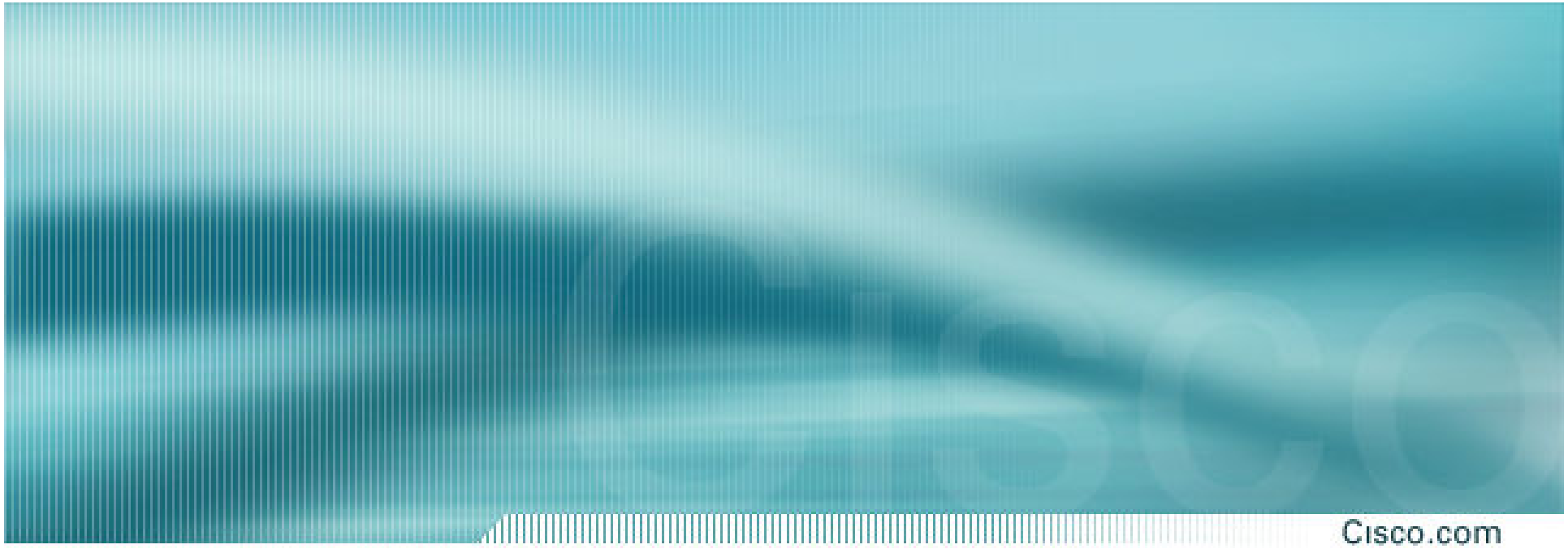


Ethernet: Layer 2 Security

Eric Vyncke

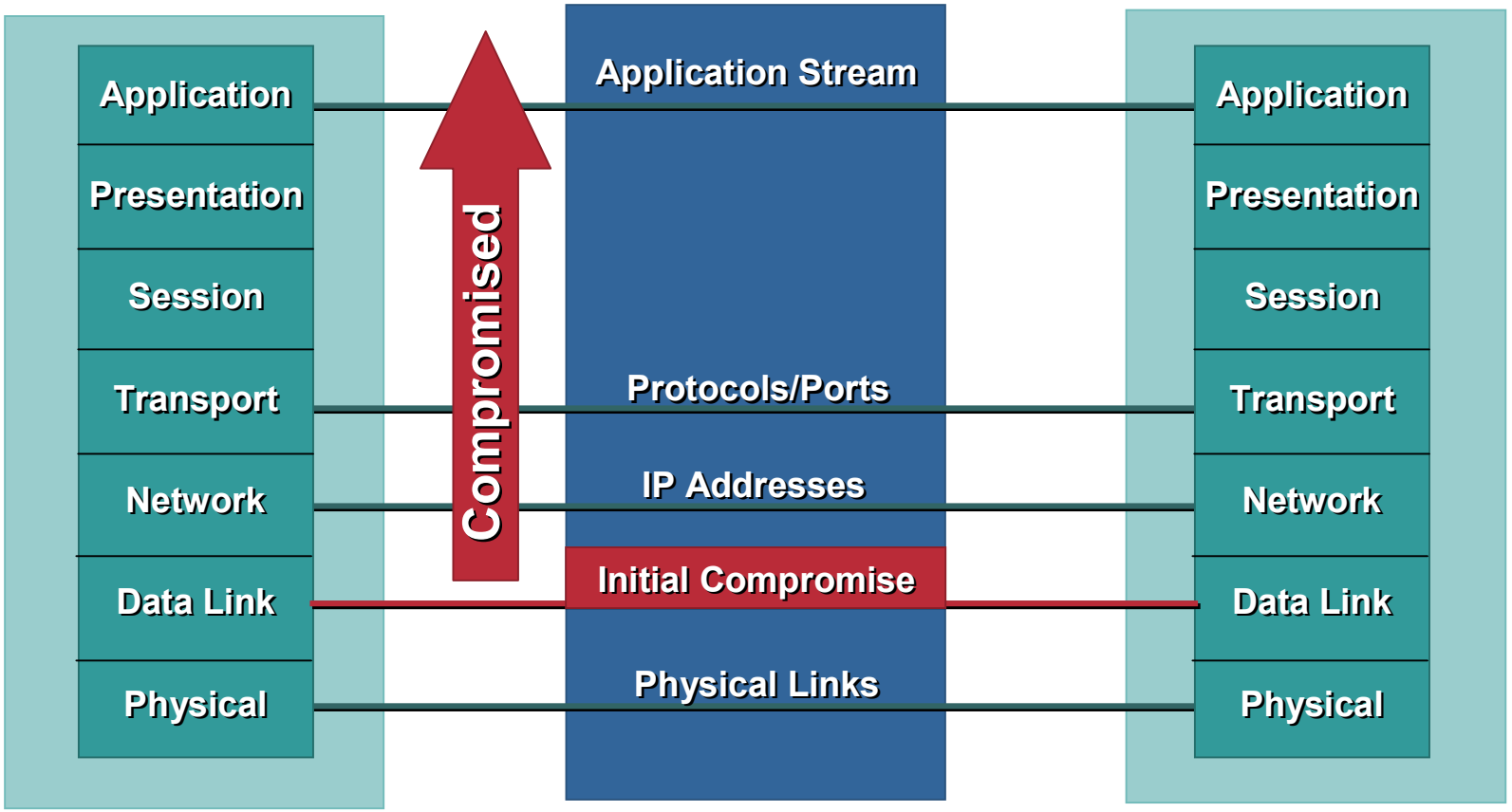
Cisco Systems

Distinguished Engineer

Evyncke@cisco.com

The Domino Effect

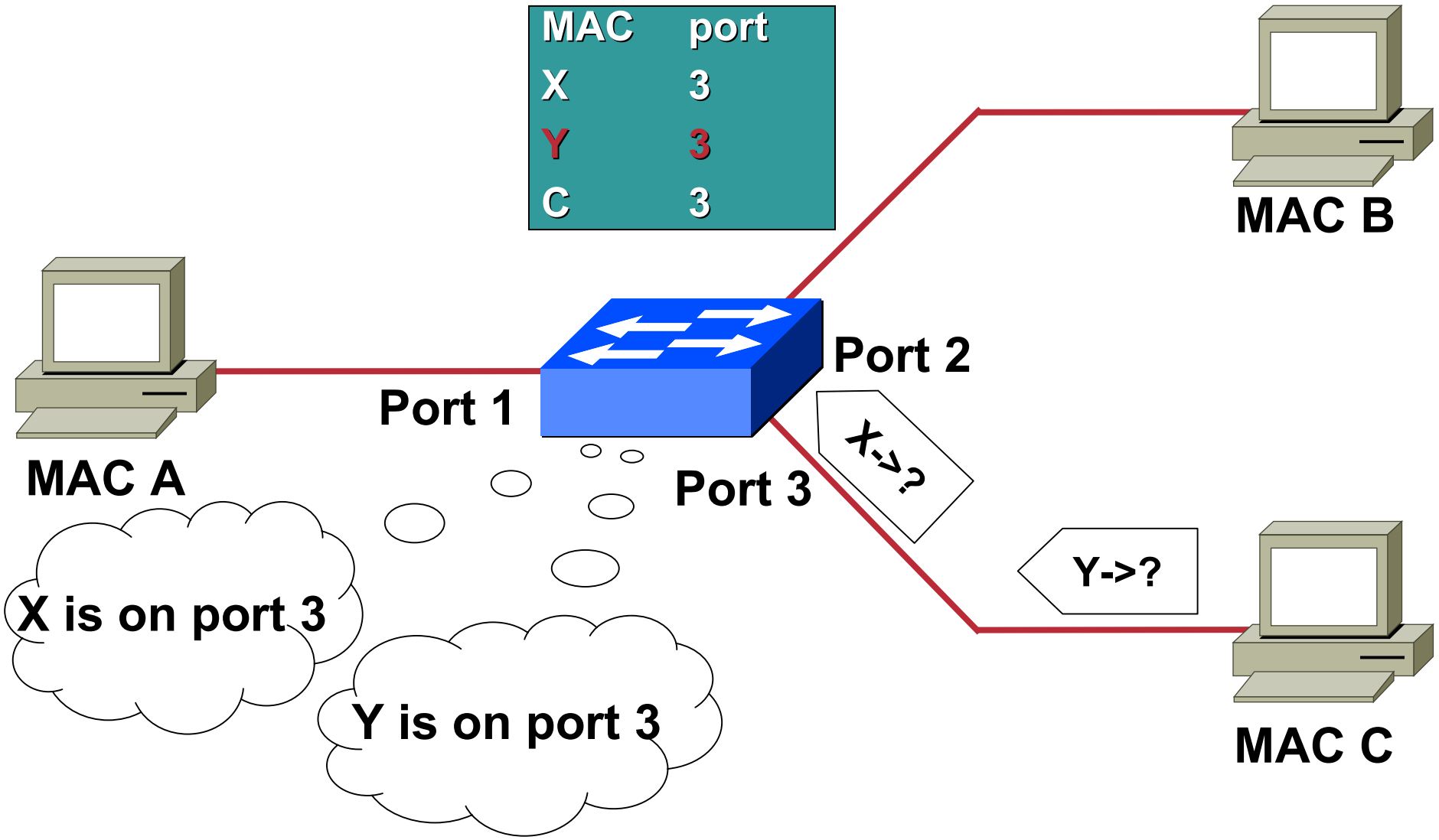
- Unfortunately this means if one layer is hacked, communications are compromised without the other layers being aware of the problem
- Security is only as strong as your weakest link
- When it comes to networking, layer 2 can be a VERY weak link



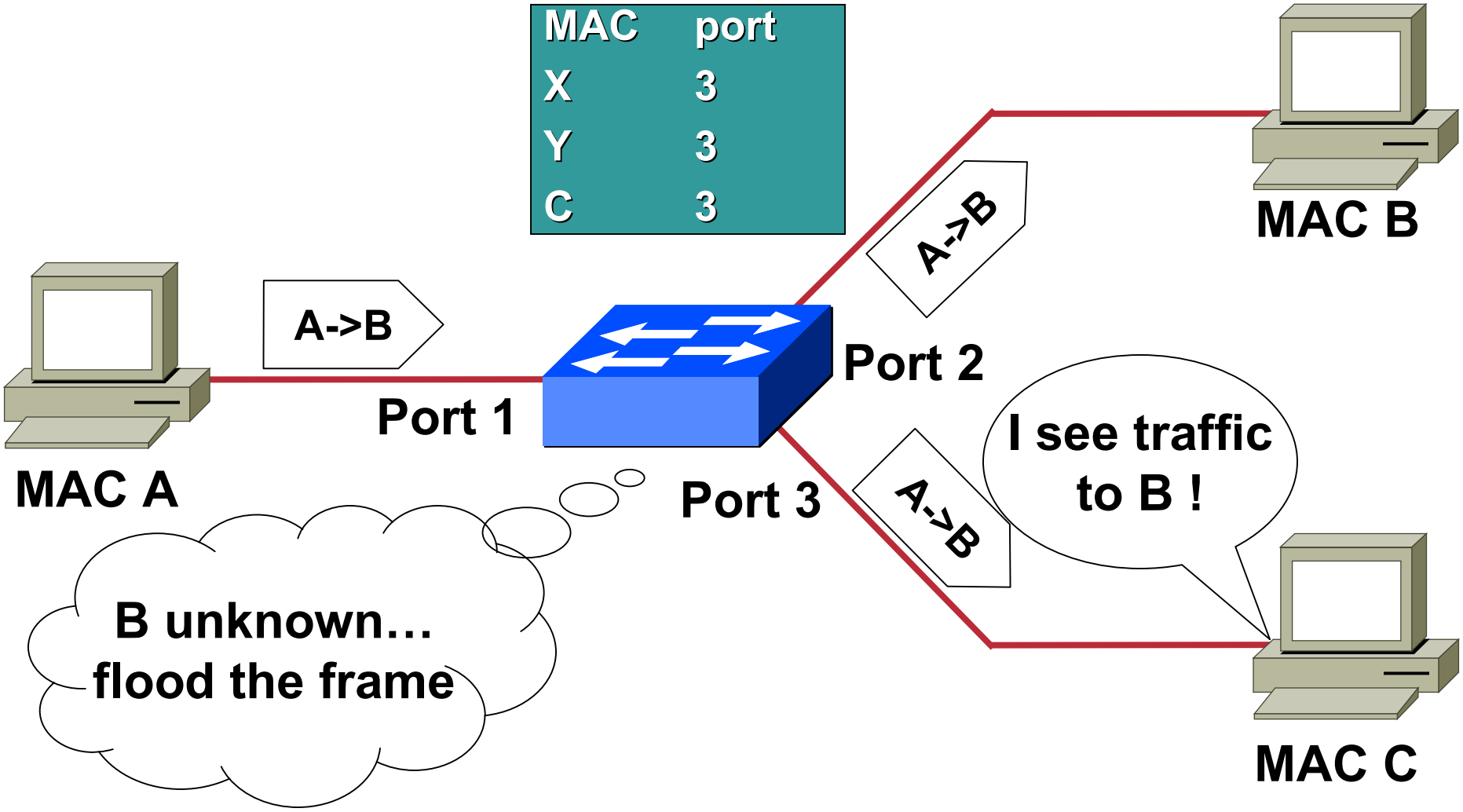
MAC Attacks

CAM Overflow 1/2

Cisco.com



CAM Overflow 2/2



MAC Flooding Attack Mitigation

- **Port Security**

  Allows you to specify MAC addresses for each port, or to learn a certain number of MAC addresses per port

  Upon detection of an invalid MAC block only the offending MAC or just shut down the port

