Network Security

Securing the Local Area Network

1

Which should be protected?

- Securing the edge device because of its WAN connection?
- Securing the internal LAN?
- Both!
  - Securing the internal LAN is just as important as securing the perimeter of a network.
- Internal LANs consists of:
  - Endpoints
  - Non-endpoint LAN devices
  - LAN infrastructure

Securing Endpoint Devices

- A LAN connects many network endpoint devices that act as a network clients.
- Endpoint devices include:
  - Laptops
  - Desktops
  - IP phones
  - Personal digital assistants (PDAs)
  - Servers
  - Printers

Securing Non-Endpoint Devices

- A LAN also requires many intermediary devices to interconnect endpoint devices.
- Non-endpoint LAN devices:
  - Switches
  - Wireless devices
  - IP telephony devices
  - Storage area networking (SAN) devices

Securing the LAN Infrastructure

- A network must also be able to mitigate specific LAN attacks including:
  - MAC address spoofing attacks
  - STP manipulation attacks
  - MAC address table overflow attacks
  - LAN storm attacks
  - VLAN attacks

IronPort

- IronPort is a leading provider of anti-spam, anti-virus, and anti-spyware appliances.
  - Cisco acquired IronPort Systems in 2007.
- It uses SenderBase, the world's largest threat detection database, to help provide preventive and reactive security measures.

Network Admission Control

NAC

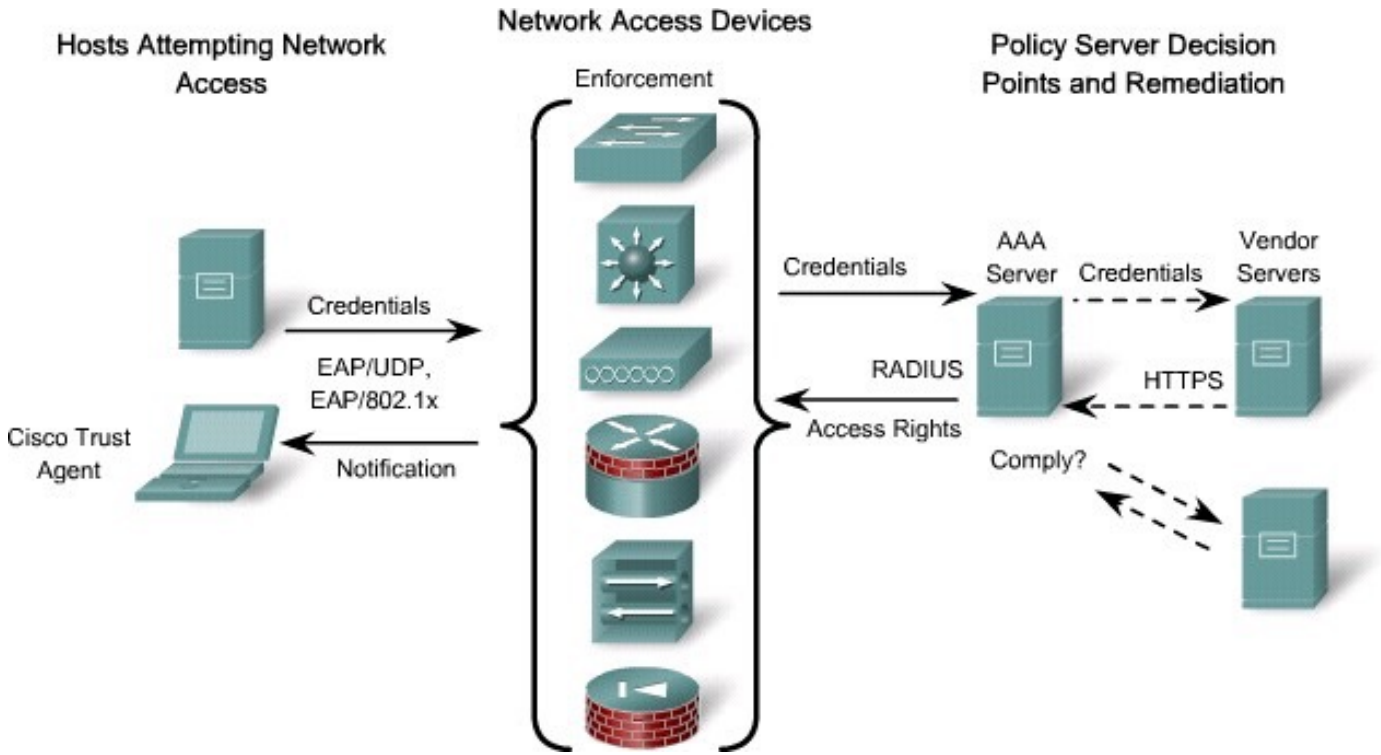
- NAC helps maintain network stability by providing four important features:
  1. Authentication and authorization
  2. Posture assessment
  3. Quarantining of noncompliant systems
  4. Remediation of noncompliant systems
- NAC can be implemented in two ways:
  - NAC Framework
  - Cisco NAC Appliance

NAC Framework

- The NAC framework uses the existing Cisco network infrastructure and third-party software to enforce security policy compliance on all endpoints.
- Suited for high-performance network with diverse endpoints.
  - Requires a consistent LAN, WAN, wireless, extranet, and remote access solution that integrates into the existing security and patch software, tools, and processes.

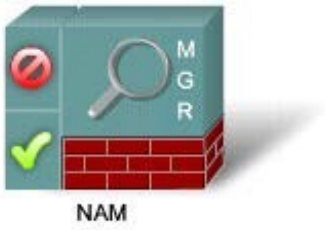
NAC Framework

- Different devices in the network, not necessarily one device, can provide the four features of NAC.



Cisco NAC Appliance

- The Cisco NAC Appliance is a turnkey solution that condenses the four NAC functions into one appliance.
  - Natural fit for medium-scaled networks that need simplified and integrated tracking of operating system and anti-virus patches and vulnerability updates.
  - It does not require a Cisco network.
  - It consolidates all the functions of the NAC framework into a single network appliance fulfilling all of the same roles.
- Several major components accomplish these tasks:



Cisco NAC Components

- **Cisco NAC Appliance Server (NAS)**
  - Device that provides in-band or out-of-band access control.
- **Cisco NAC Appliance Manager (NAM)**
  - A web-based interface for creating security policies and managing online users.
  - The Cisco NAM manages the Cisco NAS, which is the enforcement component of the Cisco NAC Appliance.
- **Cisco NAC Appliance Agent (NAA)**
  - Optional lightweight client for device-based registry scans in unmanaged environments.
  - It can determine whether a device has the required anti-virus dat file, security patch, or critical Windows hotfix.
- **Rule-set updates**
  - Provides scheduled automatic updates for antivirus, critical hotfixes, and other applications.

