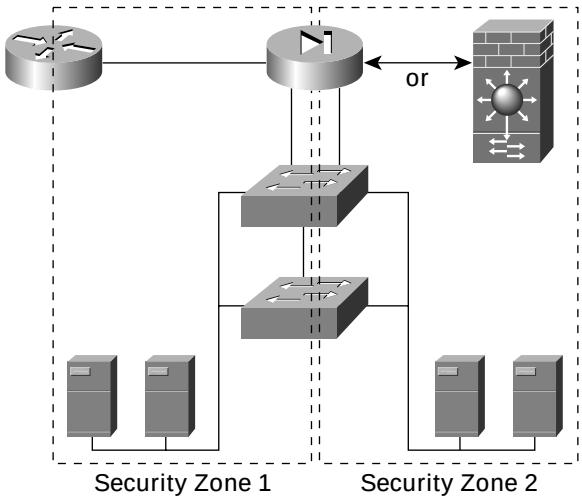
If private VLANs (PVLANs) are employed in any of the VLANs, consideration must be given to the possibility of private VLAN attacks described earlier. If the VLANs utilize DHCP for address assignment then DHCP starvation by an attacker and needs to be considered.

Case #6: Multiple Security Zones, One User Group, Multiple Physical Switches

Description:

This design represents a large data center within a single enterprise. However, the need to segregate traffic as well as data for various groups or departments within the enterprise is reflected by the separation of the data center into security zones. This can be accomplished securely through the use of VLANs within the data center, however, there are considerations which must be evaluated regarding some of the potential vulnerabilities. The two switches have a trunk between them represented by the solid green line carrying all of the VLAN traffic between the switches.

Figure 16
Multiple Security Zones, One User Group, Multiple Physical Switches



Vulnerabilities:

This designs primary Layer 2 vulnerabilities include the following:

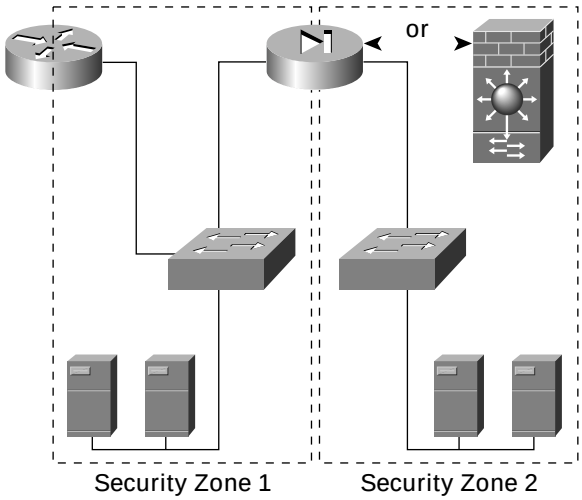
1. MAC spoofing (within VLANs)
2. CAM Table Overflow (per VLAN traffic flooding)
3. VLAN Hopping
4. Spanning Tree Protocol attacks

If private VLANs are implemented within each VLAN this design may also be vulnerable to a private VLAN proxy attack described earlier. Additionally, if one of the VLANs is large and DHCP is used for address management then this design may be vulnerable to the DHCP starvation attacks described above. Because the design utilizes VTP to carry VLAN management information between the switches, an attacker may also be able to craft spoofed VTP packets and delete VLAN information from the various switch databases.

Mitigation:

If the security zones are small enough use port security to help mitigate CAM table overflow vulnerabilities as well as the MAC spoofing vulnerability. Additionally, mitigation of VLAN hopping can be accomplished by following the VLAN best practices outlined within this paper. If necessary deploy 802.1x authentication to prevent unauthorized access to each of the security zones from an attacker who may physically connect to a switch in the design. Another possible mitigation method would be to add a firewall within the design or add a Layer 3 switch with an integrated firewall as shown in Figure 17 below. The firewall enforces additional Layer 3 traffic segregation. This solution essentially becomes the same design as the mitigation design for case #5 above. As with the previous cases, the switches must be managed as securely as possible and tested on a regular basis.

