Security Possibilities at Layer 2

Allan Alton, BSc, CISA, CISSP

http://www3.telus.net/alton

UBC

September 29, 2005

Caveats and Assumptions

- Opinions expressed are my own and do not represent the views of UBC, my employer, any vendor, or any organization to which I am associated
- Internet Protocol (IP) implementation in a switched environment is assumed
- Familiarity with basic networking assumed
- Control of user traffic, not management of the network device
  - Secure management of the switch is assumed

Caveats and Assumptions

- Concepts are from a context of Cisco Systems equipment, but sufficiently general to apply to other network hardware vendors
- Switch features are not available on all product lines – check with your vendor
- Remediations presented are possibilities not recommended best practice
- Test before implementation as bugs may be are present

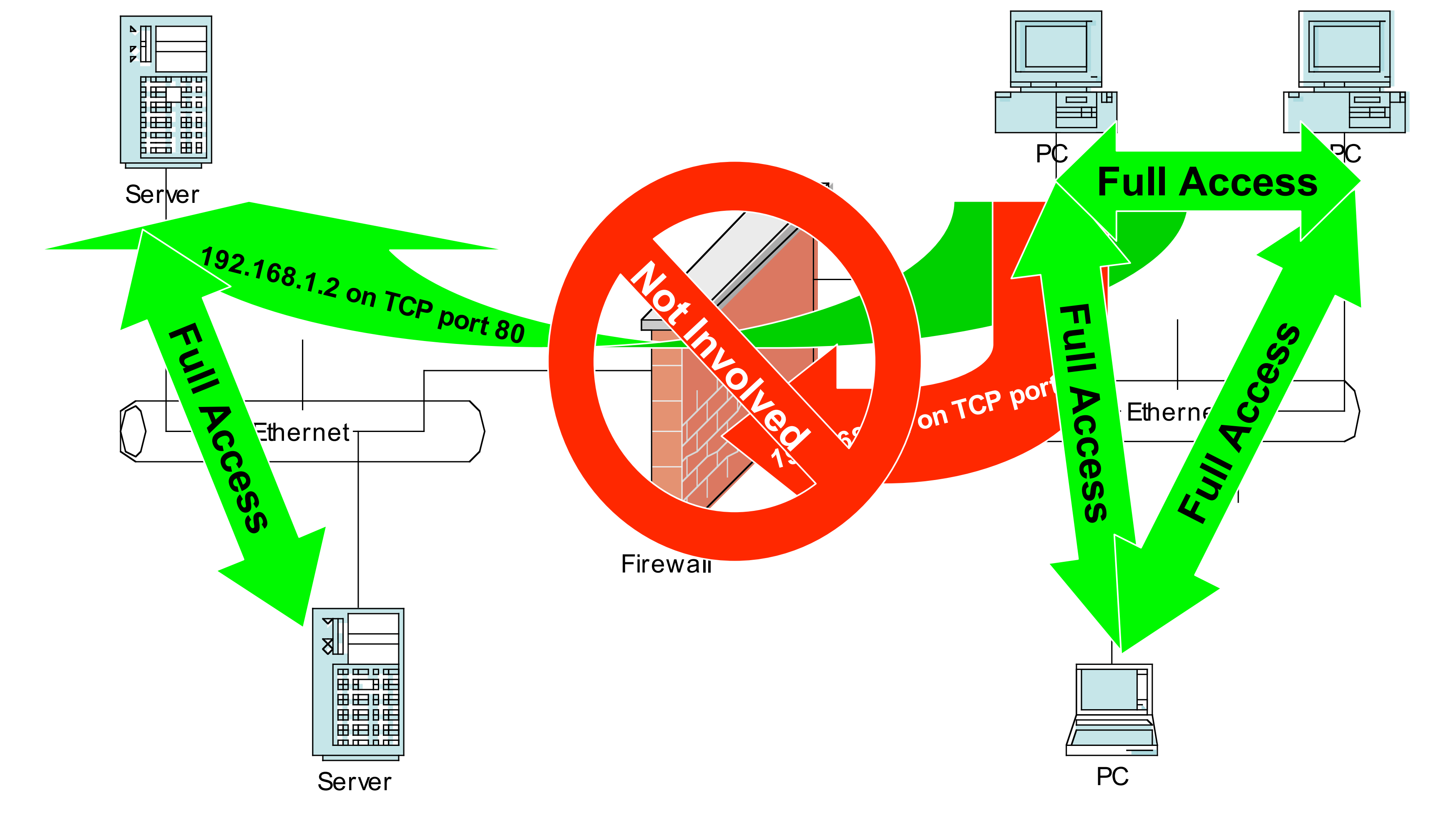
Assertion

Intelligence built into the new generation of switches will permit greater control of data as it enters your network

Traditional Network Security

- OSI Layers 3 and 4 where most network controls are implemented
  - e.g.,192.168.1.2 can only be contacted on TCP port 80 from subnets beginning with 172.16.
- Firewall rules and router access lists