Layer 2 Security

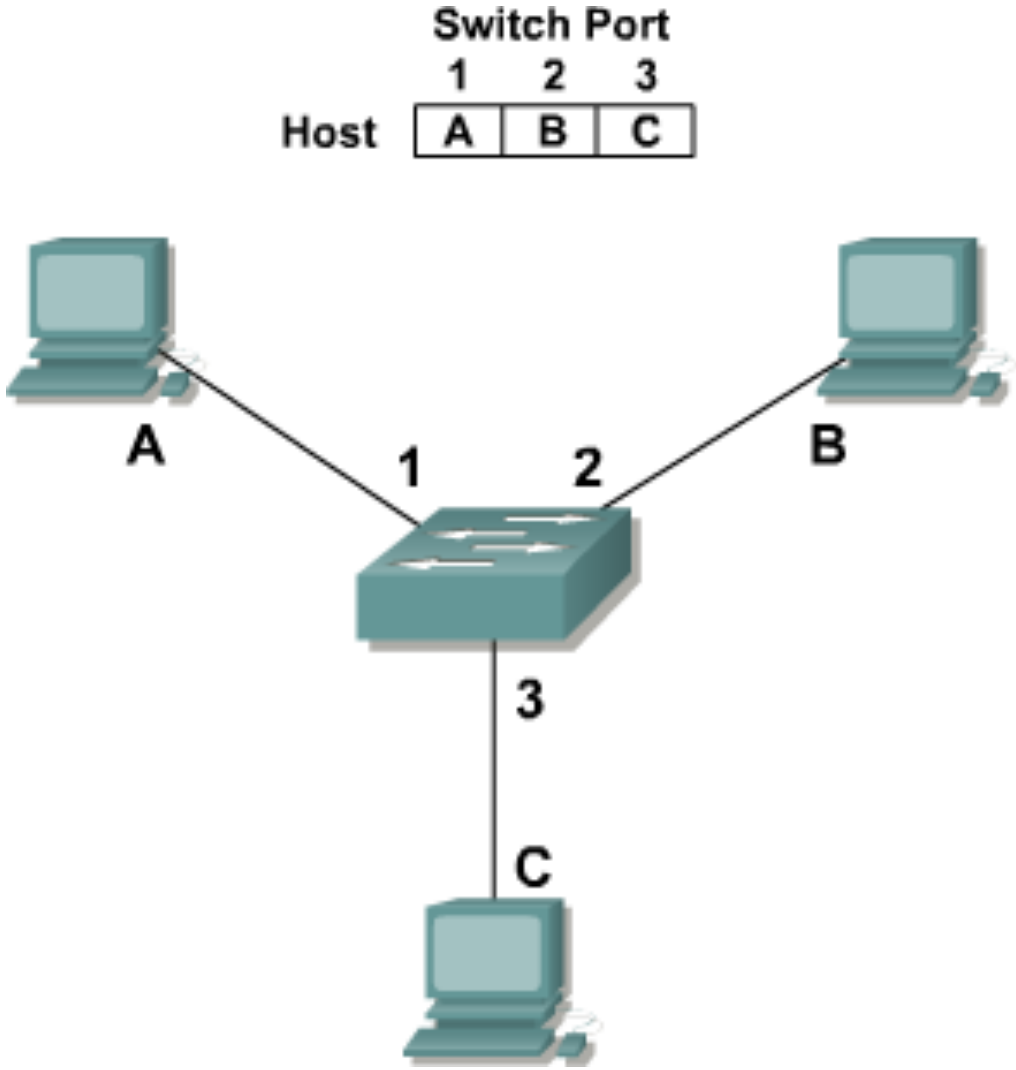
Types of Attacks

- Layer 2 and Layer 3 switches are susceptible to many of the same Layer 3 attacks as routers.
  - Most of the security techniques for routers also apply to switches.
- However, switches also have their own unique network attacks.
- Most of these attacks are from users with internal access to the network.

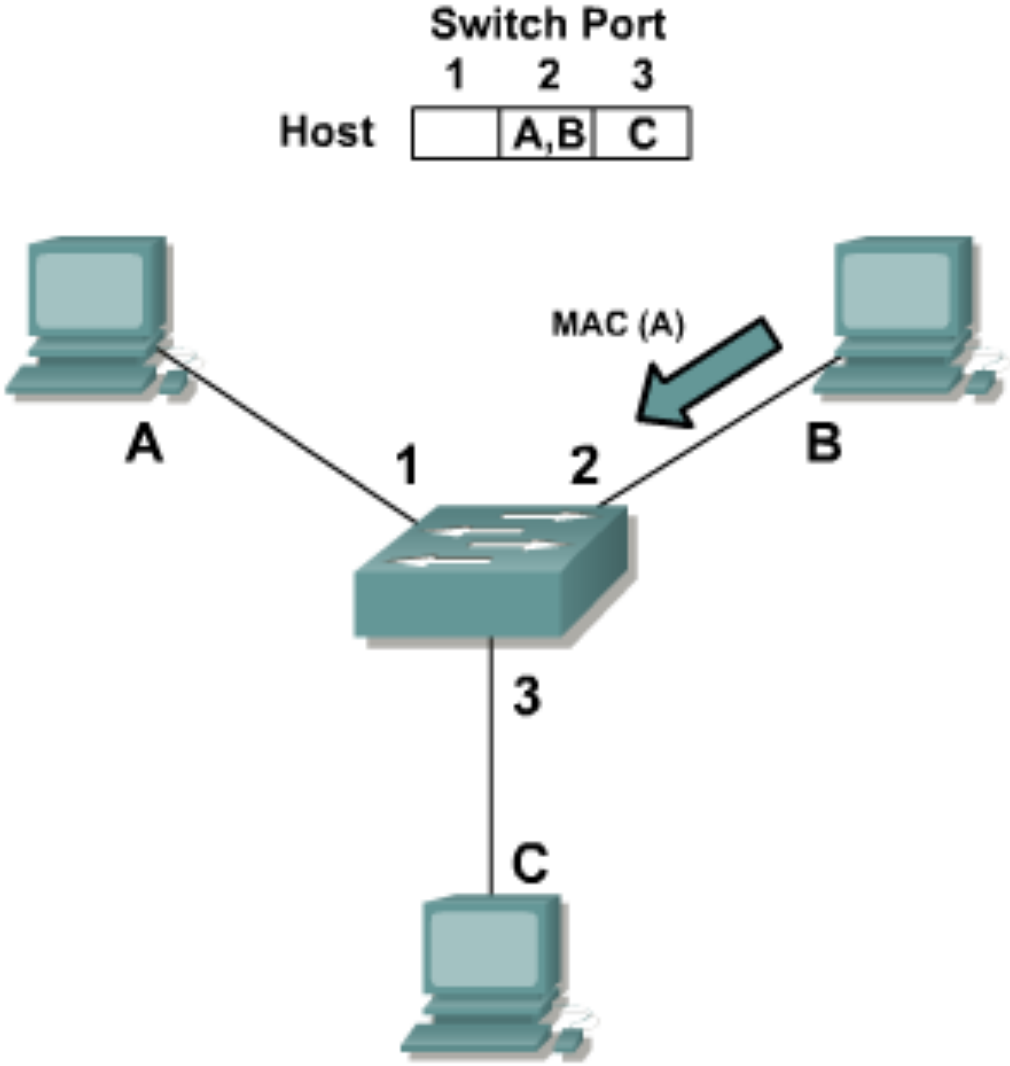
Types of Attacks

- MAC address spoofing
- MAC address table overflows
- STP manipulation
- LAN storms
- VLAN attacks