- **Smart CAM table**

  Never overwrite existing entries

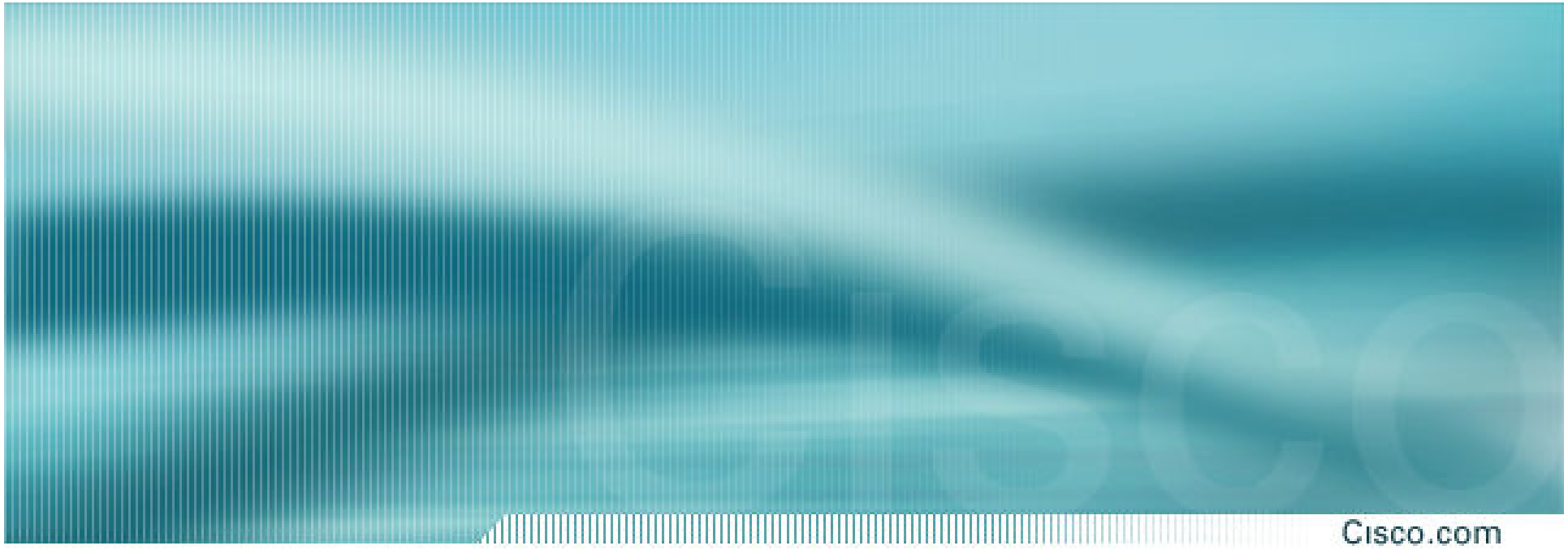
  Only time-out inactive entries

  Active hosts will never be overwritten

- **Speak first**

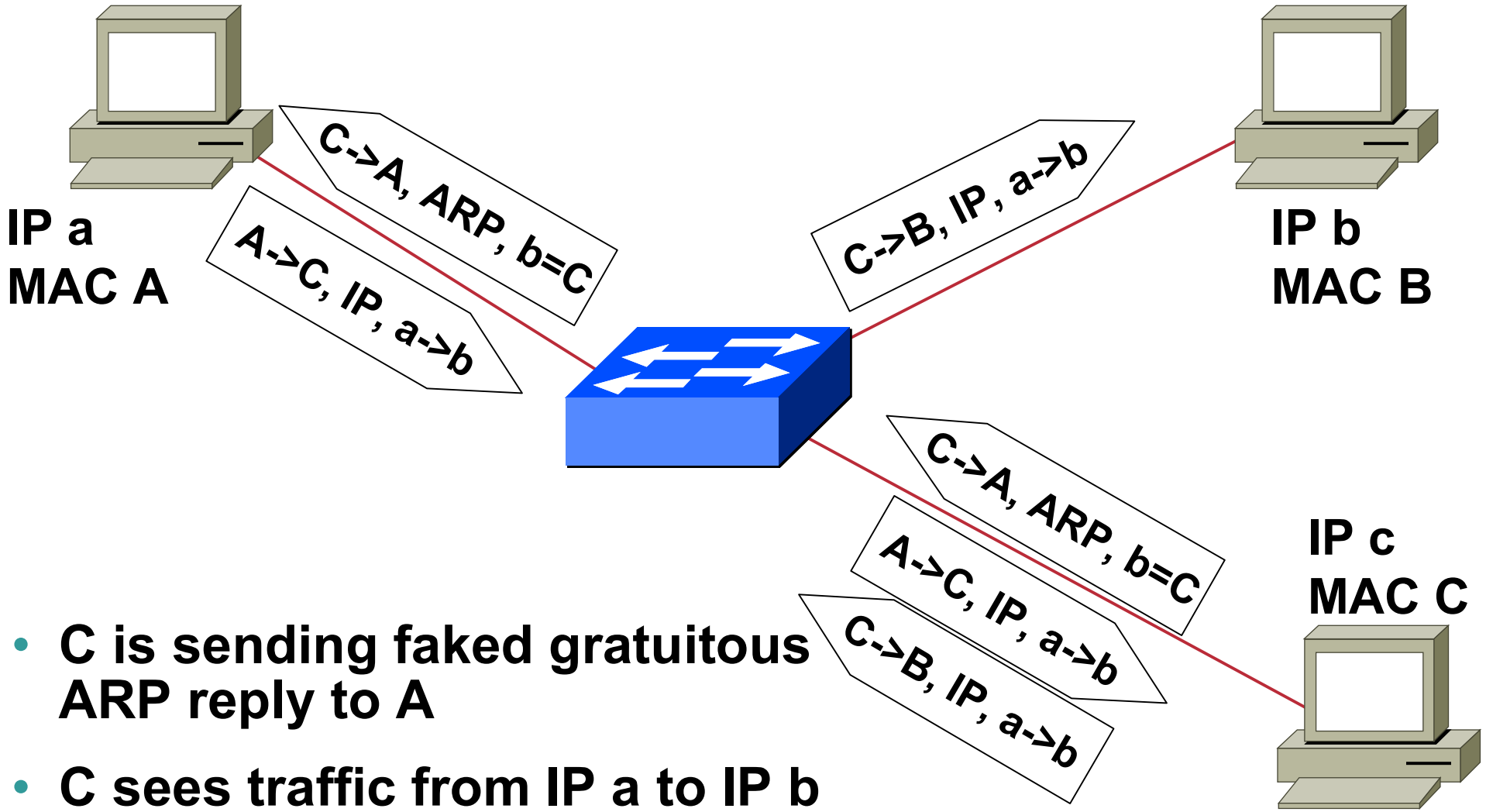
  Deviation from learning bridge: never flood

  Requires a hosts to send traffic first before receiving



ARP Attacks

ARP Spoofing



- C is sending faked gratuitous ARP reply to A
- C sees traffic from IP a to IP b