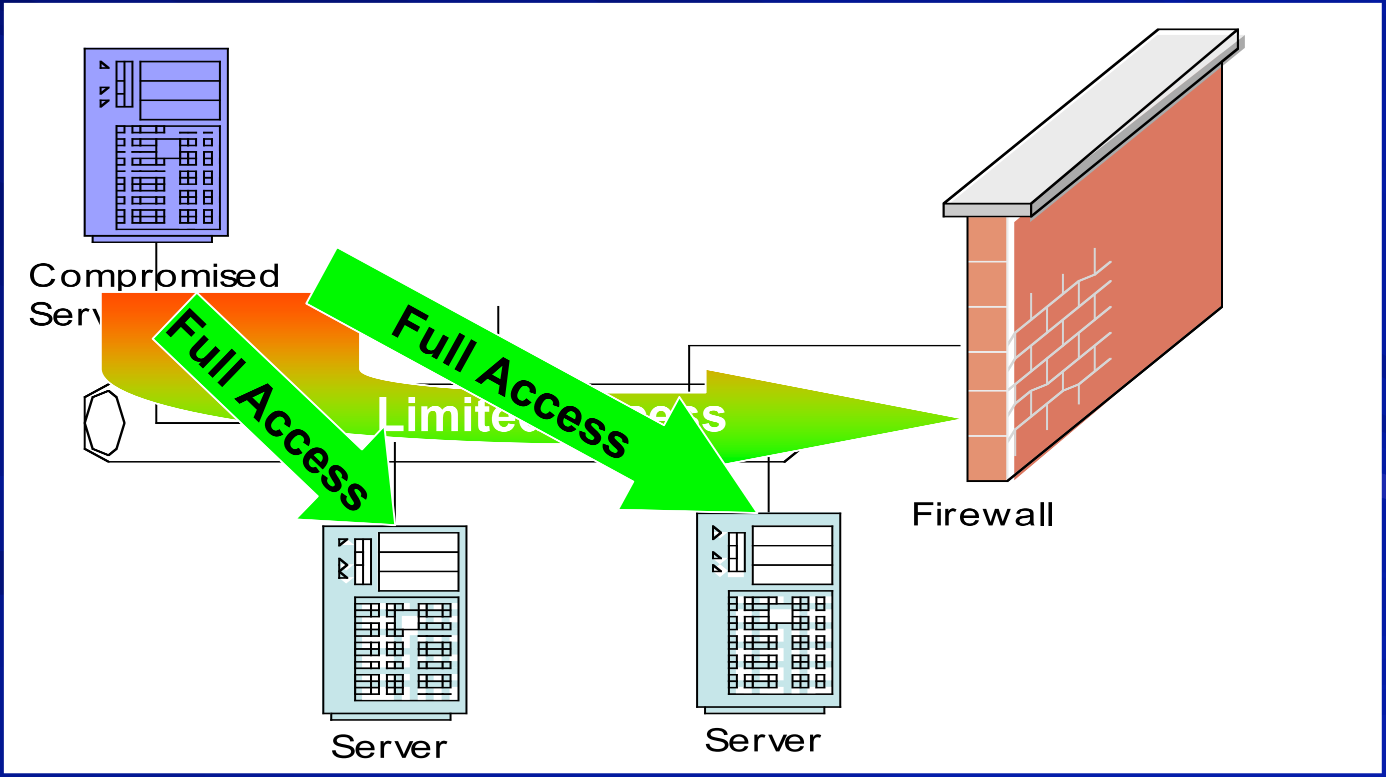
Traditional Network Security



Vulnerability

Attack within subnet

- Compromised machines can access others on the same VLAN by default



Remediation

Private VLANs

- **Promiscuous:** talks to any port
- **Isolated:** talks only to promiscuous
- **Community:** talks only to same community or promiscuous

	promiscuous	isolated	community A	community B
promiscuous	Yes	Yes	Yes	Yes
isolated	Yes	No	No	No
community A	Yes	No	Yes	No
community B	Yes	No	No	Yes

Remediation

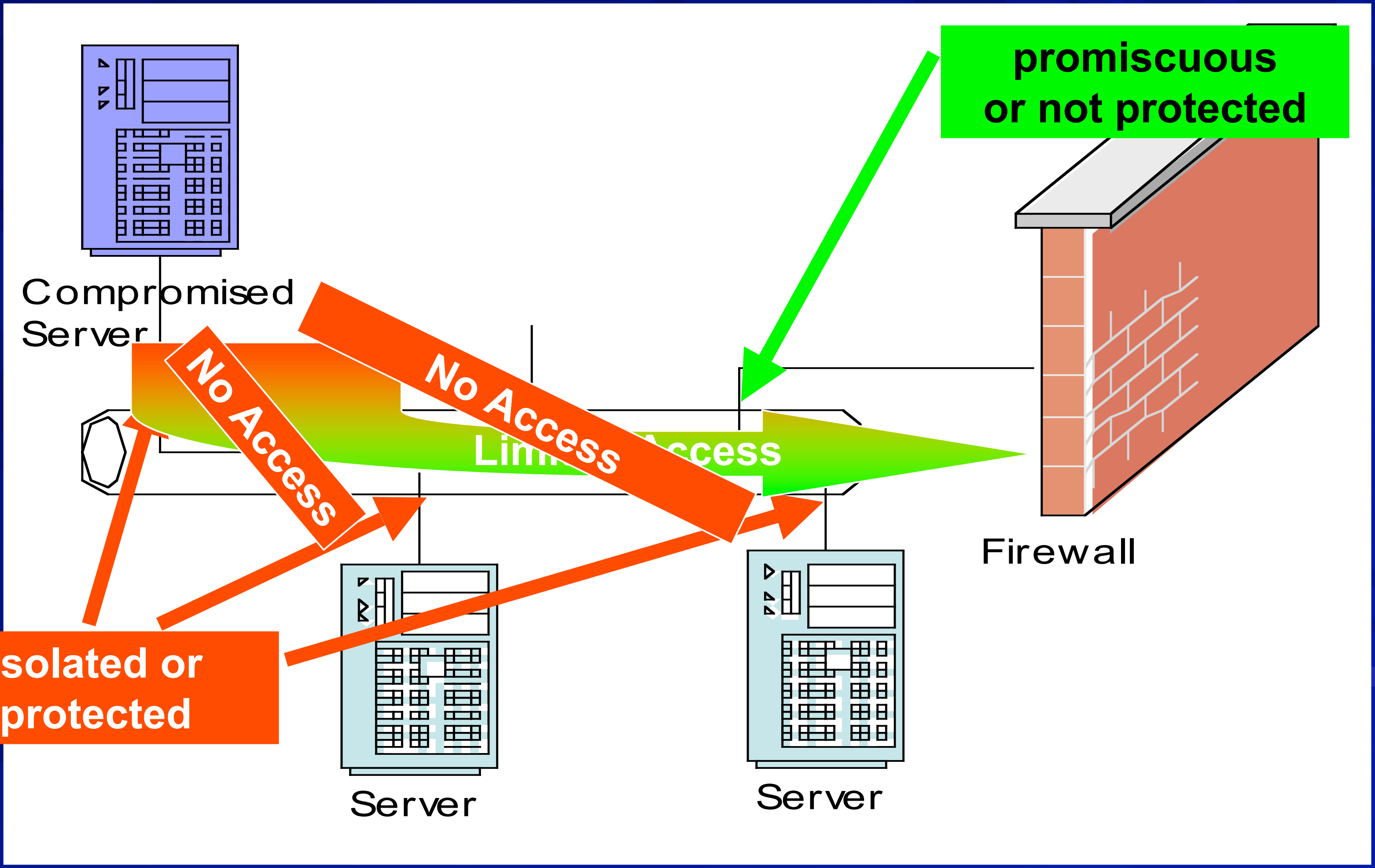
Protected Ports

- Simpler form of a Private VLAN
  - Protected: similar to Isolated
  - Not protected: similar to Promiscuous
- Only applicable to the local switch however

