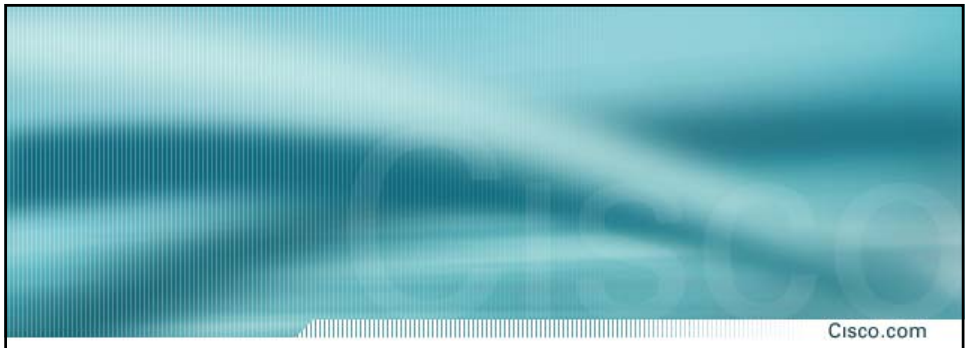


Multilayer Switching (CCNP3 v 5)

Halmstad University

© 2003, Cisco Systems, Inc. All rights reserved.

Module 8: Minimizing service loss and data theft in a campus network

Cisco.com

- Port security
- PVLANs and VACLs
- VLAN hopping
- DHCP spoofing
- ARP spoofing
- STP attacks
- Vty ACLs
- SSH

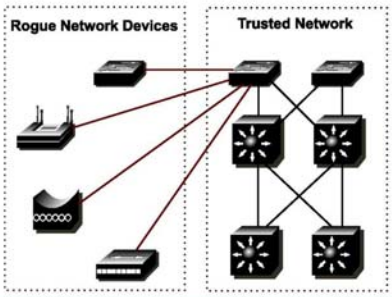
© 2003, Cisco Systems, Inc. All rights reserved.

Unauthorized Access by Rogue Devices

Cisco.com

Rogue Access Points

FIGURE 1



- Rogue network devices can be:
  - Wireless hubs
  - Wireless routers
  - Access switches
  - Hubs
- These devices are typically connected at access level switches.

All contents copyright © 2006 Cisco Systems, Inc. All rights reserved.
© 2003, Cisco Systems, Inc. All rights reserved.

Switch Attack Categories

Cisco.com

- **MAC layer attacks**
- **VLAN attacks**
- **Spoof attacks**
- **Switch device attacks**

© 2003, Cisco Systems, Inc. All rights reserved.

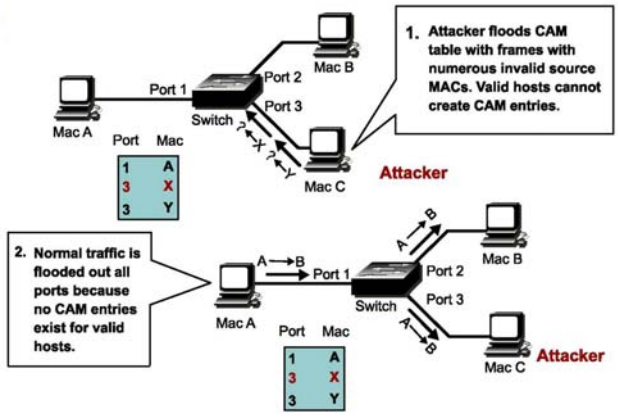
MAC Flooding Attack

Cisco.com

MAC Flood Attack

FIGURES

1
2



All contents copyright © 2006 Cisco Systems, Inc. All rights reserved.

© 2003, Cisco Systems, Inc. All rights reserved.

MAC Flood Attack Progression

FIGURES

1
2

Step	Description
1	Switch forwards traffic based on valid CAM table entries.
2	Attacker (MAC address C) sends out multiple packets with various source MAC addresses.
3	Over a short period of time, the CAM table in the switch fills up until it cannot accept new entries. As long as the attack is running, the CAM table on the switch will remain full.
4	Switch begins to flood all packets that it receives out of every port so that frames sent from host A to host B are also flooded out of port 3 on the switch.

All contents copyright © 2006 Cisco Systems, Inc. All rights reserved.