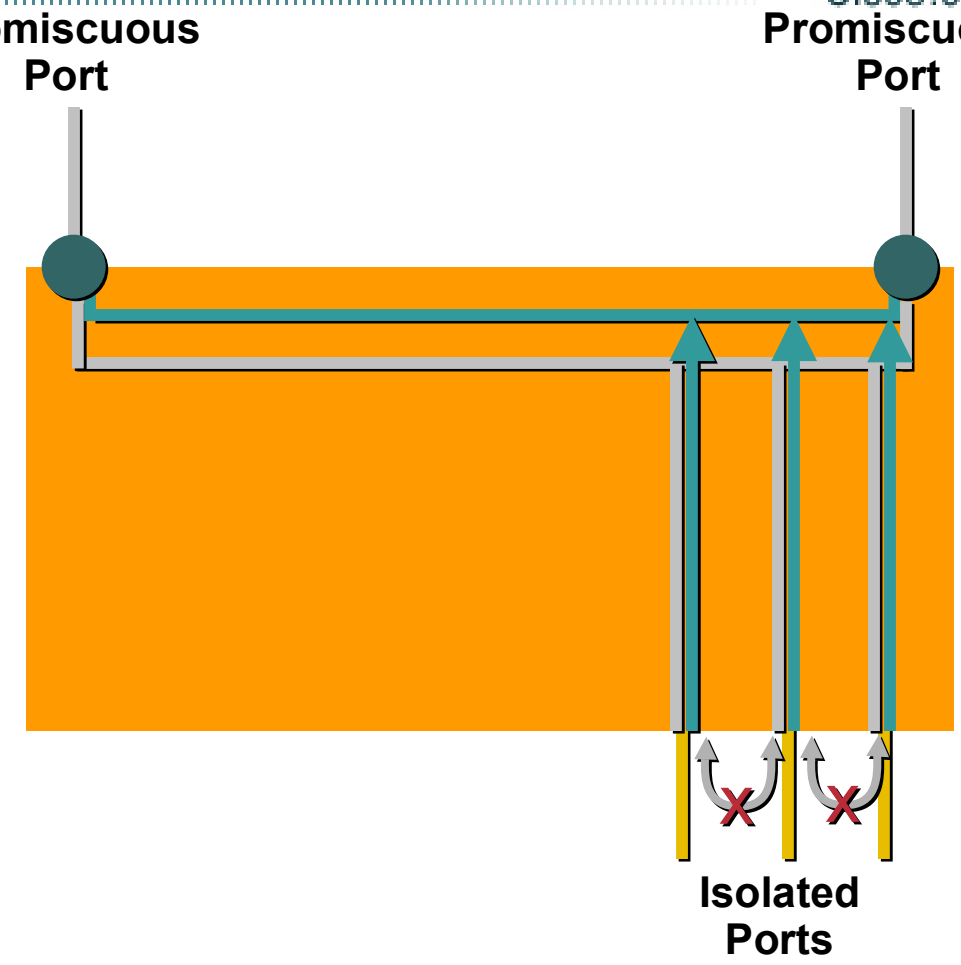
Mitigating ARP Spoofing

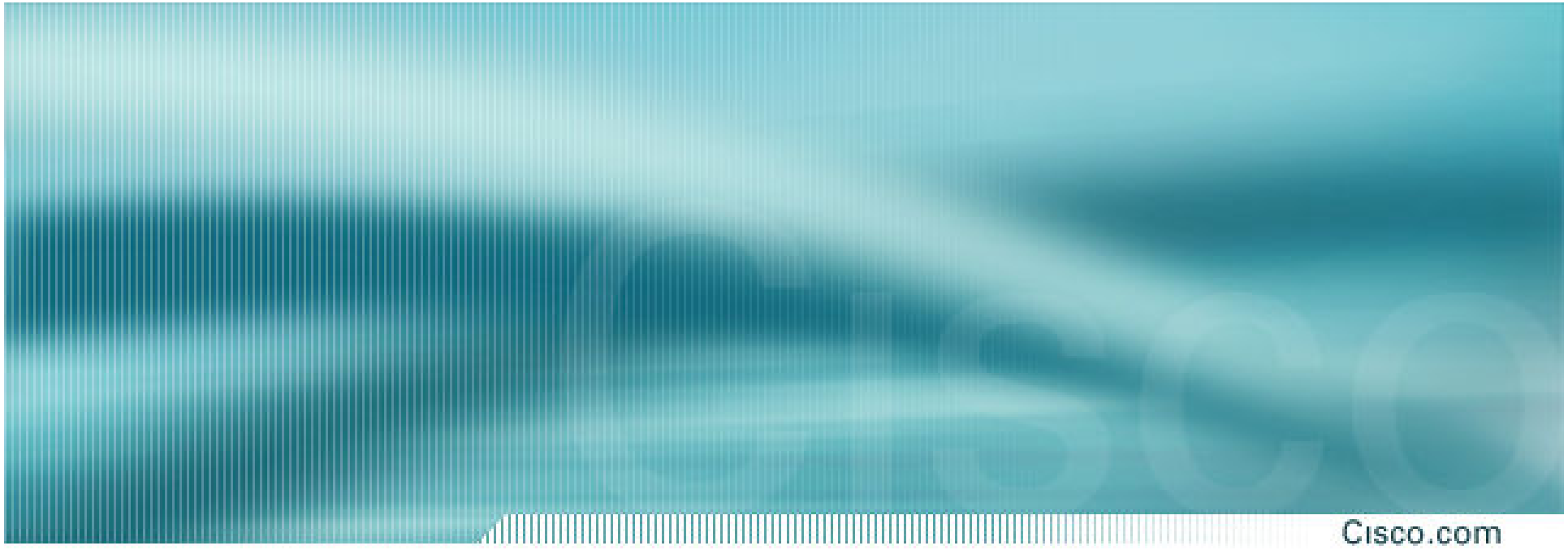
- ARP spoofing works only within one VLAN
- static ARP table on critical stations (but dynamic ARP override static ARP on most hosts!)
- ARP ACL: checking ARP packets within a VLAN
  - Either by static definition
  - Or by snooping DHCP for dynamic leases
- No direct communication among a VLAN: private VLAN
  - Spoofed ARP packet cannot reach other hosts