	protected	not protected
protected	No	Yes
not protected	Yes	Yes

Remediation

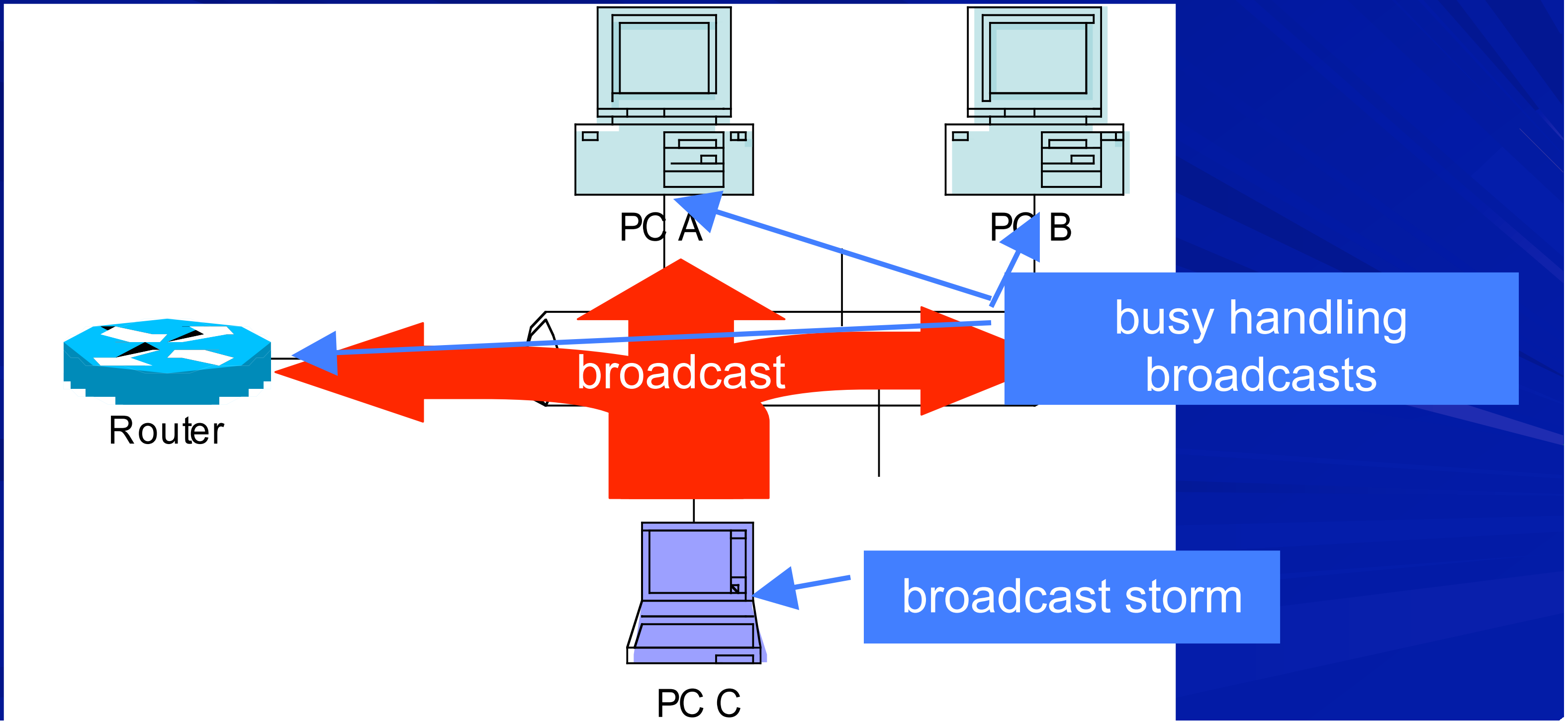
Private VLANs or Protected Ports



Vulnerability

Broadcast Storm

- All devices in VLAN / subnet must handle broadcasts, consuming resources.
- OS or application bugs may produce constant broadcasts. May also be malicious.



busy handling broadcasts

broadcast storm

Remediation

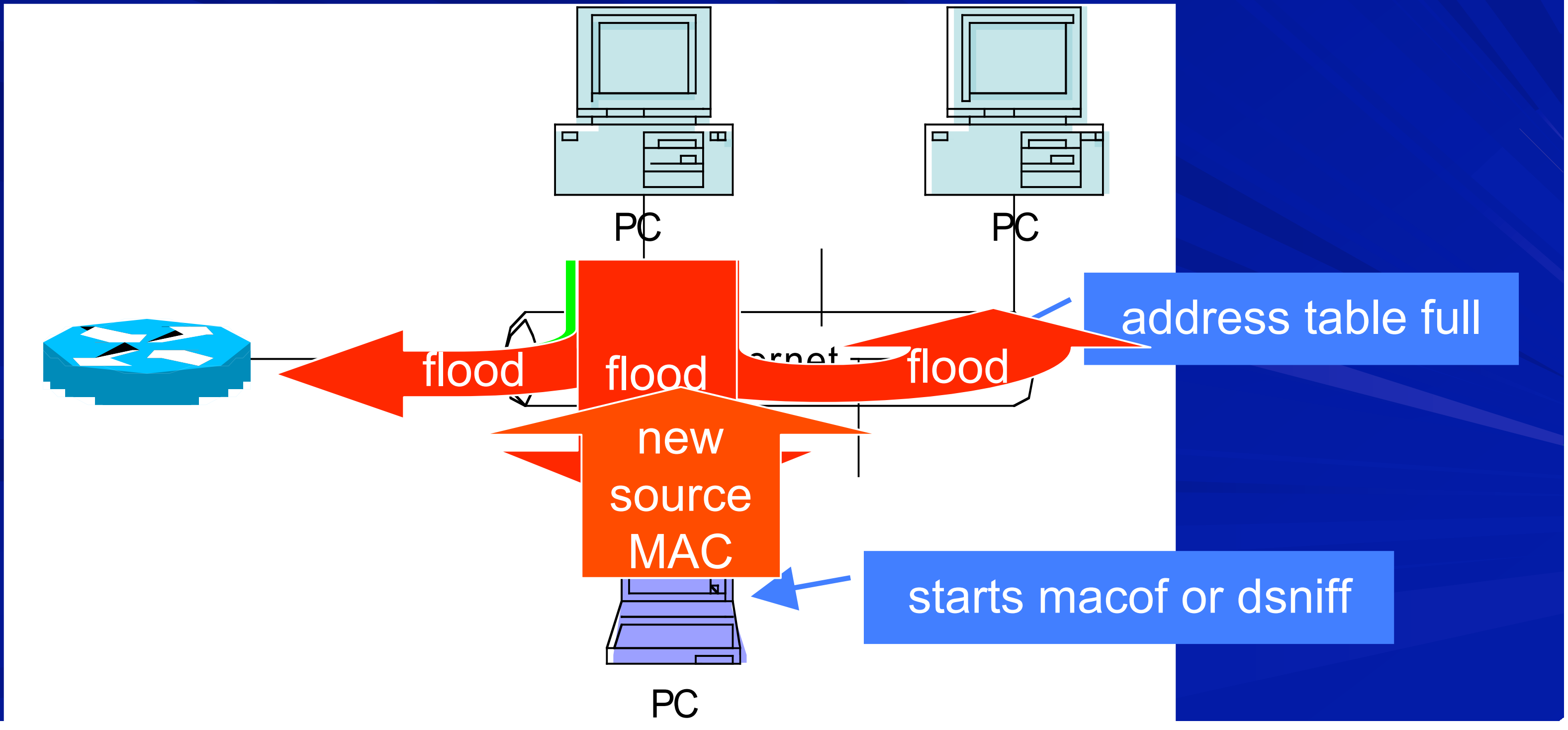
Storm Control

- Can apply to broadcasts, multicasts, or unicasts
- Set threshold as percentage of bandwidth over a 1 second period
- If threshold is exceeded, drop this type of packet for next 1 second period