To mitigate against MAC flooding, port security is configured to define the number of MAC addresses that are allowed on a given port.

© 2003, Cisco Systems, Inc. All rights reserved.

Port Security

Cisco.com

Port Security

FIGURES

1

2

Port security restricts port access by MAC address.

All contents copyright © 2006 Cisco Systems, Inc. All rights reserved.

© 2003, Cisco Systems, Inc. All rights reserved.

7

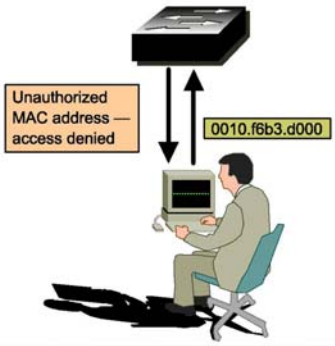
Port Security with Sticky MAC Addresses

Cisco.com

Port Security with Sticky MAC Addresses

FIGURE

1



Sticky MAC stores dynamically learned MAC addresses.

All contents copyright © 2006 Cisco Systems, Inc. All rights reserved.

© 2003, Cisco Systems, Inc. All rights reserved.

8

VLAN Hopping

Cisco.com

Explaining VLAN Hopping

FIGURES

1
2
3
4

- Attacking system spoofs itself as a legitimate trunk negotiating device.
- Trunk link is negotiated dynamically.
- Attacking device gains access to data on all VLANs carried by the negotiated trunk.

All contents copyright © 2006 Cisco Systems, Inc. All rights reserved.

© 2003, Cisco Systems, Inc. All rights reserved.

VLAN Hopping

Cisco.com

Switch Spoofing Sequence of Events

FIGURES

1
2
3
4

Step	Description
1.	Attacker gains access to a switch port and sends DTP negotiation frames toward a switch with DTP running and auto negotiation turned on (often, the default settings).
2.	Attacker and switch negotiate trunking over the port.
3.	Switch allows all VLANs (default) to traverse the trunk link.
4.	Attacker sends data to, or collects it from, all VLANs carried on that trunk.

All contents copyright © 2006 Cisco Systems, Inc. All rights reserved.

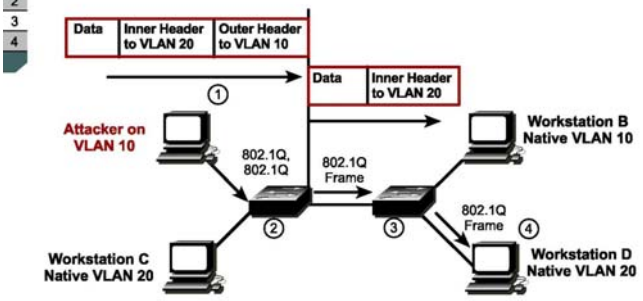
© 2003, Cisco Systems, Inc. All rights reserved.

VLAN Hopping

Cisco.com

VLAN Hopping with Double Tagging

FIGURES 1 2 3 4



Double tagging allows a frame to be forwarded to a destination VLAN other than the source's VLAN.

All contents copyright © 2006 Cisco Systems, Inc. All rights reserved.

© 2003, Cisco Systems, Inc. All rights reserved.

VLAN Hopping

Cisco.com

Double Tagging Method of VLAN Hopping

FIGURES 1 2 3 4

Step	Description
1.	Workstation A (native VLAN 10) sends a frame with two 802.1Q headers to switch 1.
2.	Switch 1 strips the outer tag and forwards the frame to all ports within the same native VLAN.
3.	Switch 2 interprets the frame according to information in the inner tag marked with VLAN ID 20.
4.	Switch 2 forwards the frame out all ports associated with VLAN 20, including trunk ports.

All contents copyright © 2006 Cisco Systems, Inc. All rights reserved.

© 2003, Cisco Systems, Inc. All rights reserved.