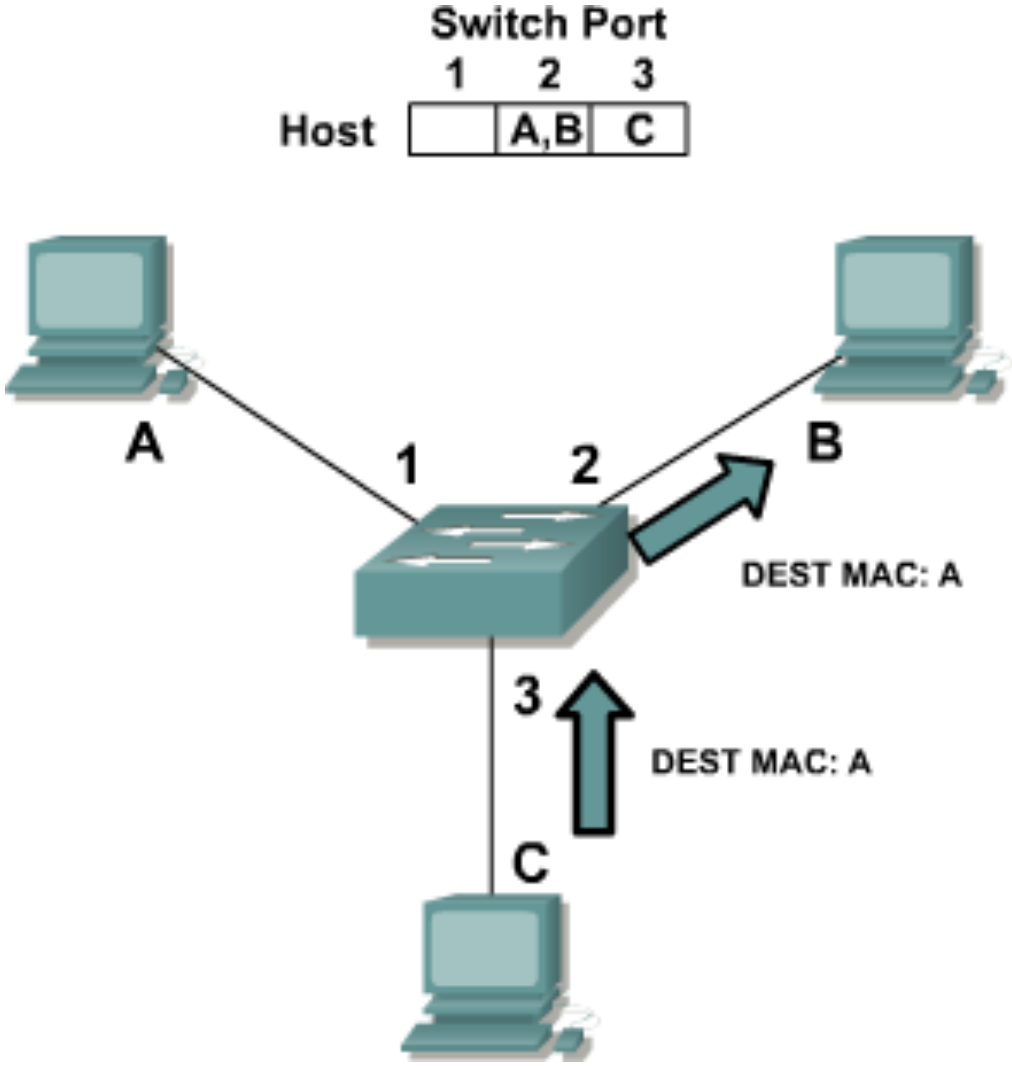
MAC Address Spoofing



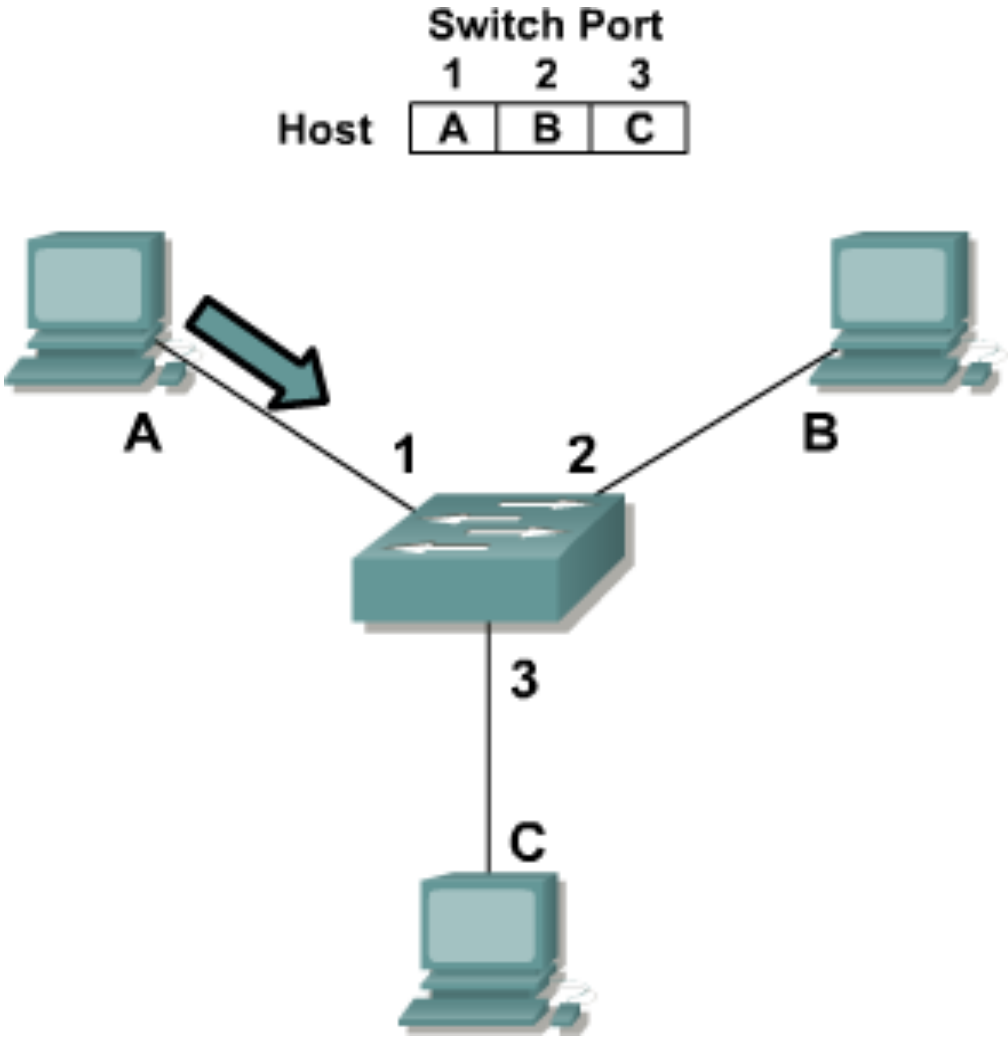
MAC Address Spoofing



MAC Address Spoofing



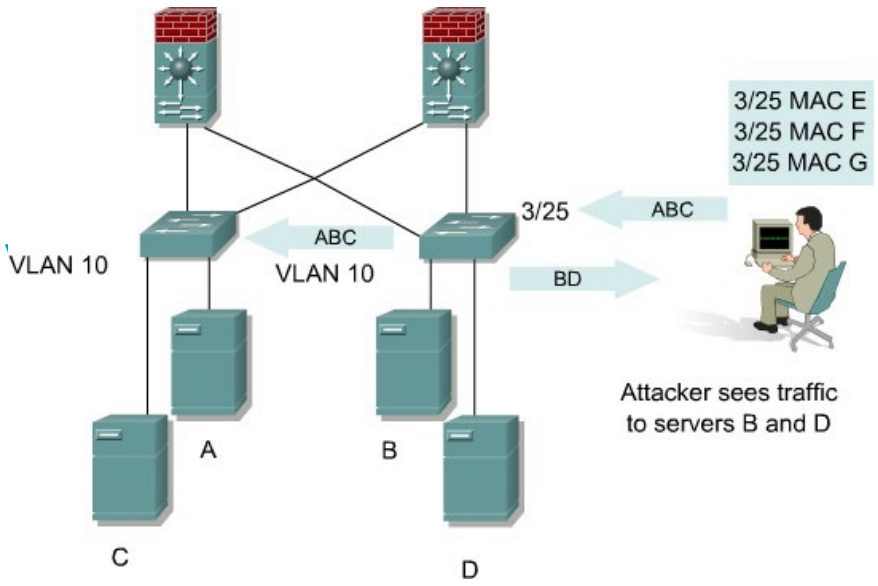
MAC Address Spoofing



Mitigation techniques include configuring port security.

MAC Address Table Overflow Attack

An attacker wishes to sniff packets destined to Servers A and B. To do so, he launch a MAC flood attack.



- Attacker uses macof to generate multiple packets with spoofed source MAC address.
- Over a short period of time, the MAC address table fills and no longer accepts new entries.
  - As long as the attack continues, the MAC address table remains full.
- Switch starts to broadcast (flood) packets all packets that it receives out every port, making it behave like a hub.
- The attacker can now sniff packets destined for the servers.