Vulnerability

Flooding for Data Capture or Performance Hit

- Switches flood to all ports when MAC unknown
- Switches learn MAC addresses at each port
- Table of addresses is a finite size



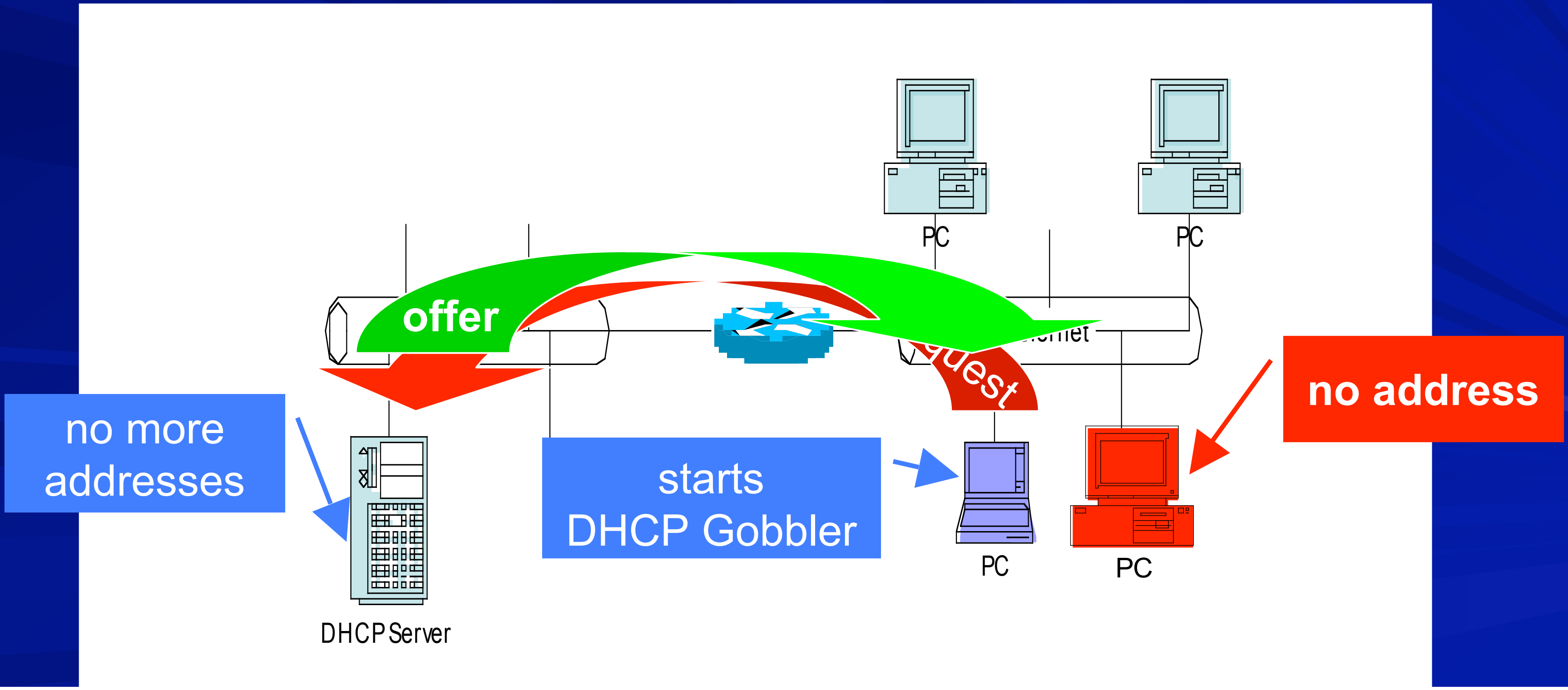
address table full

starts macof or dsniff

Vulnerability

DHCP Denial of Service

- Attacker requests new addresses for bogus MACs
- Finite number of DHCP addresses in a subnet
- PCs coming on the network can not get address