Mitigating VLAN Hopping

Cisco.com

- **Configure all unused ports as access ports so that trunking cannot be negotiated across those links.**
- **Place all unused ports in the shutdown state and associate with a VLAN designated only for unused ports, carrying no user data traffic.**
- **When establishing a trunk link, configure the following:**
  - **Make the native VLAN different from any data VLANs**
  - **Set trunking as "on," rather than negotiated**
  - **Specify the VLAN range to be carried on the trunk**

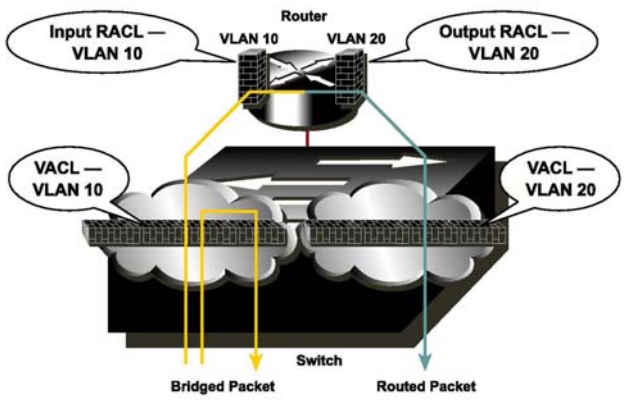
© 2003, Cisco Systems, Inc. All rights reserved.

ACL

Cisco.com

Types of ACLs

FIGURE 1

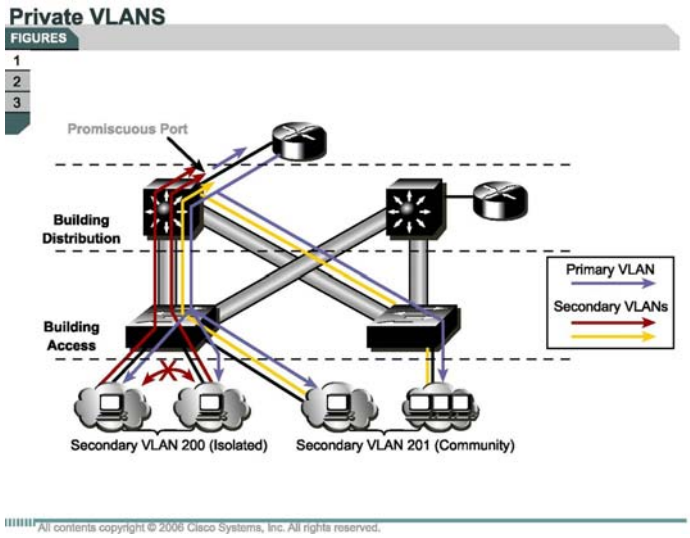


All contents copyright © 2006 Cisco Systems, Inc. All rights reserved.

© 2003, Cisco Systems, Inc. All rights reserved.

Private VLANs and Protected Ports

Cisco.com



All contents copyright © 2006 Cisco Systems, Inc. All rights reserved.

© 2003, Cisco Systems, Inc. All rights reserved.

15

Private VLANs

Cisco.com

- **Isolated: Has complete Layer 2 separation from other ports within the same PVLAN, except for the promiscuous port. PVLANs block all traffic to isolated ports, except the traffic from promiscuous ports. Traffic received from an isolated port is forwarded only to promiscuous ports.**
- **Promiscuous: Communicates with all ports within the PVLAN, including the community and isolated ports. The default gateway for the segment would likely be hosted on a promiscuous port, given that all devices in the PVLAN need to communicate with that port.**
- **Community: Communicate among themselves and with their promiscuous ports. These interfaces are isolated at Layer 2 from all other interfaces in other communities, or in isolated ports within their PVLAN.**

© 2003, Cisco Systems, Inc. All rights reserved.

16

DHCP Spoof Attack

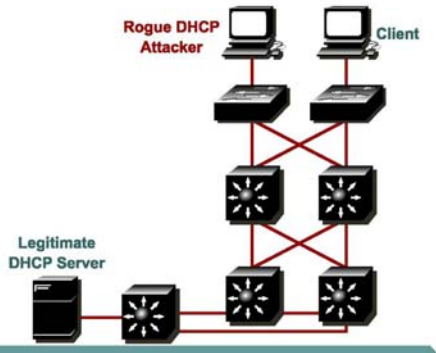
Cisco.com

DHCP Spoof Attacks

FIGURES

1

2



- Attacker activates DHCP server on VLAN.
- Attacker replies to valid client DHCP requests.
- Attacker assigns IP configuration information that establishes rogue device as client default gateway.
- Attacker establishes "man-in-the-middle" attack.

All contents copyright © 2006 Cisco Systems, Inc. All rights reserved.

© 2003, Cisco Systems, Inc. All rights reserved.