MAC Address Mitigation Techniques

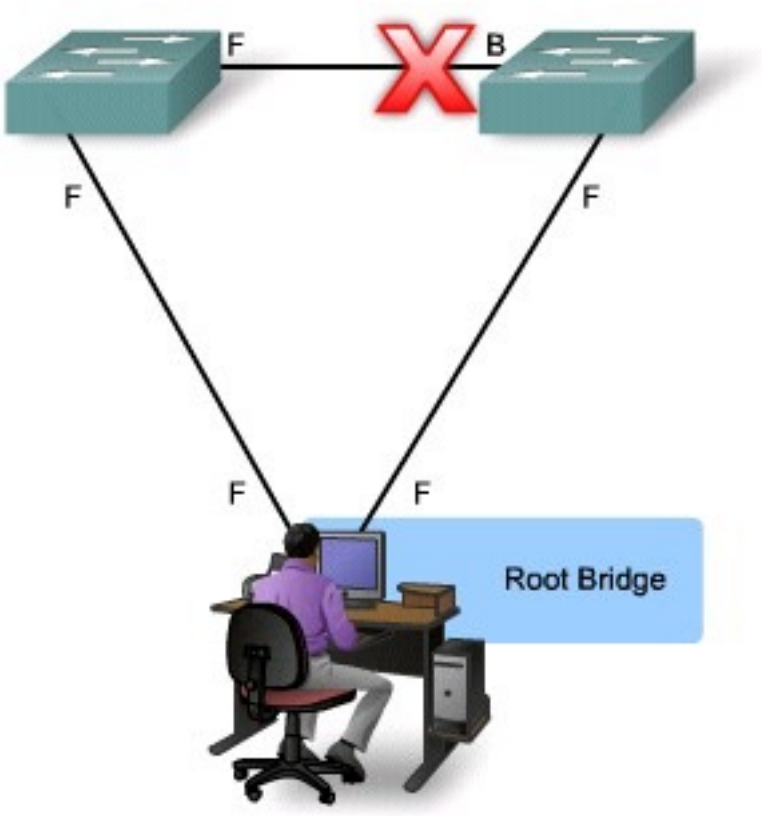
- Both MAC spoofing and MAC address table overflow attacks can be mitigated by configuring port security on the switch.
- Port security can either:
  - Statically specify the MAC addresses on a particular switch port.
  - Allow the switch to dynamically learn a fixed number of MAC addresses for a switch port.
- Statically specifying the MAC addresses is not a manageable solution for a production environment.
  - Allowing the switch to dynamically learn a fixed number of MAC addresses is an administratively scalable solution.

STP Attack

- An STP attack typically involves the creation of a bogus Root bridge.
- This can be accomplished using available software from the Internet such as brconfig or stp-packet.
  - These programs can be used to simulate a bogus switch which can forward STP BPDUs.

Mitigation techniques include enabling PortFast, root guard and BPDU guard.

STP Attack



- The attacking host broadcasts STP configuration and topology change BPDUs to force spanning-tree recalculations.
- The BPDUs sent by the attacking host announce a lower bridge priority in an attempt to be elected as the root bridge.
- If successful, the attacking host becomes the root bridge and sees a variety of frames that otherwise are not accessible.

LAN Storm Attacks

- A LAN storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance.
  - Possible causes:
    - Errors in the protocol stack implementation
    - Mis-configurations
    - Users issuing a DoS attack
- Broadcast storms can also occur on networks.
  - Remember that switches always forward broadcasts out all ports.
  - Some necessary protocols, such as ARP and DHCP use broadcasts; therefore, switches must be able to forward broadcast traffic.

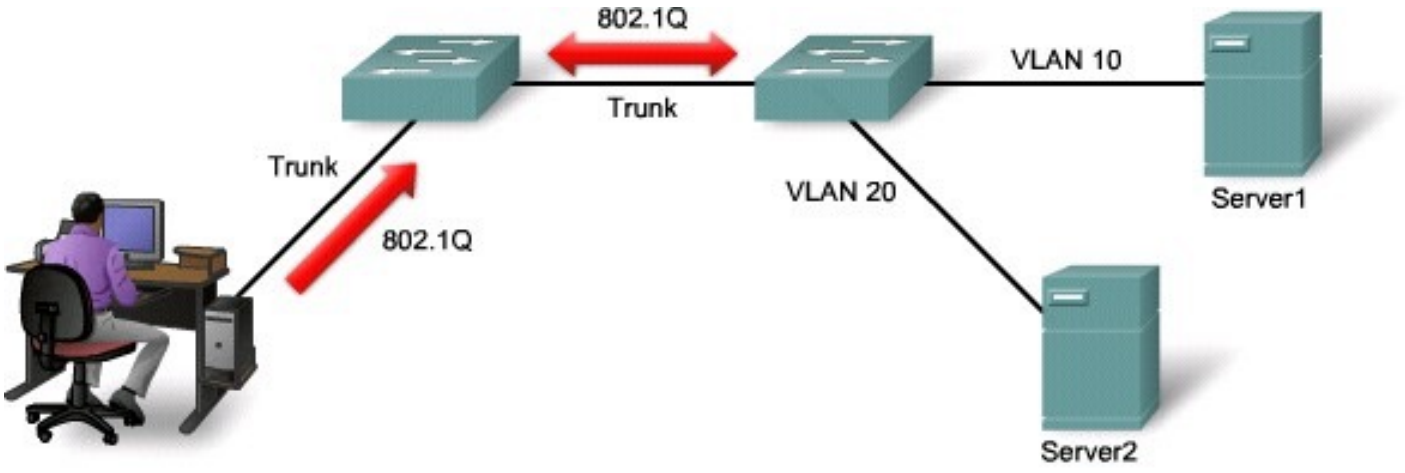
Mitigation techniques include configuring storm control.

VLAN Attacks

- Trunk ports pass traffic for all VLANs using either IEEE 802.1Q or inter-switch link (ISL) VLAN encapsulation.
- A VLAN hopping attack can be launched in one of two ways:
  - Introducing a rogue switch on a network with DTP enabled.
    - DTP enables trunking to access all the VLANs on the target switch.
  - Double-tagging VLAN attack by spoofing DTP messages from the attacking host to cause the switch to enter trunking mode.
    - The attacker can then send traffic tagged with the target VLAN, and the switch then delivers the packets to the destination.

VLAN Hopping Attack - Rogue Switch

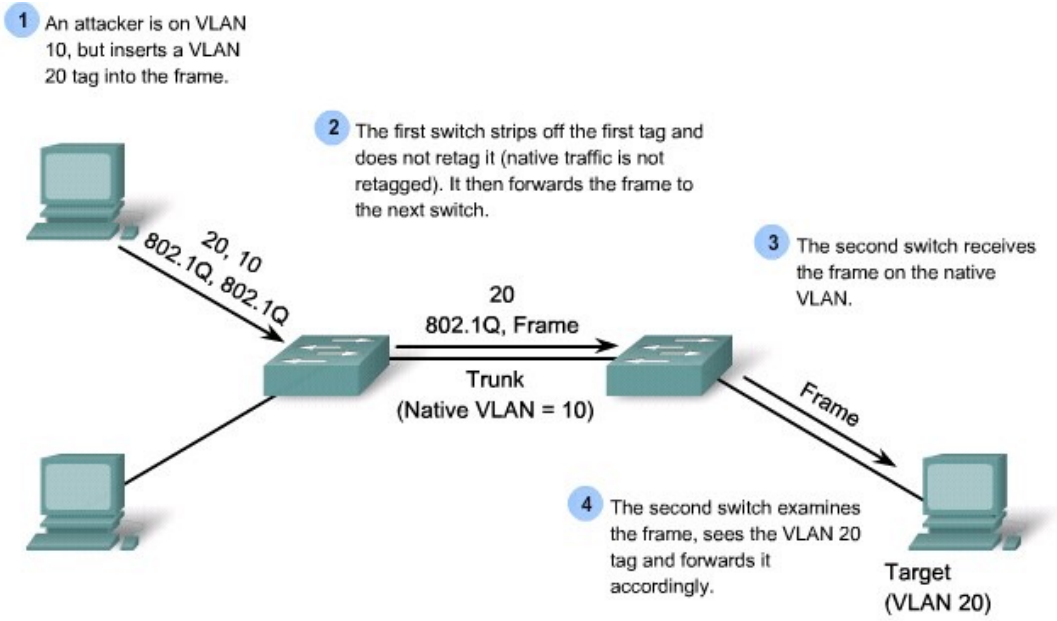
- By default most switches support Dynamic Trunk Protocol (DTP) which automatically try to negotiate trunk links.
  - An attacker could configure a host to spoof a switch and advertise itself as being capable of using either ISL or 802.1q.
  - If successful, the attacking system then becomes a member of all VLANs.



Attacker sees traffic destined for servers.