ARP Spoof Mitigation: Private VLANs

Primary VLAN

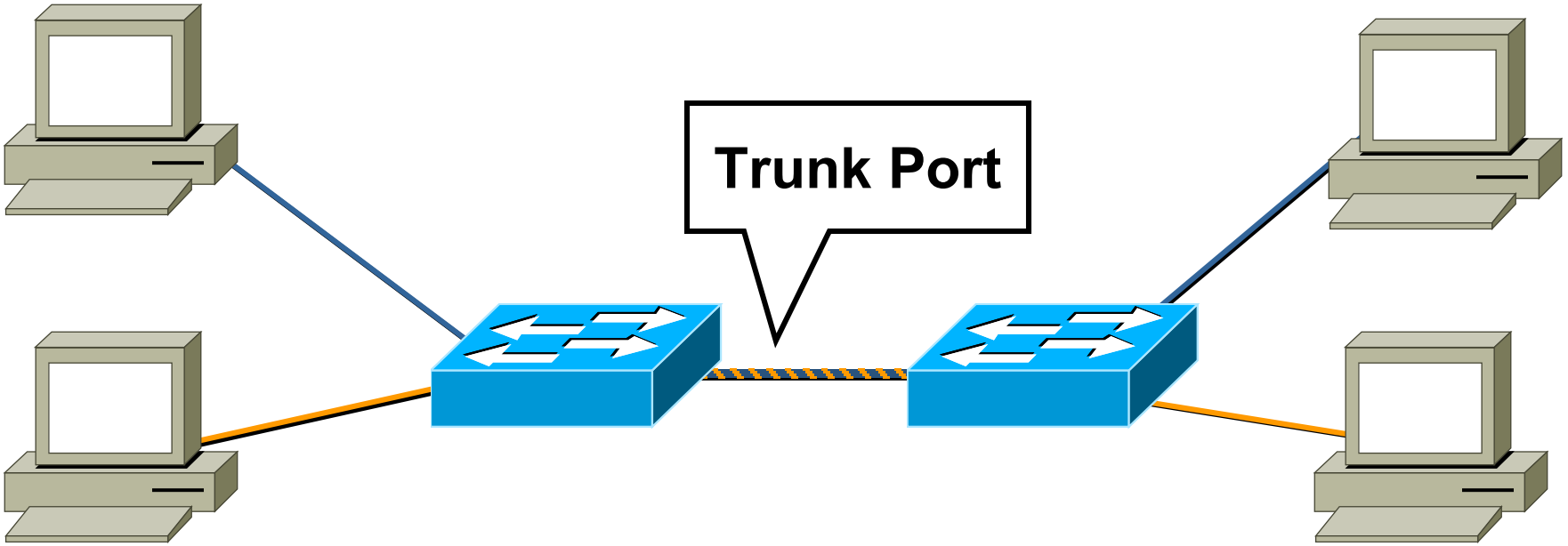
Isolated VLAN





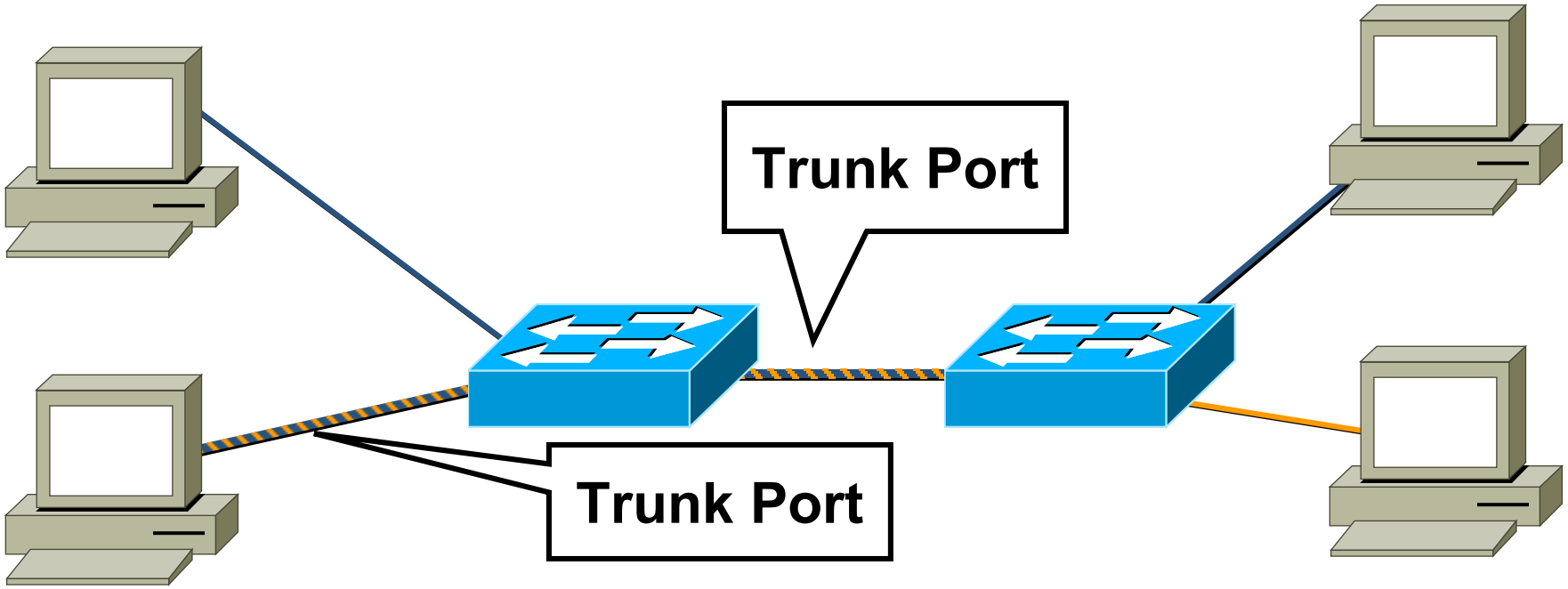
VLAN “Hopping” Attacks

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)**

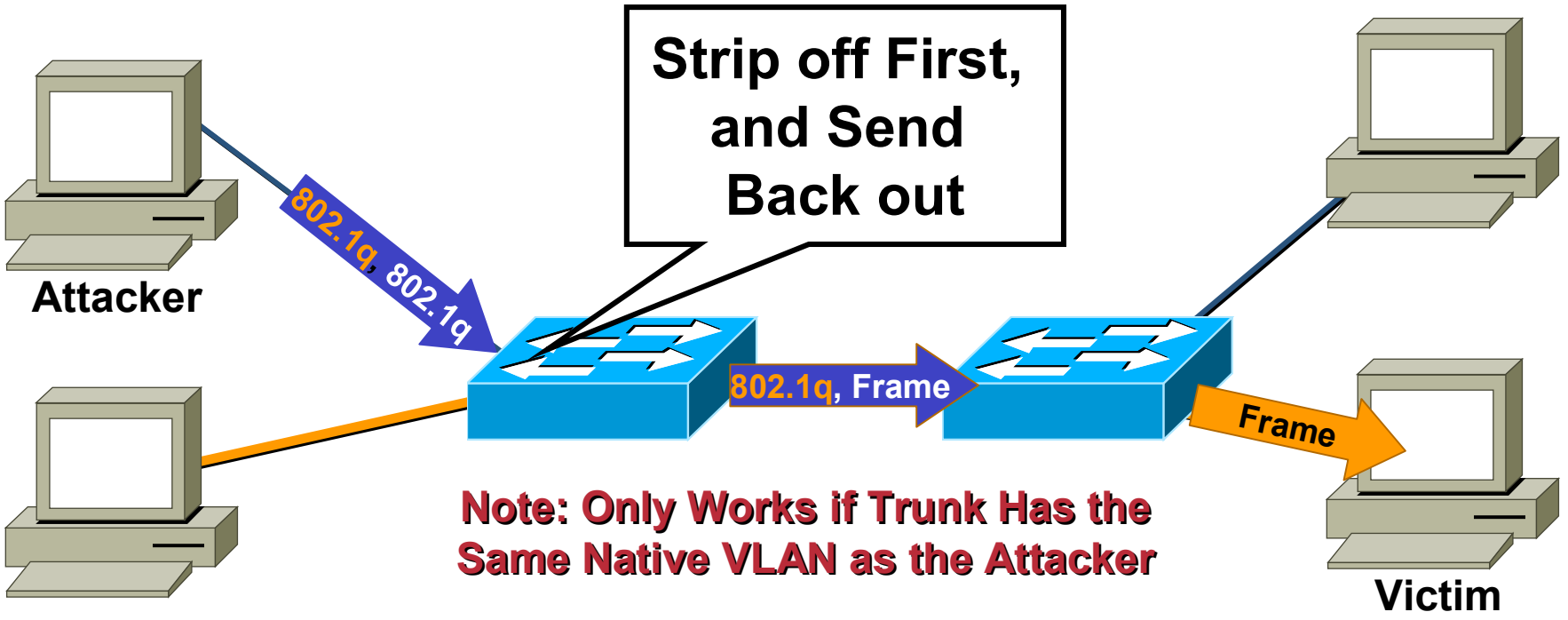
Basic VLAN Hopping Attack



- A station can spoof as a switch with 802.1Q signaling
- 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