17

DHCP Snooping

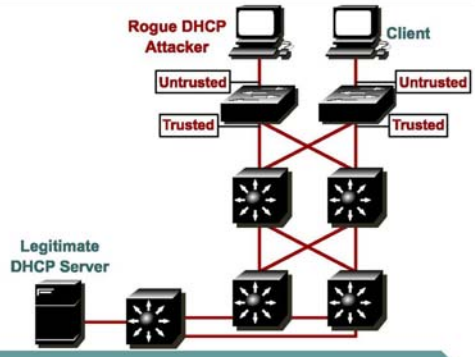
Cisco.com

Securing against DHCP Spoofing Attacks

FIGURES

1

2



- DHCP snooping allows the configuration of ports as trusted or untrusted.
- Untrusted ports cannot process DHCP replies.
- Configure DHCP snooping on uplinks to a DHCP server.
- Do not configure DHCP snooping on client ports.

All contents copyright © 2006 Cisco Systems, Inc. All rights reserved.

© 2003, Cisco Systems, Inc. All rights reserved.

18

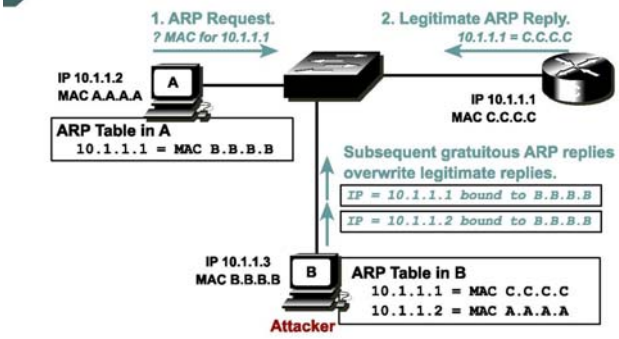
ARP Spoofing

Cisco.com

ARP Spoofing

FIGURES

1
2



All contents copyright © 2006 Cisco Systems, Inc. All rights reserved.

© 2003, Cisco Systems, Inc. All rights reserved.

19

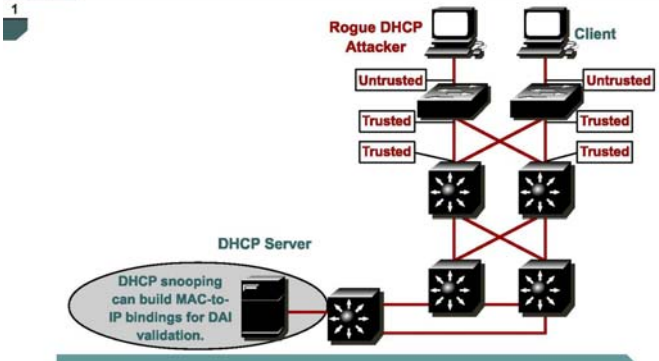
Dynamic ARP Inspection

Cisco.com

Dynamic ARP Inspection

FIGURE

1



- DAI associates each interface with a trusted state or an untrusted state.
- Trusted interfaces bypass all dynamic ARP inspection.
- Untrusted interfaces undergo DAI validation.

All contents copyright © 2006 Cisco Systems, Inc. All rights reserved.

© 2003, Cisco Systems, Inc. All rights reserved.

20

Protecting Against ARP Spoofing Attacks

Cisco.com

To mitigate the chances of ARP spoofing:

- **Step 1**

Implement protection against DHCP spoofing.

- **Step 2**

Enable dynamic ARP inspection.

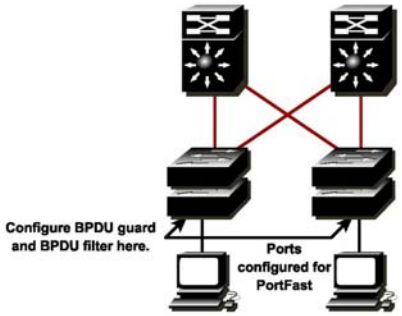
© 2003, Cisco Systems, Inc. All rights reserved.

Protecting the Operation of STP

Cisco.com

Protecting the Operation of STP

FIGURE 1



Protection against switches being added on PortFast ports.
- BPDU guard shuts ports down.
- BPDU filter specifies action to be taken when BPDUs are received.

All contents copyright © 2006 Cisco Systems, Inc. All rights reserved.