VLAN Hopping Attack - Double-Tagging

- Involves tagging transmitted frames with two 802.1q headers in order to forward the frames to the wrong VLAN.
  - The first switch strips the first tag off the frame and forwards the frame.
  - The second switch then forwards the packet to the destination based on the VLAN identifier in the second 802.1q header.



Mitigation techniques include ensuring that the native VLAN of the trunk ports is different from the native VLAN of the user ports.

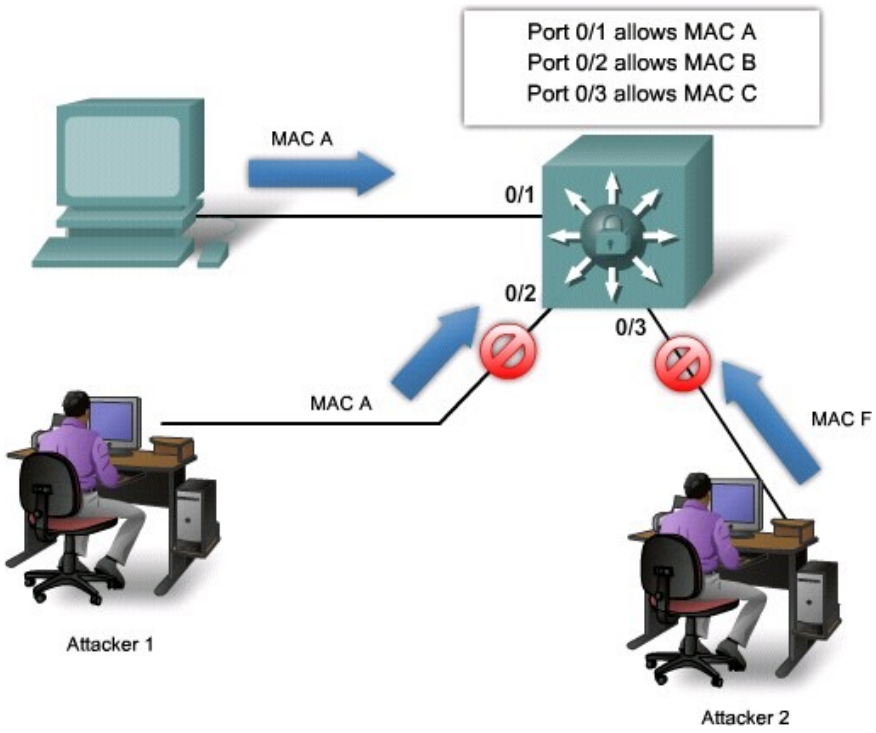
Mitigating VLAN Hopping Attacks

- Use a dedicated native VLAN for all trunk ports.
  - Set the native VLAN on the trunk ports to an unused VLAN.
- Disable trunk negotiation on all ports connecting to workstations.

Mitigating MAC Spoofing and MAC table overflow attacks

Configuring Port Security

- To prevent MAC spoofing and MAC table overflows, enable port security.
- Port Security can be used to statically specify MAC addresses for a port or to permit the switch to dynamically learn a limited number of MAC addresses.
- By limiting the number of permitted MAC addresses on a port to one, port security can be used to control unauthorized expansion of the network.



Port Security

- Once MAC addresses are assigned to a secure port, the port does not forward frames with source MAC addresses outside the group of defined addresses.
- Secure source addresses can be:
  - Manually configured
  - Autoconfigured (learned)

Port Security

- When a MAC address differs from the list of secure addresses, the port either:
  - Shuts down until it is administratively enabled (default mode).
  - Drops incoming frames from the insecure host (restrict option).
- The port behavior depends on how it is configured to respond to a security violation.
- Shutdown is the recommended security violation.

Enable Port Security

- Set the interface to access mode.

```
Switch(config-if)#
switchport mode access
```

- Enable port security on the interface.

```
Switch(config-if)#
switchport port-security
```

Configure Parameters

- Set the maximum number of secure MAC addresses for the interface. (optional)
- The range is 1 to 132. The default is 1.

```
Switch(config-if)#
switchport port-security maximum value
```

- Enter a static secure MAC address for the interface. (optional)

```
Switch(config-if)#
switchport port-security mac-address mac-address
```

- Enable sticky learning on the interface. (optional)

```
Switch(config-if)#
switchport port-security mac-address sticky
```

Port Security Parameters

Parameter	Description
maximum *value*	• (Optional) Set the maximum number of secure MAC addresses for the interface. • The default setting is 1.
mac-address *mac-address*	• (Optional) Specify a secure MAC address by entering a 48-bit MAC address. • Additional secure MAC addresses can be added up to the maximum value.
mac-address sticky [*mac-address*]	• (Optional) Enable the interface for sticky learning. • When enabled, the interface adds all secure MAC addresses that are dynamically learned to the running configuration and converts these addresses to sticky secure MAC addresses.
vlan *vlan-id*	• (Optional) On a trunk port only, specify the VLAN ID and the MAC address. • If no VLAN ID is specified, the native VLAN is used.
vlan access	• (Optional) On an access port only, specify the VLAN as an access VLAN.
vlan voice	• (Optional) On an access port only, specify the VLAN as a voice VLAN. • Note: The **voice** keyword is available only if voice VLAN is configured on a port and if that port is not the access VLAN.

vlan [*vlan-list*]	• (Optional) For trunk ports, you can set the maximum number of secure MAC addresses on a VLAN. If the **vlan** keyword is not entered, the default value is used.
	  • **vlan**: set a per-VLAN maximum value.
	  • **vlan** *vlan-list*: set a per-VLAN maximum value on a range of VLANs separated by a hyphen or a series of VLANs separated by commas.

Establish the Violation Rules

- Set the violation mode. (optional)
- The default is shutdown.
  - **shutdown** is recommended rather than **protect** (dropping frames).
  - The **restrict** option might fail under the load of an attack.

```
Switch(config-if)#
switchport port-security violation {protect | restrict | shutdown}
```

Violation Parameters

Parameter	Description
`protect`	• When the number of secure MAC addresses reaches the limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses or increase the number of maximum allowable addresses. • You are not notified that a security violation has occurred.
`restrict`	• Does the same as protect but also sends an SNMP trap, a syslog message is logged, and the violation counter increments.

`shutdown`	• (Default) A port security violation causes the interface to immediately become error-disabled and turns off the port LED.
	• It also sends an SNMP trap, logs a syslog message, and increments the violation counter.
	• When a secure port is in the error-disabled state, it can be re-enabled by:
	  • Entering the **`errdisable recovery cause psecure-violation`** global configuration command.
	  • Entering the **`shutdown`** and **`no shutdown`** interface configuration commands.

`shutdown vlan`	• In this mode, only the VLAN on which the violation occurred is error-disabled.

Port Aging

- Port security aging can be used to set the aging time for static and dynamic secure addresses on a port.
- Two types of aging are supported per port:
  - **absolute** - The secure addresses on the port are deleted after the specified aging time.
  - **inactivity** - The secure addresses on the port are deleted only if they are inactive for the specified aging time.

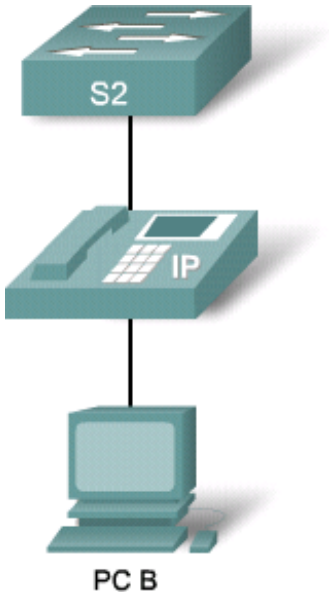
```
Switch(config-if)#
```

switchport port-security aging {static | time *minutes* **| type {absolute | inactivity}}**

Aging Parameters

Parameter	Description
static	• Enable aging for statically configured secure addresses on this port.
time *minutes*	• Specify the aging time for this port. • The range is 0 to 1440 minutes. • If the time is 0, aging is disabled for this port.
type absolute	• Set absolute aging type. • All the secure addresses on this port age out exactly after the time (minutes) specified and are removed from the secure address list.
type inactivity	• Set the inactivity aging type. • The secure addresses on this port age out only if there is no data traffic from the secure source address for the specified time period.