Remediation

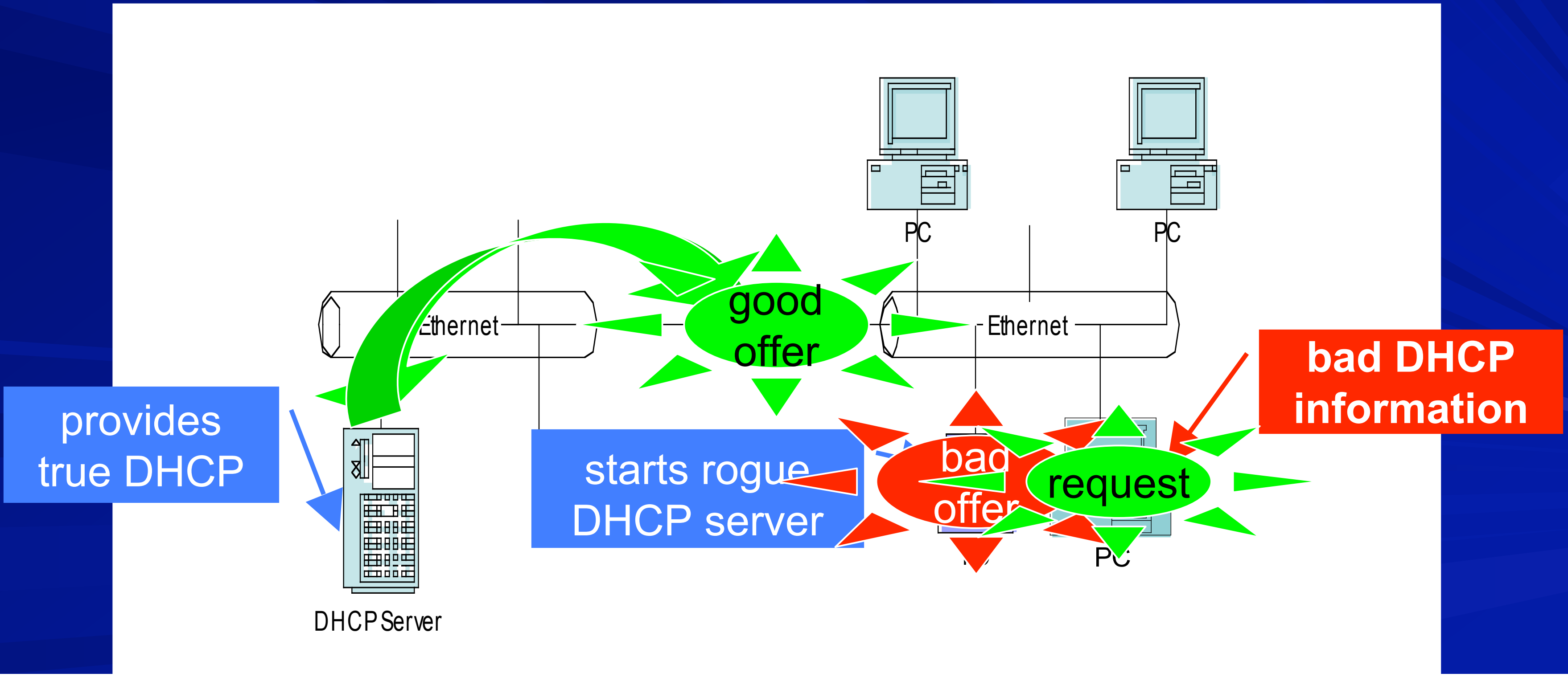
Port Security

- Limits the source MAC addresses on a port
- Can specify static addresses or maximum number
- Violations on ports can
  - disable port
  - send trap and syslog
  - continue forwarding; drop frames with new MACs
  - continue forwarding; age out MAC entries from inactivity

Vulnerability

DHCP Rogue Server

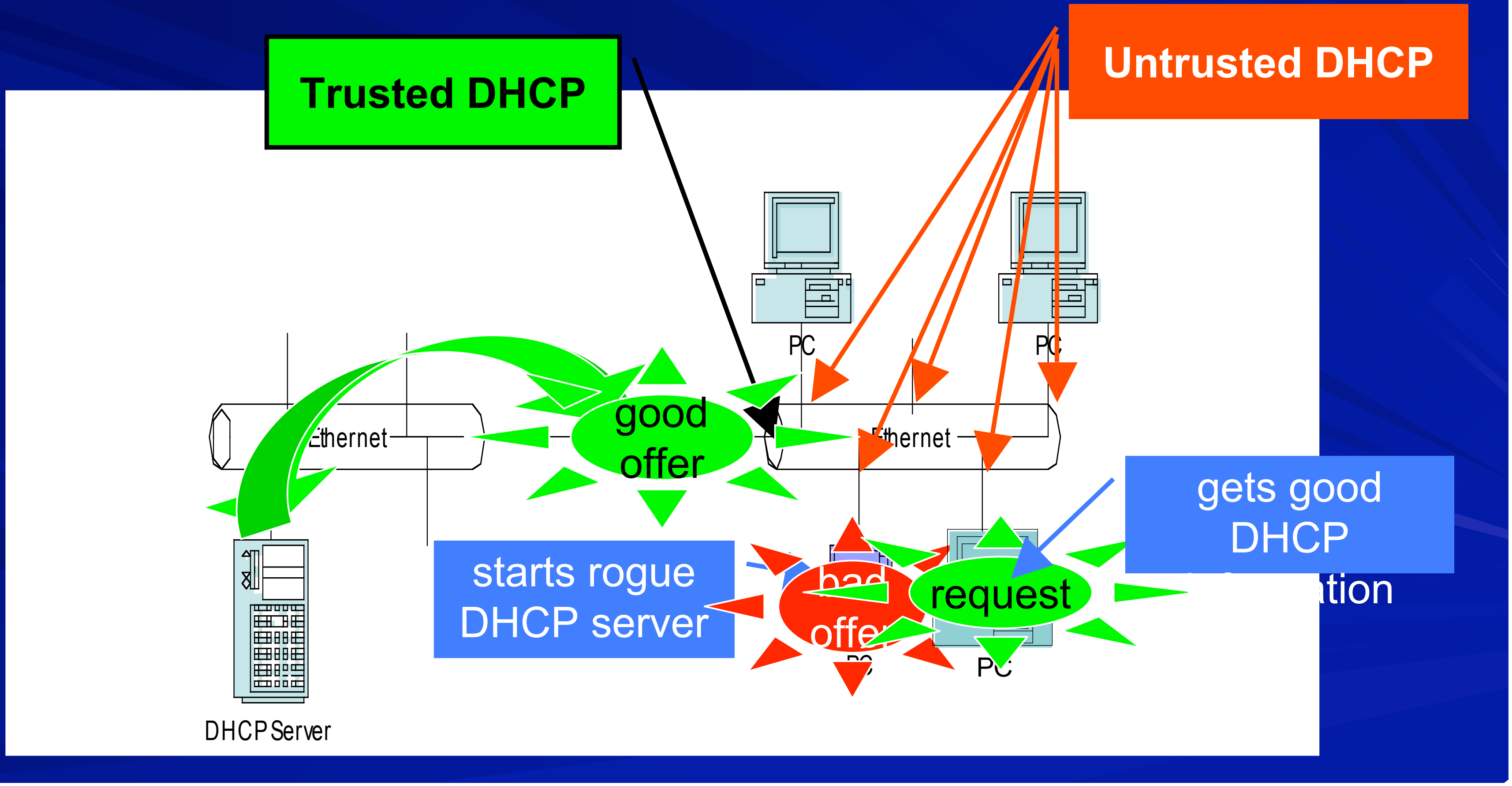
- Attacker uses rogue DHCP server to provide false settings (e.g., DNS, default gateway, etc.)