Figure 17
Alternative Design for Multiple Security Zones, One User Group, Multiple Switches

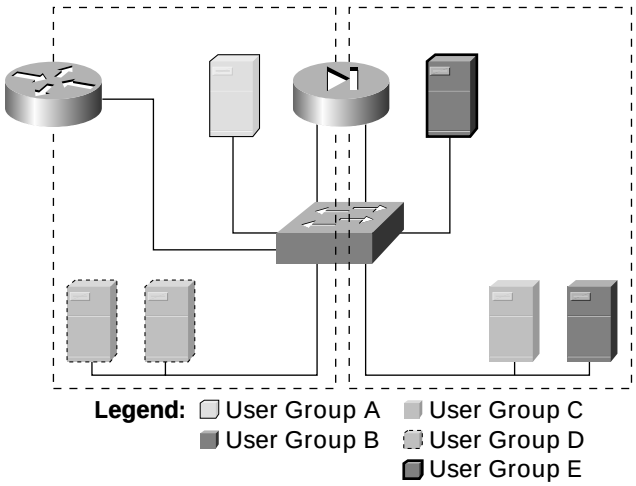


Case #7: Multiple Security Zones, Multiple User Groups, Single Physical Switch

Description:

This design is very similar to the previous scenario by having multiple user groups within the data center each requiring their own level of security for their systems. However in this case, all of the user groups connect to a single central switch. VLANs can be used to provide traffic segregation between the security zones.

Figure 18
Multiple Security Zones, Multiple User Groups, One Physical Switch



Vulnerabilities:

This designs primary Layer 2 vulnerabilities include the following:

1. MAC spoofing (within VLANs)
2. CAM Table Overflow (per VLAN traffic flooding)
3. VLAN Hopping
4. Private VLAN Attacks (on a per VLAN basis)

Mitigation:

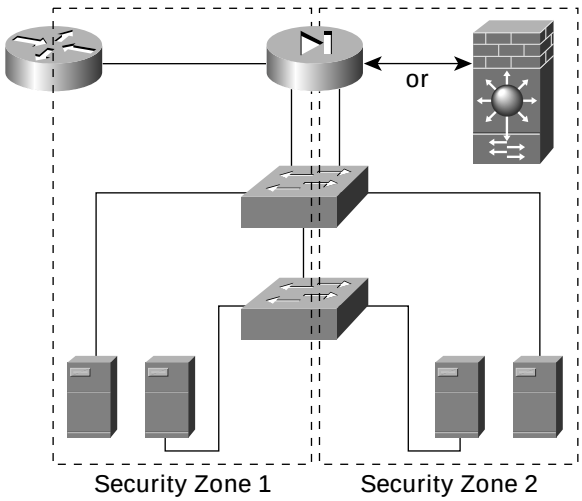
If the security zones are small enough use port security to help mitigate CAM table overflow vulnerabilities as well as the MAC spoofing vulnerability. Additionally, mitigation of VLAN hopping can be accomplished by following the VLAN best practices outlined within this paper. If necessary deploy 802.1x authentication to prevent unauthorized access to each of the security zones from an attacker who may physically connect to a switch in the design. Another possible mitigation method would be to add a firewall within the data center design and integrate it into the central switch similar to that employed in the previous design. The firewall enforces additional Layer 3 traffic segregation between the various user groups. As with the previous cases, the switches must be managed as securely as possible and tested on a regular basis.

Case #8: Multiple Security Zones, Multiple User Groups, Multiple Physical Switches

Description:

This design represents the most complex of the series. It is very similar to the previous scenario by having multiple user groups within the data center each requiring their own level of security for their systems. Instead of all the user groups connecting to a single central switch there are multiple switches (both Layer 2 and Layer 3) throughout the design. VLANs can be used to provide traffic segregation between the security zones; however, the need to provide high security in some of the zones may require additional measures.

Figure 19
Multiple Security Zones, Multiple User Groups, Multiple Physical Switches



Vulnerabilities:

This designs primary Layer 2 vulnerabilities include the following:

1. MAC spoofing (within VLANs)
2. CAM Table Overflow (per VLAN traffic flooding)
3. VLAN Hopping
4. Spanning Tree Protocol Attacks
5. VTP Attacks

If private VLANs are implemented within each VLAN this design may also be vulnerable to a private VLAN proxy attack described earlier. Additionally, if one of the VLANs is large and DHCP is used for address management then this design may be vulnerable to the DHCP starvation attacks described above.

Mitigation:

If the security zones are small enough use port security to help mitigate CAM table overflow vulnerabilities as well as the MAC spoofing vulnerability. Additionally, mitigation of VLAN hopping can be accomplished by following the VLAN best practices outlined within this paper. If necessary deploy 802.1x authentication to prevent unauthorized access to each of the security zones from an attacker who may physically connect to a switch in the design. Another

possible mitigation method would be to add a firewall within the data center design and integrate it into the one or more of the switches similar to that employed in the case 6 design. The firewall enforces additional Layer 3 traffic segregation between the various user groups. As with the previous cases, the switches must be managed as securely as possible and tested on a regular basis.