Sample Port Security Configuration




```
S2(config-if)# switchport mode access
S2(config-if)# switchport port-security
S2(config-if)# switchport port-security maximum 2
S2(config-if)# switchport port-security violation shutdown
S2(config-if)# switchport port-security mac-address sticky
S2(config-if)# switchport port-security aging time 120
```

show port-security Command

```
SW2# show port-security
Secure Port     MaxSecureAddr     CurrentAddr     SecurityViolation      Security Action
                  (Count)           (Count)           (Count)
-------------    ---------------------------    ---------------------------------------    ------------------------------
     Fa0/12                 2                0                          0              Shutdown
-----------------------------------------------------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)      : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

```
SW2# show port-security interface f0/12
Port Security               : Enabled
Port status                 : Secure-down
Violation mode              : Shutdown
Maximum MAC Addresses       : 2
Total MAC Addresses         : 1
Configured MAC Addresses    : 0
Aging time                  : 120 mins
Aging type                  : Absolute
SecureStatic address aging : Disabled
Security Violation Count    : 0
```

```
SW2# show port-security address

Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                  Ports    Remaining Age
                                                          (mins)
-----    ---------------       -----                 -------    -----------------
   1    0000.ffff.aaaa    SecureConfigured    Fa0/12        -
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)      : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

MAC Address Notification

- The MAC Address Notification feature sends SNMP traps to the network management station (NMS) whenever a new MAC address is added to or an old address is deleted from the forwarding tables.

```
Switch(config)#
mac address-table notification
```

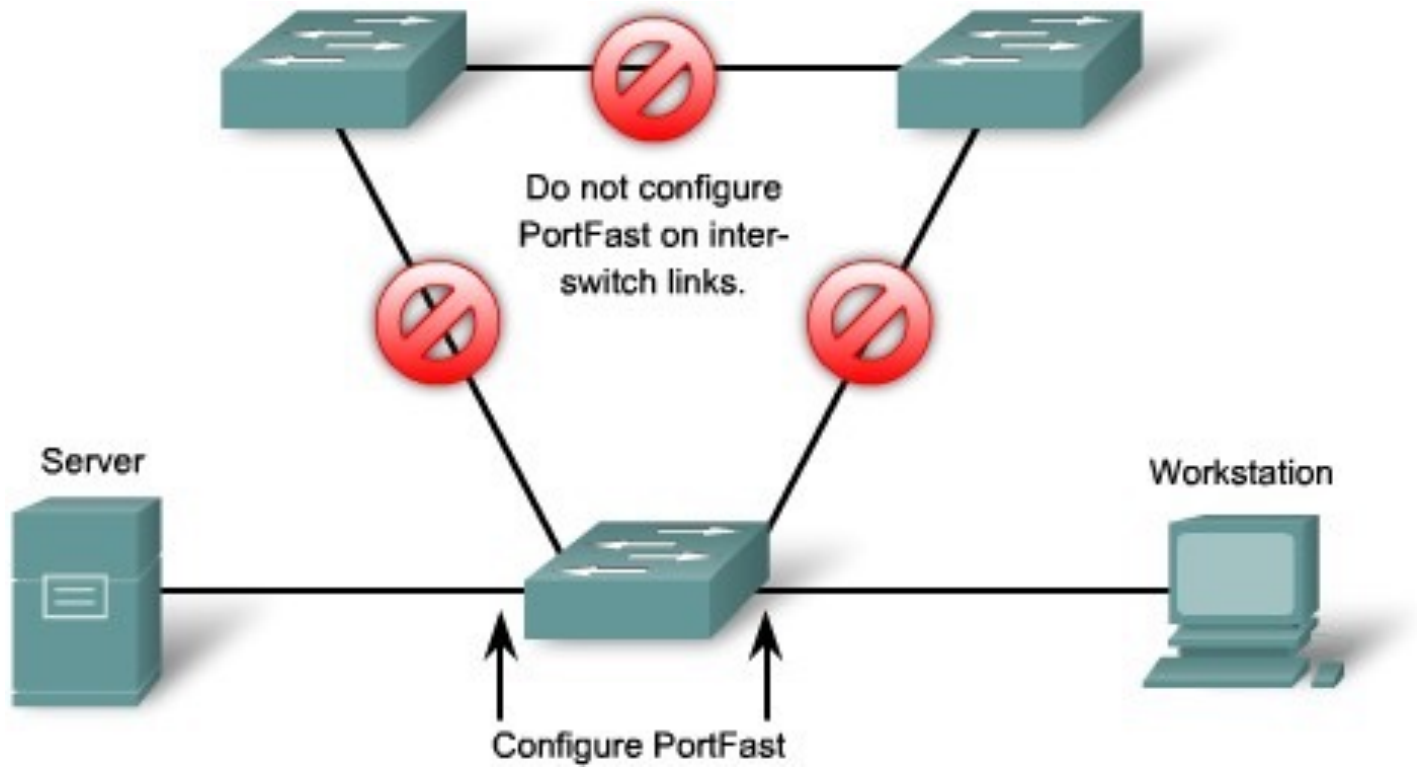
Mitigating STP Manipulation

PortFast

- Causes a Layer 2 interface to transition from the blocking to the forwarding state immediately, bypassing the listening and learning states.
- Used on Layer 2 access ports that connect to a single workstation or server.
  - It allows those devices to connect to the network immediately, instead of waiting for STP to converge.
- Configured using the **`spanning-tree portfast`** command.

PortFast

- It should only be used on access ports!
  - If PortFast is enabled on a port connecting to another switch, there is a risk of creating a spanning-tree loop.



Configure PortFast

- Enable PortFast on a Layer 2 access port and force it to enter the forwarding state immediately.

```
Switch(config-if)#
spanning-tree portfast
```

- Disable PortFast on a Layer 2 access port. PortFast is disabled by default.

```
Switch(config-if)#
no spanning-tree portfast
```

- Globally enable the PortFast feature on all nontrunking ports.

```
Switch(config-if)#
spanning-tree portfast default
```

- Determine if PortFast has been configured on a port.

```
Switch#
show running-config interface type slot/port
```