Remediation

DHCP Snooping

- Define trusted ports for DHCP responses



Trusted DHCP

Untrusted DHCP

good offer

starts rogue DHCP server

bad offer

request

gets good DHCP

Remediation

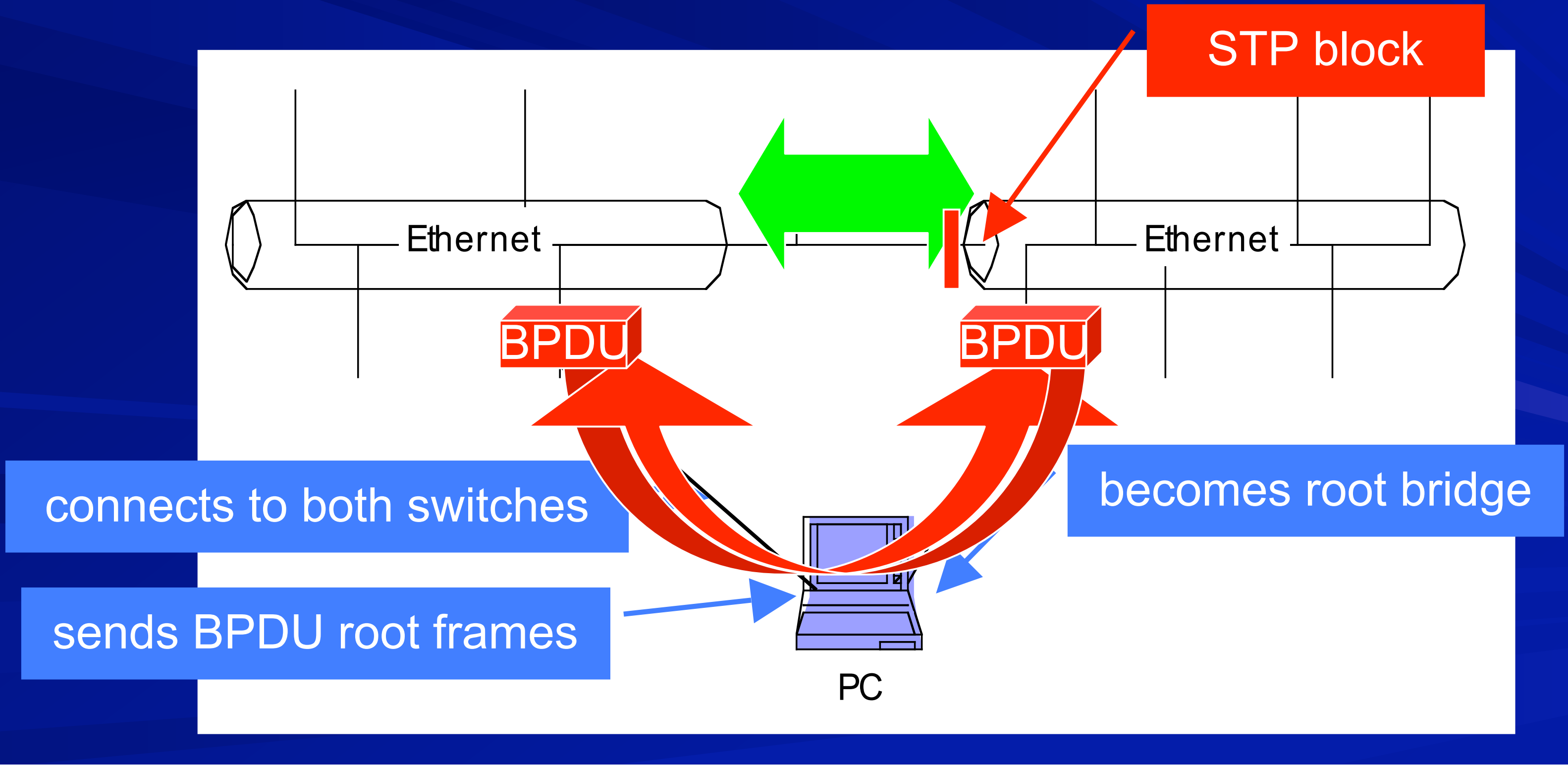
DHCP Snooping – other vulnerabilities covered

- Comparison of MAC address in layers 2 and 7
  - hardware address must match "chaddr" (client hardware address) field in DHCP packet from untrusted ports
  - recall DHCP Gobbler attack and Port Security
- Switch keeps track of the DHCP bindings to prevent DoS release attacks
  - DHCP releases or declines must have the hardware address match the original bound address

Vulnerability

Spanning Tree Root Hijack for Data Capture or Performance Hit

- Spanning Tree Protocol resolves loops
- Bridge Protocol Data Units sent from switches
- Loops broken based on root selection