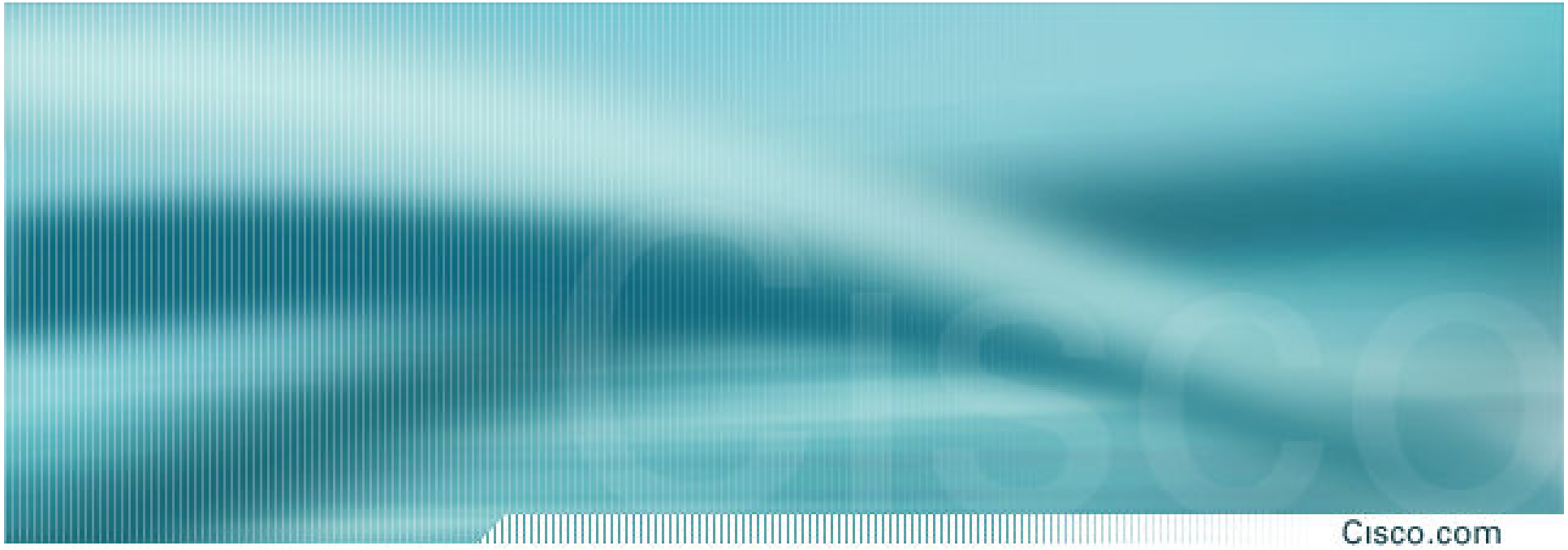


- Send double encapsulated 802.1Q frames
- Switch performs only one level of decapsulation
- Unidirectional traffic only
- Works even if trunk ports are set to off

Mitigation

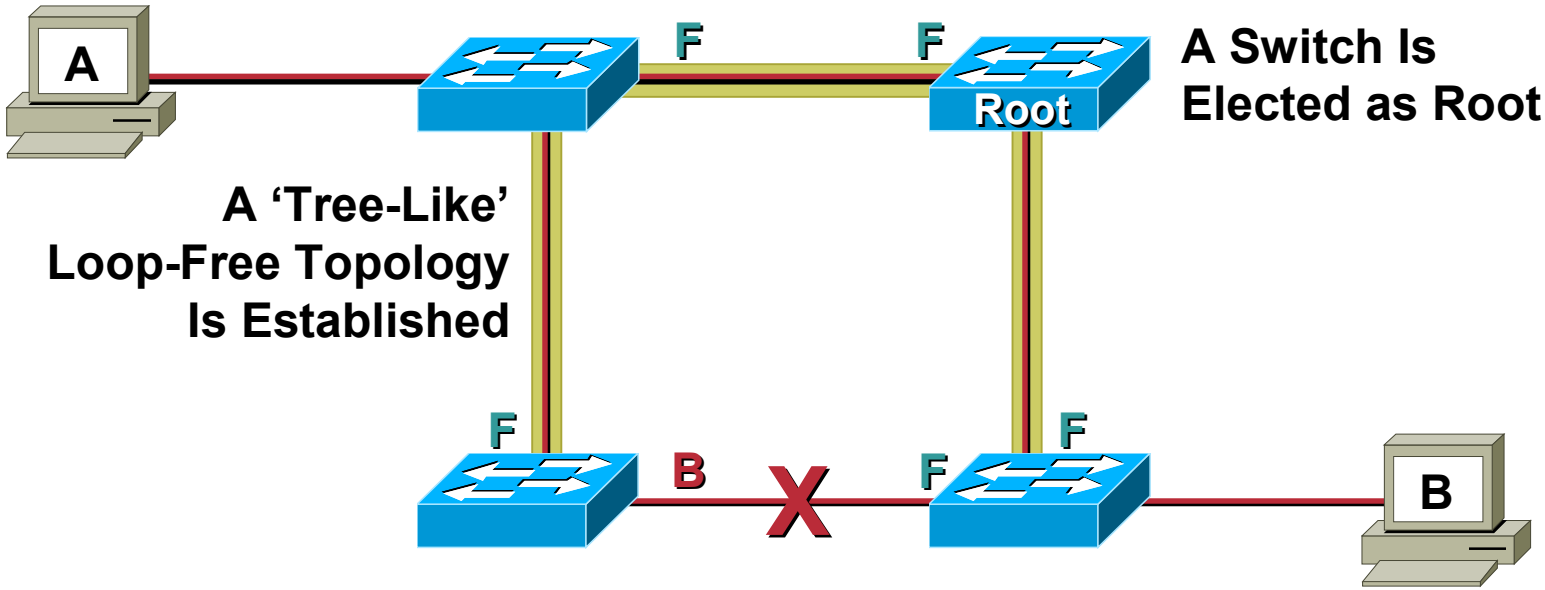
Cisco.com

- Use recent switches
- Disable auto-trunking
- Never put host in the trunk native VLAN
- Put unused ports in an unused VLAN