© 2003, Cisco Systems, Inc. All rights reserved.

Protecting the Operation of STP

Cisco.com

- BPDU Guard
- BPDU Filtering
- Root Guard
- Unidirectional Link Detection

© 2003, Cisco Systems, Inc. All rights reserved.

Vulnerabilities in CDP

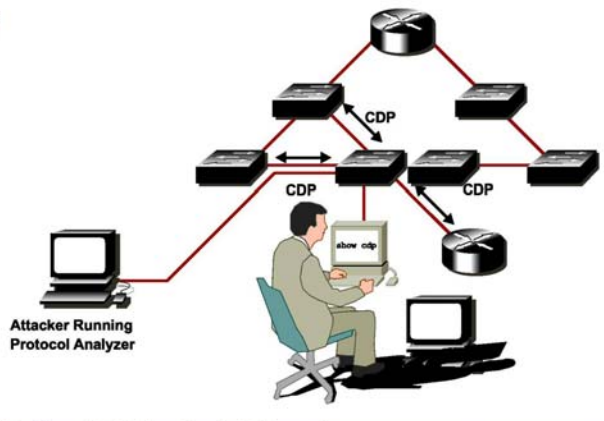
Cisco.com

Describing Vulnerabilities in CDP

FIGURES

1

2



All contents copyright © 2006 Cisco Systems, Inc. All rights reserved.

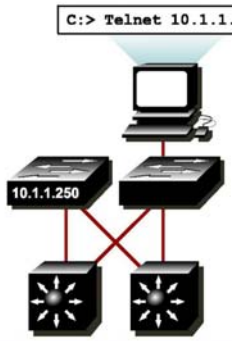
© 2003, Cisco Systems, Inc. All rights reserved.

vty ACLs

Cisco.com

Describing vty ACLs

FIGURE 1



- Set up standard IP ACL.
- Use line configuration mode to filter access with the `access-class` command.
- Set identical restrictions on every vty line.

All contents copyright © 2006 Cisco Systems, Inc. All rights reserved.

© 2003, Cisco Systems, Inc. All rights reserved.

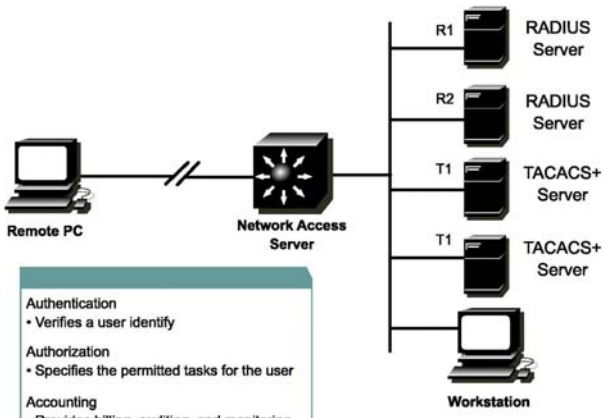
25

AAA

Cisco.com

AAA Network Configuration

FIGURE 1



Authentication
- Verifies a user identify

Authorization
- Specifies the permitted tasks for the user

Accounting
- Provides billing, auditing, and monitoring

All contents copyright © 2006 Cisco Systems, Inc. All rights reserved.

© 2003, Cisco Systems, Inc. All rights reserved.

26

Best Practices for Switch Security

Cisco.com

The following steps are required whenever placing new equipment in service:

- **Step 1 Consider or establish organizational security policies.**
- **Step 2 Secure switch devices.**
- **Step 3 Secure switch protocols.**
- **Step 4 Mitigate compromises launched through a switch.**

© 2003, Cisco Systems, Inc. All rights reserved.

Best practices for secure switch access

Cisco.com

- **Set system passwords**
- **Secure access to the console**
- **Secure access to vty lines**
- **Use SSH**
- **Configure system-warning banners**
- **Disable unneeded services**
- **Disable the integrated HTTP daemon if not in use**
- **Configure basic logging**

© 2003, Cisco Systems, Inc. All rights reserved.

Best practices to mitigate compromises through a switch

Cisco.com

- Use CDP only as needed
- Secure the spanning tree topology
- Proactively configure unused router and switch ports
- Disable automatic trunk negotiation
- Monitor physical device access
- Establish port-based security

© 2003, Cisco Systems, Inc. All rights reserved.