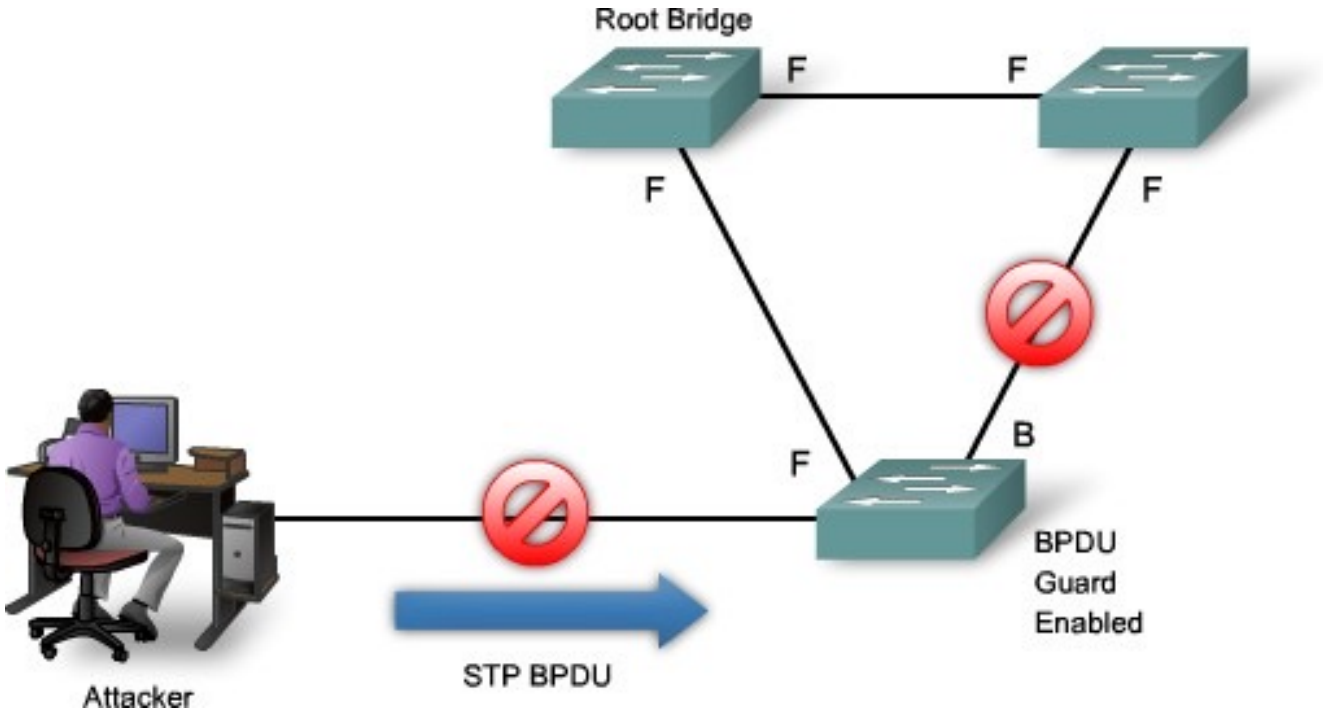
BPDU Guard

- The feature keeps the active network topology predictable.
  - It protects a switched network from receiving BPDUs on ports that should not be receiving them.
  - Received BPDUs might be accidental or part of an attack.
- If a port configured with PortFast and BPDU Guard receives a BPDU, the switch will put the port into the disabled state.
  - BPDU guard is best deployed toward user-facing ports to prevent rogue switch network extensions by an attacking host.

BPDU Guard

- To enable BPDU guard on all PortFast enabled ports, use the global configuration command.

```
Switch(config)#
spanning-tree portfast bpduguard default
```



Display STP State Information

```
SW1# show spanning-tree summary totals
Root bridge for: none.
PortFast BPDU Guard is enabled
UplinkFast is disabled
BackboneFast is disabled
Spanning tree default pathcost method used is short
Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
  1 VLAN                    0         0        0          1          1

<output omitted>
```

BPDU Filtering

- The feature prevents interfaces that are in a PortFast-operational state from sending or receiving BPDUs.
- The interfaces still send a few BPDUs at link-up before the switch begins to filter outbound BPDUs.
- The feature can be configured globally or at the interface level.
  - Globally enable BPDU filtering on a switch so that hosts connected to these interfaces do not receive BPDUs. If a BPDU is received on a PortFast-enabled interface because it is connected to a switch, the interface loses its PortFast-operational status, and BPDU filtering is disabled.
  - At the interface level, the feature prevents the interface from sending or receiving BPDUs. Note that enabling BPDU filtering on an interface is the same as disabling spanning tree on it and can result in spanning-tree loops.

Configuring BPDU Filtering

- To enable BPDU filtering on all PortFast enabled ports, use the global configuration command:

```
Switch(config)#
spanning-tree portfast bpdufilter default
```

- To enable BPDU filtering on an interface, without having to enable PortFast, use the interface configuration command:

```
Switch(config-if)#
spanning-tree bpdufilter enable
```

Verifying BPDU Filtering

```
SW1# show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
EtherChannel misconfiguration guard is enabled
Extended system ID is enabled
Portfast is disabled by default
PortFast BPDU Guard is disabled by default
Portfast BPDU Filter is disabled by default
Loopguard is disabled by default
UplinkFast is enabled
BackboneFast is enabled
Pathcost method used is short


Name Blocking Listening Learning Forwarding STP Active
---------------------------- ------------------- ------------ ----------- -------------- --------------------
VLAN0001 1 0 0 11 12
VLAN0002 3 0 0 1 4
VLAN0004 3 0 0 1 4
VLAN0006 3 0 0 1 4
VLAN0031 3 0 0 1 4
VLAN0032 3 0 0 1 4

<output omitted>
```

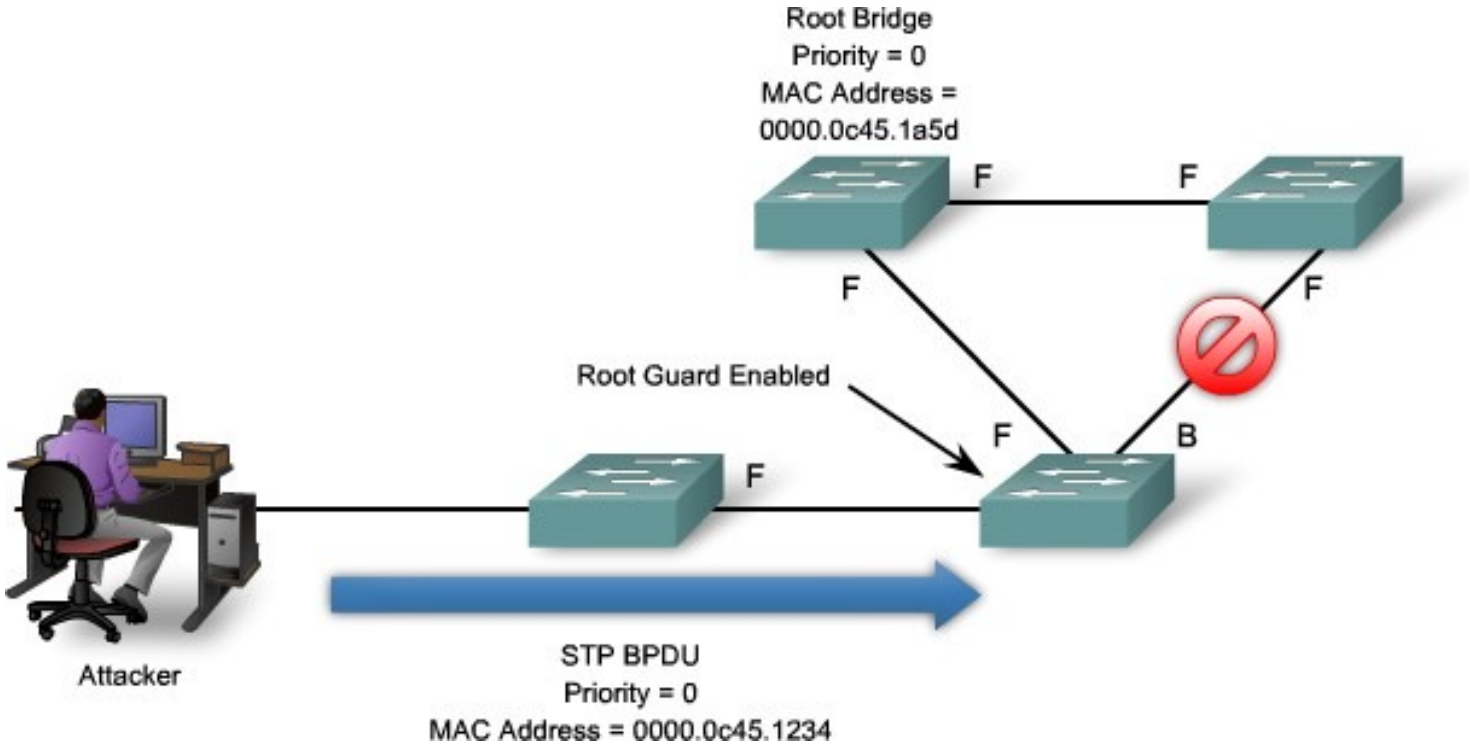
Root Guard

- Root guard enforces the placement of root bridges by limiting the switch ports out of which the root bridge can be negotiated.
- If a root-guard-enabled port receives BPDUs that are superior to those that the current root bridge is sending, that port is moved to a root-inconsistent state.
  - This effectively is equal to an STP listening state, and no data traffic is forwarded across that port.
- If an attacking host sends out spoofed BPDUs in an effort to become the root bridge, the switch, upon receipt of a BPDU, ignores the BPDU and puts the port in a root-inconsistent state.
  - The port recovers as soon as the offending BPDUs cease.