Spanning Tree Attacks

Spanning Tree Basics

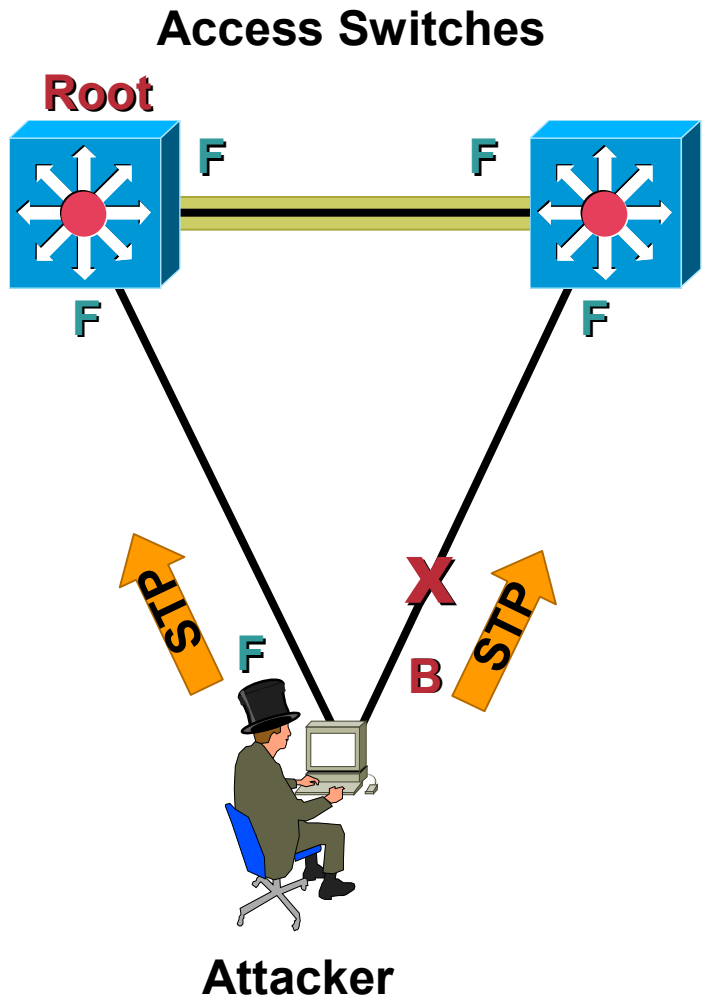


Loop-Free Connectivity

Spanning Tree Attack Example 1/2

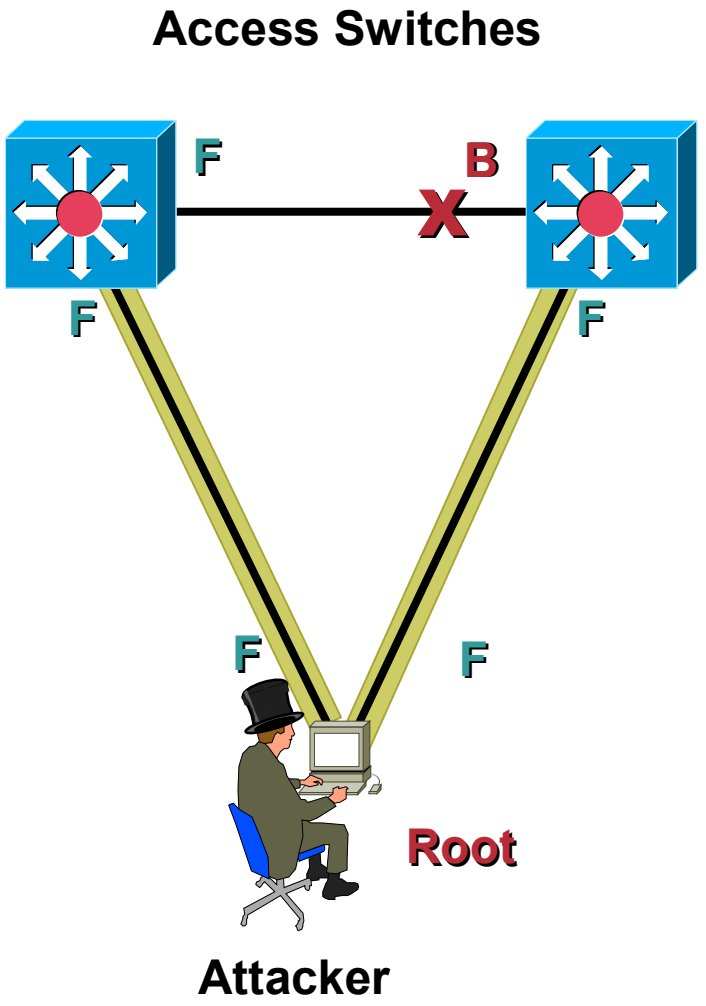
Cisco.com

- **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**

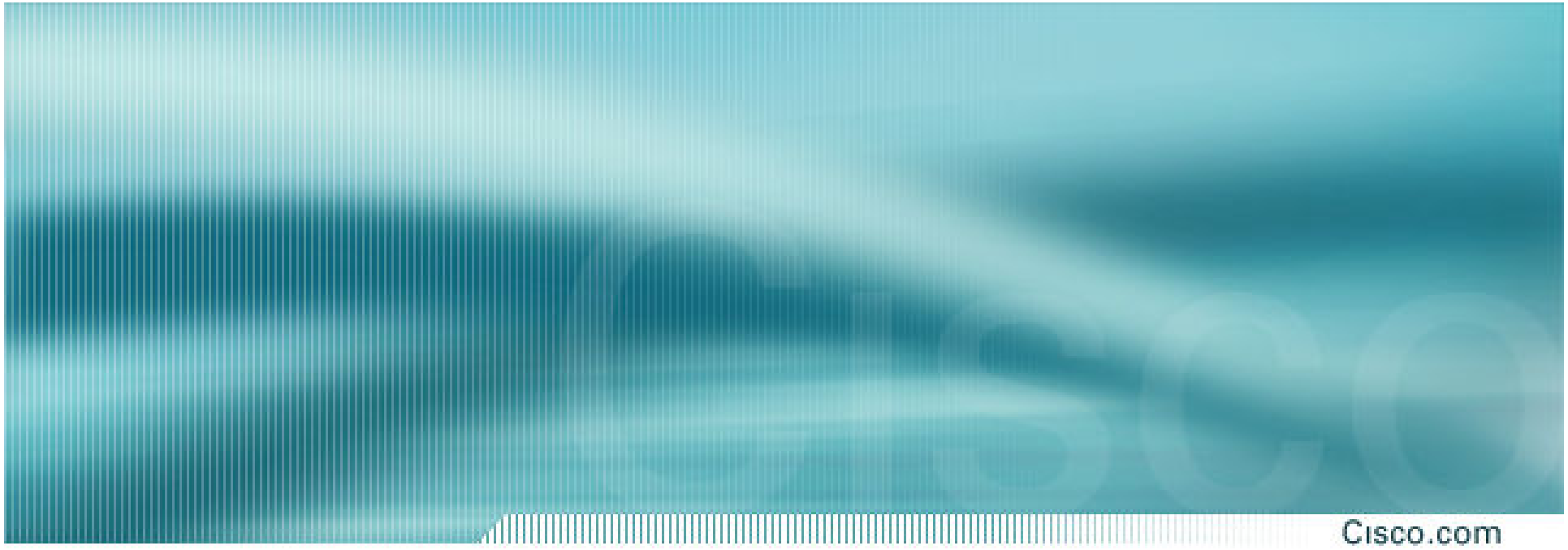


STP Attack Mitigation

- **Disable STP**
  (It is not needed in loop free topologies)
- **BPDU Guard**

  Disables ports upon detection of a BPDU message on the port
- **Root Guard**

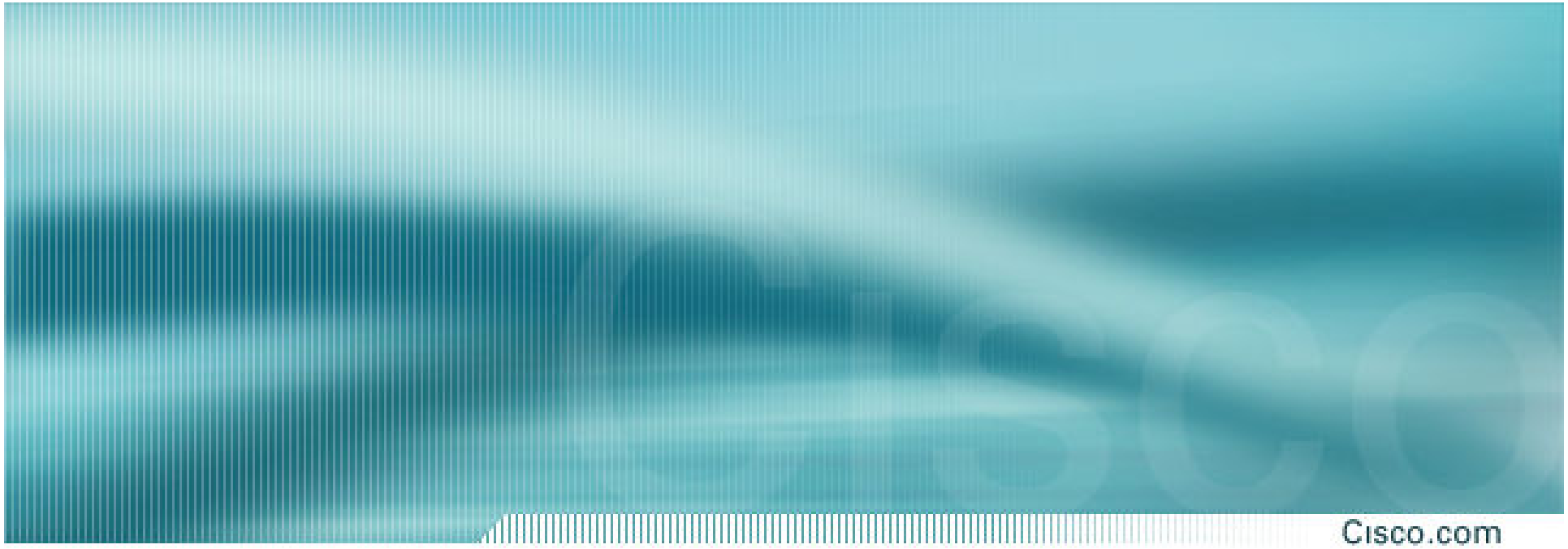
  Disables ports who would become the root bridge due to their BPDU advertisement