SUMMARY

Although security attacks on networks aren't new events, attacks that use Layer 2 to bypass VLAN restrictions are quickly gaining sophistication and popularity. To mitigate the effects of these attacks as much as possible, the following precautions are recommended:

- Manage switches as securely as possible. Use Secure Shell (SSH) Protocol if possible, or an out-of-band management system. Avoid the use of cleartext management protocols such as Telnet or SNMP Version 1.
- Use IP-permit lists to restrict access to management ports.
- Selectively use SNMPv3 and treat community strings like root passwords.
- When SNMPv3 is used as a management protocol, restrict management access to the VLAN so that entities on untrusted networks cannot access management interfaces or protocols. Consider using DHCP snooping and IP source guard to mitigate DHCP starvation attacks.
- Always use a dedicated VLAN ID for all trunk ports.
- Avoid using VLAN 1.
- Set all user ports to non-trunking mode.
- Deploy port security where possible for user ports. When feasible, configure each port to associate a limited number of MAC addresses (approximately two to three). This will mitigate MAC flooding and other network attacks. Alternatively, deploy dynamic port security using DHCP snooping along with Dynamic ARP Inspection (DAI).
- Have a plan for the ARP security issues in your network. Consider using DHCP Snooping along with Dynamic ARP Inspection and IP source guard to protect against MAC spoofing and IP spoofing on the network.
- Use VACLs to prevent rogue DHCP servers by limiting replies to DHCP clients to valid DHCP servers on the network. A more flexible approach would be to use DHCP snooping to block unauthorized DHCP servers from responding to DHCP Request packets.
- Enable Spanning-Tree Protocol attack mitigation (BPDU Guard, Root Guard).
- Use private VLANs where appropriate to further divide Layer 2 networks.
- Use Cisco Discovery Protocol only where appropriate.
- Disable all unused ports and put them in an unused VLAN. This setup prevents network intruders from plugging into unused ports and communicating with the rest of the network.
- Use Cisco IOS Software ACLs on IP-forwarding devices to protect Layer 2 proxy on private VLANs.
- Eliminate native VLANs from 802.1q trunks.
- Use VTP passwords to authenticate VTP advertisements.
- Consider using Layer 2 port authentication such as 802.1X to authenticate clients attempting connectivity to a network.

- Procedures for change control and configuration analysis must be in place to ensure that changes result in a secure configuration. This is especially valuable in cases where several organizational groups may control the same switch, and even more valuable in network security deployments where even greater care must be taken.

Many of the above features are available in the Cisco's Catalyst switches. Table 1 below details the availability of a feature discussed in this document in the Catalyst family of switches.

	Cat 2900 XL	Cat 3500 XL	Cat 2950	Cat 3550	Cat 4000 CatOS	Cat 5000 CatOS	Cat 6000 CatOS	Cat 4000 IOS	Cat 6000 IOS
Port Security	X	X	X	X	X	X	X	X	X
Private VLANs	X	X	X	X	X		X	X	X
STP BPDU Guard			X	X	X	X	X	X	X
STP Root Guard	X	X	X	X	X		X	X	X
SSH Support			X	X	X		X	X	X
VMPS Client	X	X	X	X	X	X	X	X	
VMPS Server					X	X	X		
802.1x Authentication			X	X	X		X	X	X
Wire Rate ACLs			X	X	X		X	X	X
DHCP Snooping								X	
ARP Inspection							X		
Dynamic ARP Inspection					X[1]		X	X[2]	X[2]

1. Available Q4 2003
2. Available Q1 2004

By employing the additional precautions discussed above in the existing network configurations, the effects of Layer 2-based attacks can be significantly mitigated. Although not all of these precautions are necessary, depending on the network configuration, they do represent a single set of recommendations that can be used in addition to current network security guidelines.

ACKNOWLEDGMENTS

The author wishes to publicly thank all the individuals who contributed to the SAFE architecture as well as the writing of this white paper. The successful completion of this project would not have been possible without the valuable input and review feedback from all of the Cisco employees both in the corporate headquarters as well as in the field. In addition, many individuals contributed additional assistance during the validation and review phases of this project. This group includes Jason Halpern, Troy Sherman, Daniel Tulledge, Sean Convery, Greg Abelar, and John Stuppi. Thank you all for your effort.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

DB/KC/LW5634 3/04