STP block

connects to both switches

sends BPDU root frames

becomes root bridge

Remediation

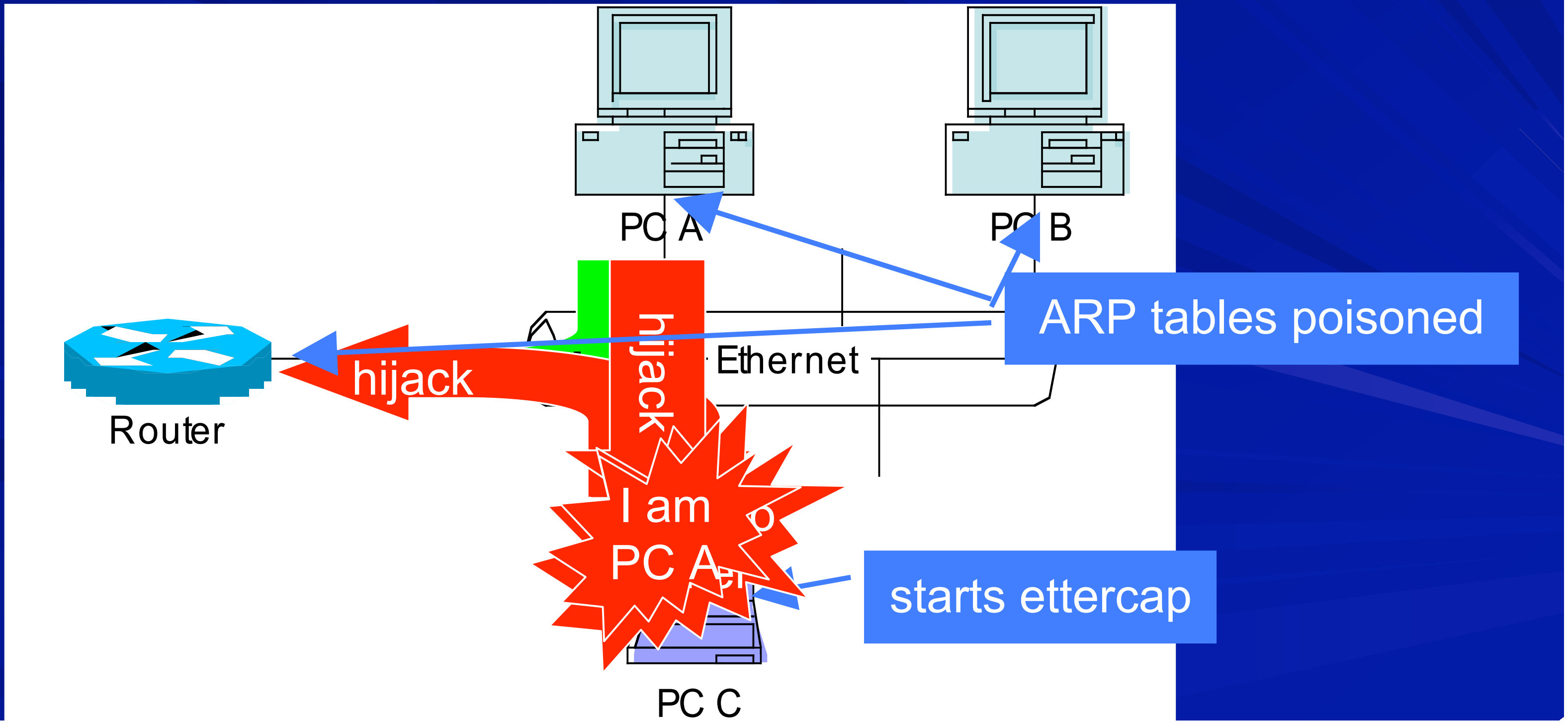
BPDU Guard

- BPDUs should not be received on an access port
- BPDU receipt may indicate unauthorized switch or hub, or an attack
- BPDU receipt puts port into error disabled mode

Vulnerability

ARP Table Poisoning

- ARPs (Address Resolution Protocol) associate layer 3 addresses to layer 2 (IP to MAC)
- Requests are broadcast
- Responses unauthenticated and can be sent without a request (gratuitous)



ARP tables poisoned

starts ettercap

Remediation

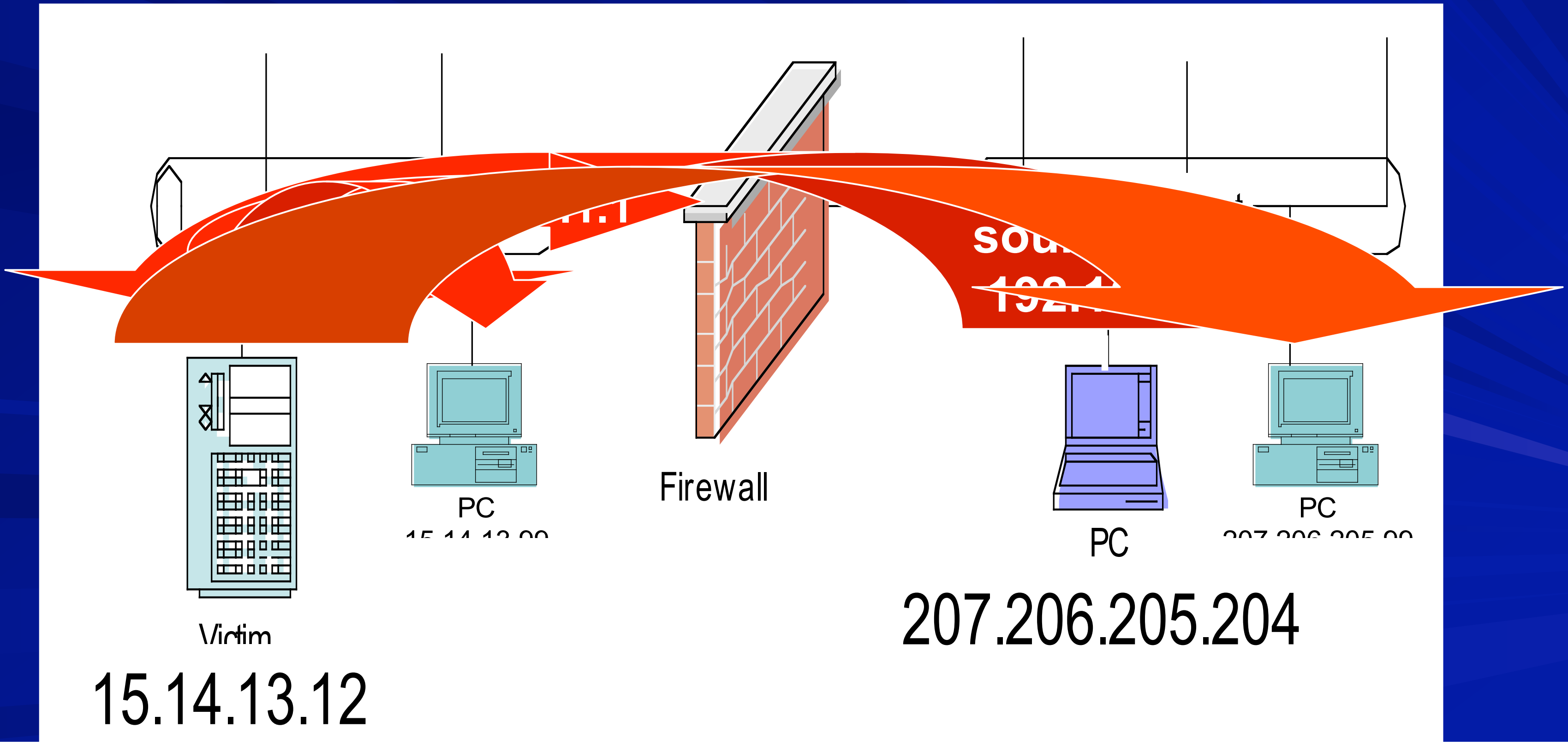
Dynamic ARP Inspection

- Validates against DHCP Snooping binding table (if DHCP Snooping used)
- Can build access lists of MAC and IP pairs for non-DHCP environments or set port to be trusted
- Can limit the rate of ARPs to prevent DoS attacks

Vulnerability

IP Address Spoofing

- Attacker sends packet with spoofed source IP address
- Victim's response packet dies or goes to wrong source (another victim)