Other Attacks

DHCP Rogue Server Attack

- **Simply the installation of an unknown DHCP Server in the local subnet**
- **Other attack: exhaustion of DHCP pools**
- **RFC 3118 “Authentication for DHCP Messages” will help, but has yet to be implemented**
- **Mitigation:**
  - **Consider using multiple DHCP servers for the different security zones of your network**
  - **Use intra VLAN ACL to block DHCP traffic from unknown server**



ProActive Defense

Wire-Speed Access Control Lists

- Many current switches offer wire-speed ACLs to control traffic flows (with or without a router port)
- Allows implementation of edge filtering that might otherwise not be deployed due to performance concerns
- VLAN ACLs and Router ACLs are typically the two implementation methods

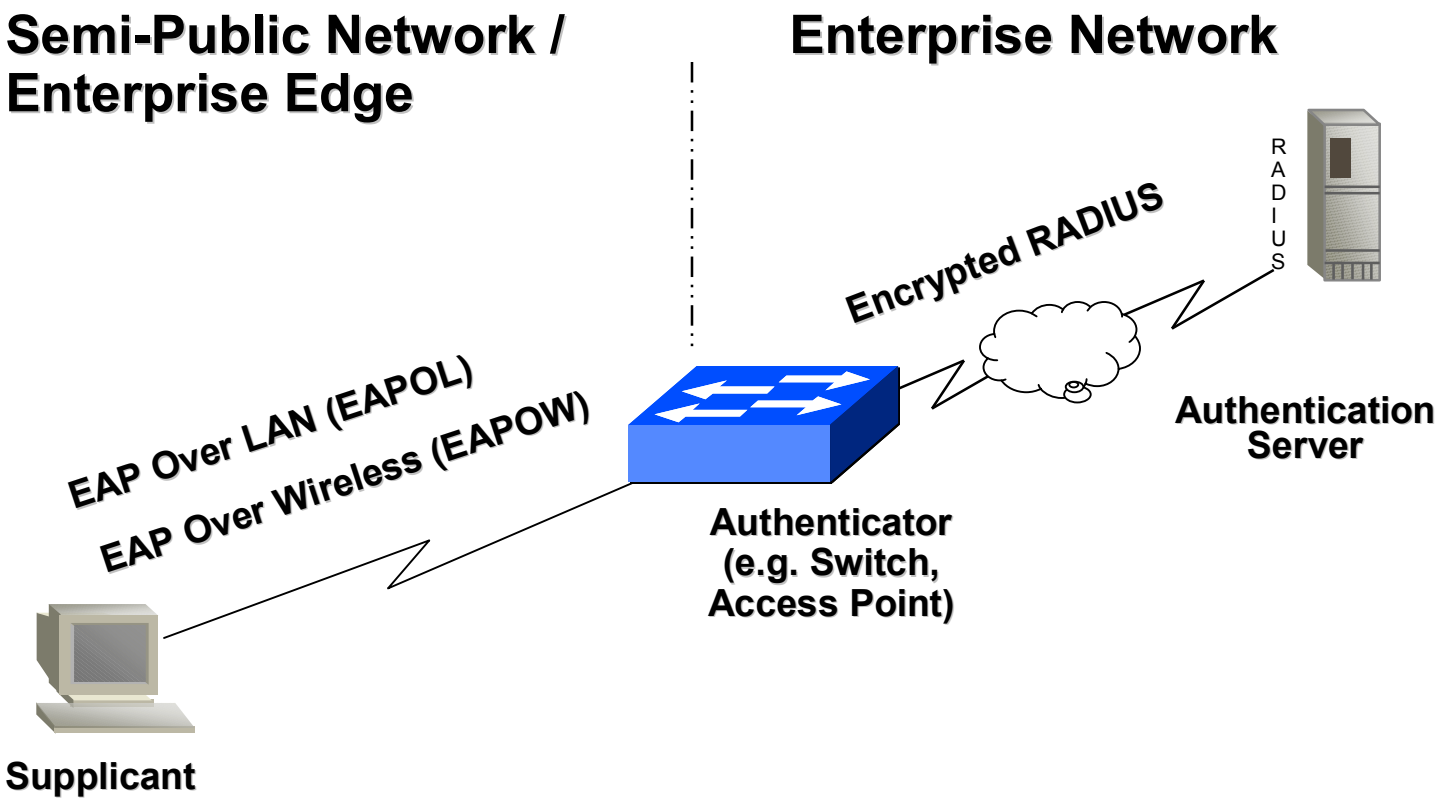
Network Intrusion Detection System

- **Network IDS are now able to**
  - **Understand trunking protocols**
  - **Fast enough to handle 1 Gbps**
    - *Including management of alerts !*
  - **Understand layer 2 attacks**

802.1x

- **802.1x is an IEEE Standard for *Port Based Network Access Control***
  - **EAP based**
  - **Improved user authentication: username and password**
  - **Can work on plain 802.3 or 802.11**

IEEE 802.1X Terminology



What Does it Do?

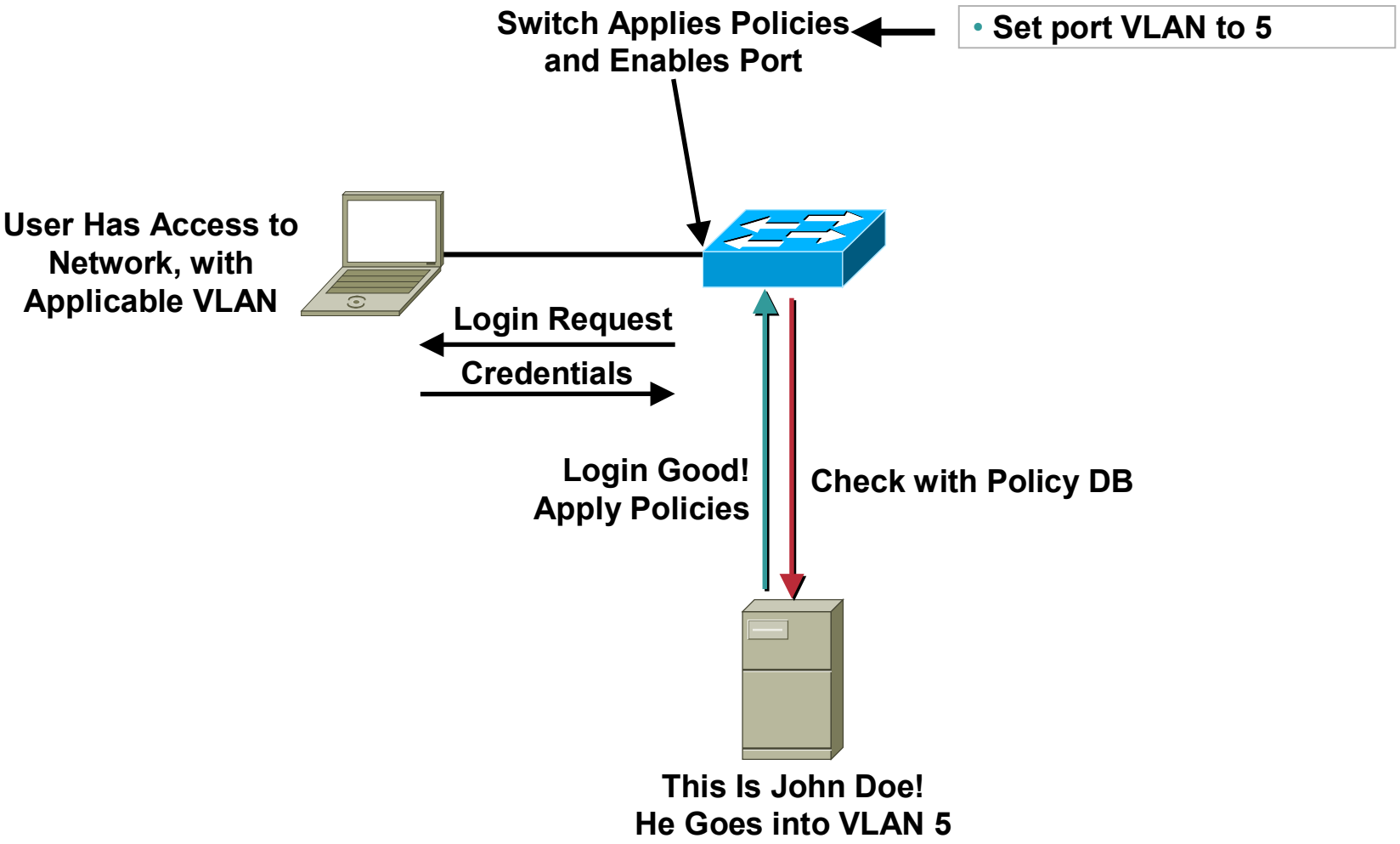
- Transport authentication information in the form of Extensible Authentication Protocol (EAP) payloads.
- The authenticator (switch) becomes the middleman for relaying EAP received in 802.1x packets to an authentication server by using RADIUS to carry the EAP information.
- Three forms of EAP are specified in the standard