Remediation

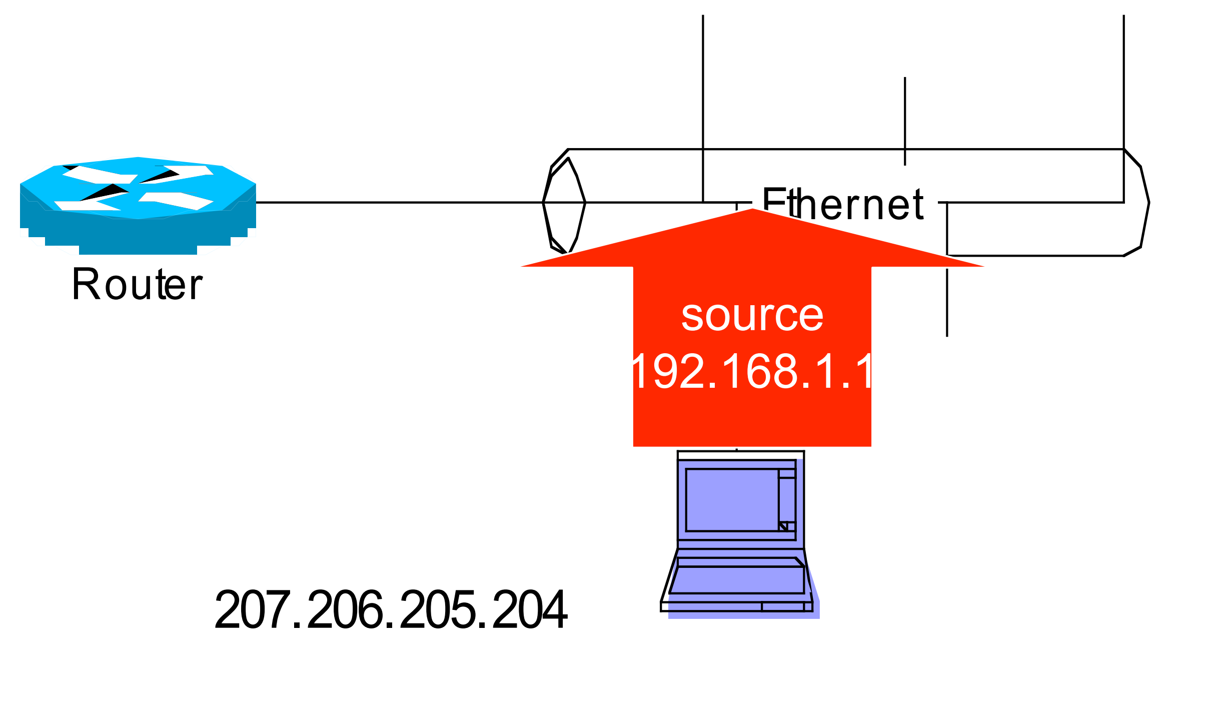
Ingress Access List

- RFC 2827 normally done by router can be done at layer 2 device closer to end device
- Helps protect other devices on subnet
- Source IP address should always be 0.0.0.0 for DHCP request or within subnet (e.g., 207.206.205.x)
  - Vulnerability: Attacker could still use another IP address within that subnet

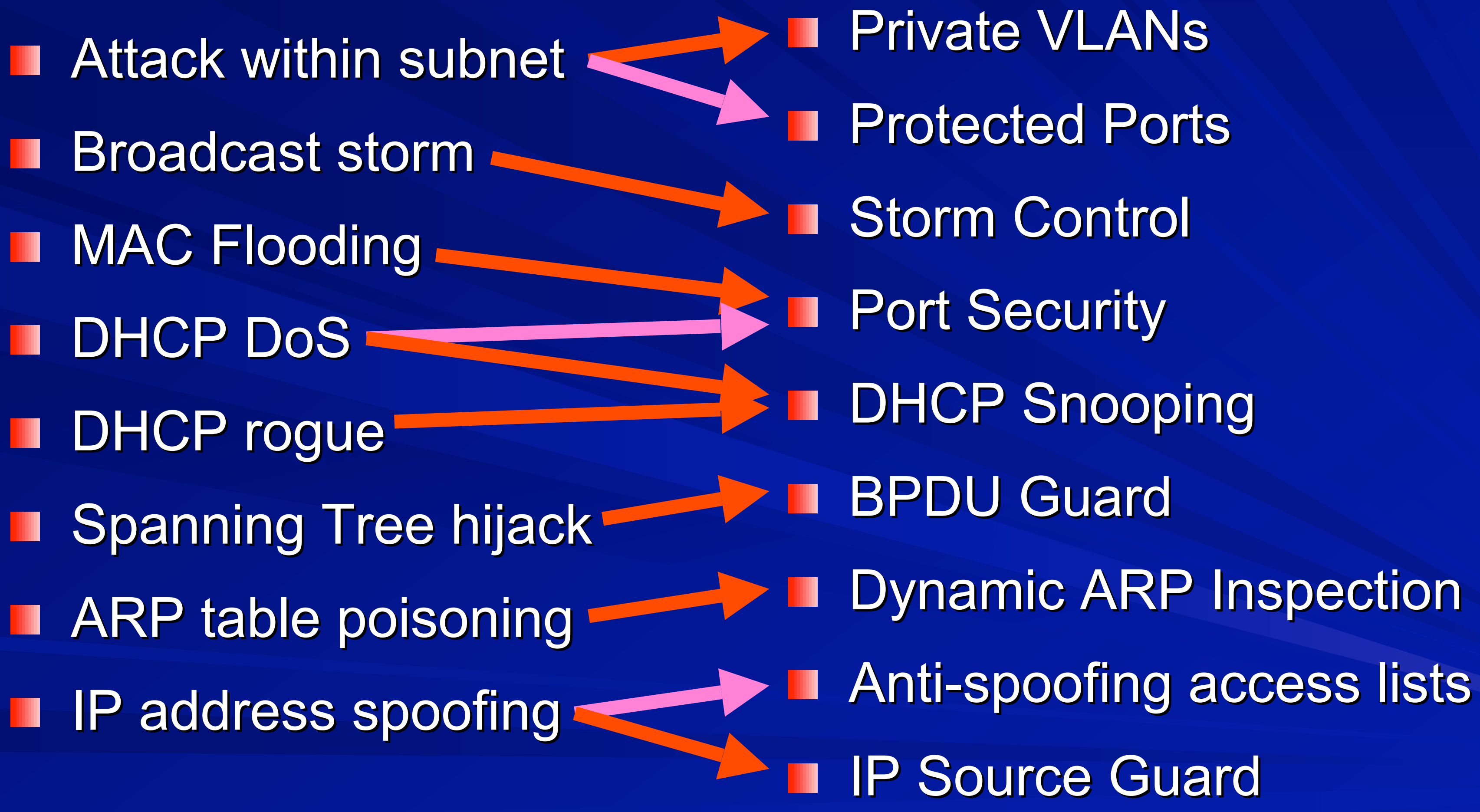
Remediation

IP Source Guard

- Based on DHCP Snooping — source IP address must be the one listed in DHCP Snooping table.
- Can add static mappings for non-DHCP devices
- Can also check MAC address source



Conclusion



- Attack within subnet
- Broadcast storm
- MAC Flooding
- DHCP DoS
- DHCP rogue
- Spanning Tree hijack
- ARP table poisoning
- IP address spoofing

- Private VLANs
- Protected Ports
- Storm Control
- Port Security
- DHCP Snooping
- BPDU Guard
- Dynamic ARP Inspection
- Anti-spoofing access lists
- IP Source Guard

Further Reading

- SAFE Layer 2 Security In-depth Version 2
  http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/sfblu_wp.pdf