  EAP-MD5 – MD5 Hashed Username/Password

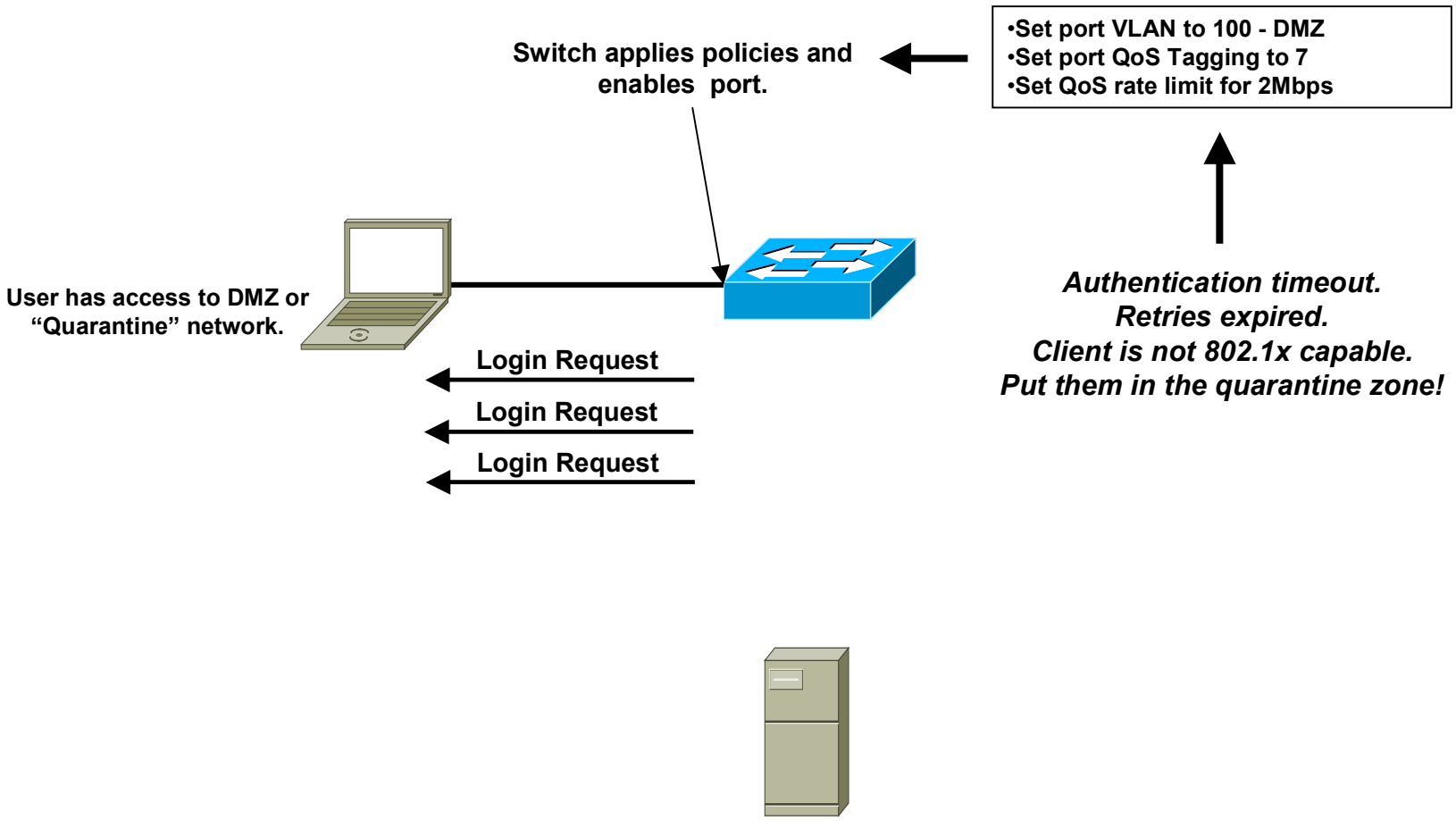
  EAP-OTP – One-Time Passwords

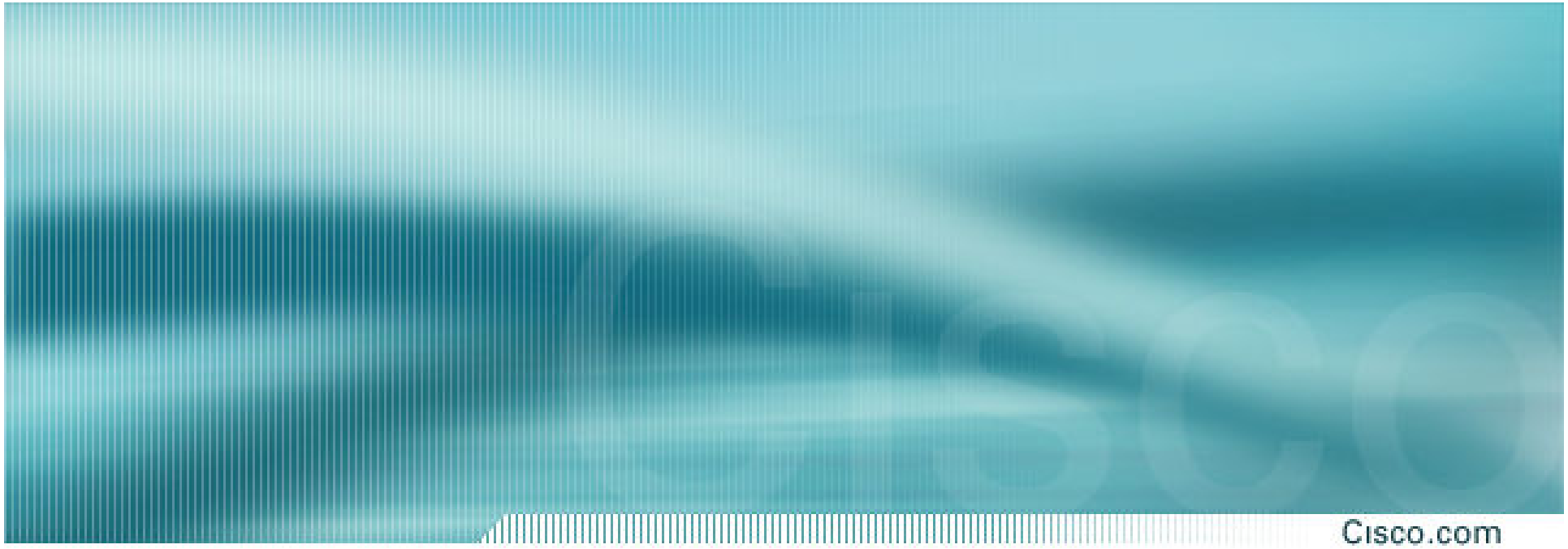
  EAP-TLS – Strong PKI Authenticated Transport Layer Security (SSL) - Preferred Method Of Authentication

Example Solution “A”—Access Control and User Policy Enforcement



Example Solution “B” – Access For Guest Users





Summary

Layer 2 Security Best Practices 1/2

Cisco.com

- 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
- Disable all unused ports and put them in an unused VLAN
- Consider 802.1X for middle term

All of the Preceding Features Are Dependant on Your Own Security Policy

Final Word

- **Switches were not designed for security**
- **Now, switches are designed with security in mind**
- **In most cases, with good configuration, they can even enhance your network security**