Root Guard

- Root guard is best deployed toward ports that connect to switches that should not be the root bridge using the interface configuration command:

```
Switch(config-if)#
spanning-tree guard root
```



BPDU Guard versus Root Guard

- BPDU guard and root guard are similar, but their impact is different.
- BPDU guard disables the port upon BPDU reception if PortFast is enabled on the port.
  - The administrator must manually re-enable the port that is put into errdisable state or configure an errdisable timeout.
- Root guard allows the device to participate in STP as long as the device does not try to become the root.
  - If root guard blocks the port, subsequent recovery is automatic.
  - Recovery occurs as soon as the offending device ceases to send superior BPDUs.

Verifying Root Guard

- To verify configured ports with root guard, use the **`show spanning-tree inconsistentports`** command.

```
SW1# show spanning-tree inconsistentports
Name                 Interface              Inconsistency
-------------------- ---------------------- ------------------
VLAN0001             FastEthernet3/1        Port Type  Inconsistent
VLAN0001             FastEthernet3/2        Port Type  Inconsistent
VLAN1002             FastEthernet3/1        Port Type  Inconsistent
VLAN1002             FastEthernet3/2        Port Type  Inconsistent
VLAN1003             FastEthernet3/1        Port Type  Inconsistent
VLAN1003             FastEthernet3/2        Port Type  Inconsistent
VLAN1004             FastEthernet3/1        Port Type  Inconsistent
VLAN1004             FastEthernet3/2        Port Type  Inconsistent
VLAN1005             FastEthernet3/1        Port Type  Inconsistent
VLAN1005             FastEthernet3/2        Port Type  Inconsistent

Number of inconsistent ports (segments) in the system :10
```

Configuring Storm Control

Storm Control

- LAN storm attacks can be mitigated by using storm control to monitor predefined suppression-level thresholds.
  - Both a rising threshold and a falling threshold can be set.
- Storm control uses one of these methods to measure traffic activity:
  - Bandwidth as a percentage (%) of the total available bandwidth of the port.
  - Traffic rate in packets/sec or bits/sec at which packets are received.
  - Traffic rate in packets per second and for small frames.

Storm Control

- With each method, the port blocks traffic when the predefined rising threshold is reached.
- The port remains blocked until the traffic rate drops below the falling threshold if one is specified, and then resumes normal forwarding.
- Use the **`storm-control`** interface configuration command to enable storm control and set the threshold value for each type of traffic.

Storm Control

- When the traffic suppression level is specified as a percentage of the total bandwidth, the level can be from 0.00% to 100.00%.
  - A value of 100.00% means that no limit is placed on the specified type of traffic.
  - A value of 0.00% means that all traffic of that type on that port is blocked.
- Threshold percentages are approximations because of hardware limitations and the way in which packets of different sizes are counted.
  - The actual enforced threshold might differ from the configured level by several percentage points.

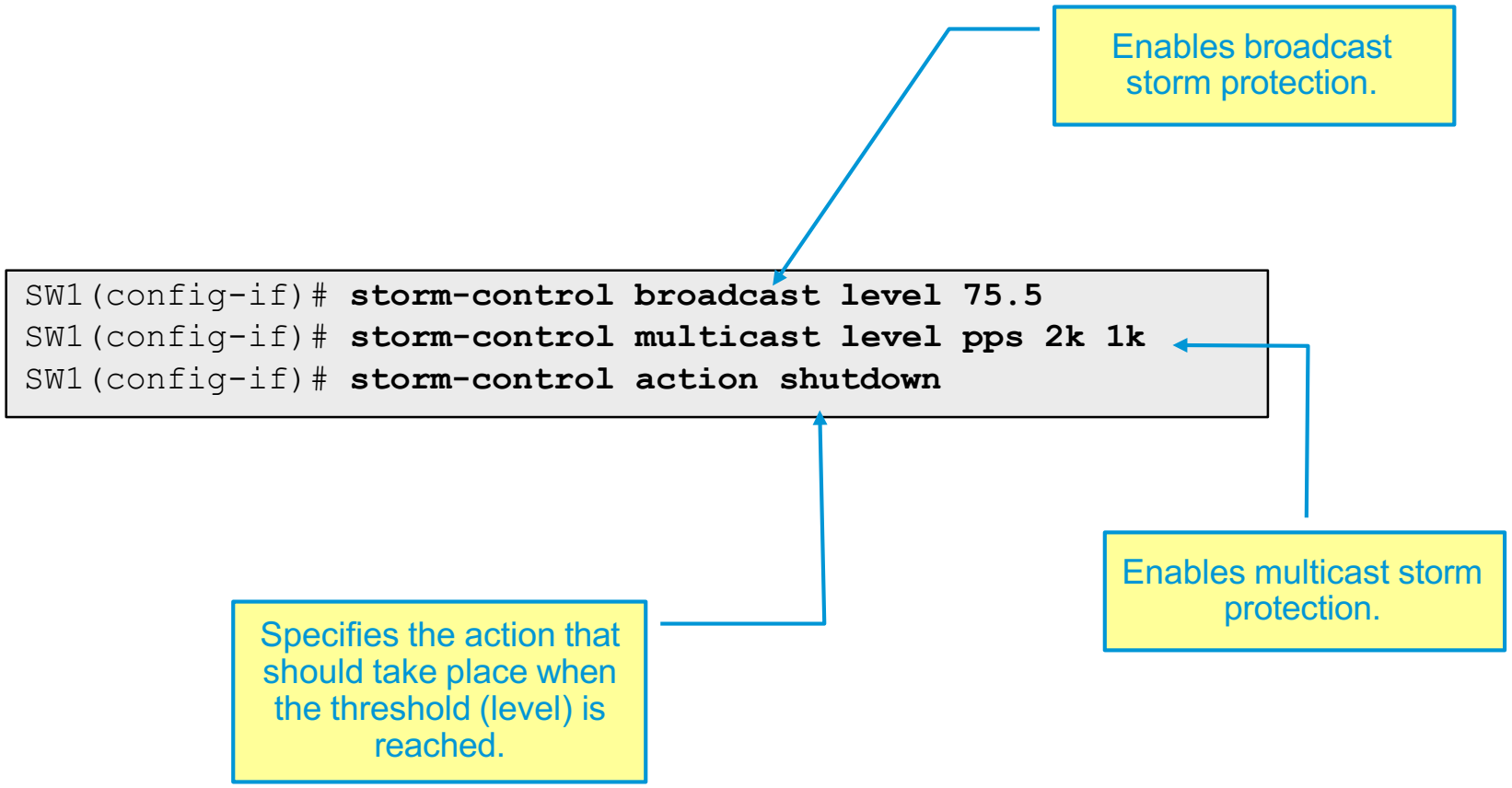
Configure Storm Control

- Storm control is configured using the **storm-control** command.
- If the:
  - **trap** action is configured, the switch sends SNMP log messages when a storm occurs.
  - **shutdown** action is configured, the port is error-disabled during a storm.
    - The **no shutdown** interface configuration command must be used to bring the interface out of this state.

```
Switch(config)#
```

```
storm-control {{broadcast | multicast | unicast} level {level [level-low]
| bps bps [bps-low] | pps pps [pps-low]}} | {action {shutdown | trap}}
```

Storm Control Example



Verify Storm Control

- Use the **`show storm-control [interface] [{broadcast | multicast | unicast | history}]`** command to verify storm control settings.
  - This command displays storm control suppression levels set on all interfaces, or the specified interface, for the specified traffic type.
  - If no traffic type is specified, the default is broadcast traffic.

```
SW1# show storm-control
Interface     Filter State    Upper         Lower       Current
------------  --------------  ------------  ----------  ----------
Gi0/1         Forwarding      20 pps        10 pps      5 pps
Gi0/2         Forwarding      50.00%        40.00%      0.00%

<output omitted>
```

Mitigating VLAN Attacks

Mitigate VLAN Attacks

- To mitigate VLAN hopping attacks, ensure that trunking is only enabled on ports that require trunking.
  - Also be sure to disable DTP (auto trunking) negotiations and manually enable trunking.
- To mitigate double 802.1Q encapsulation VLAN attacks, the switch must look further into the frame to determine whether more than one VLAN tag is attached to it.
  - Use a dedicated native VLAN for all trunk ports.
  - Also disable all unused switch ports and place them in an unused VLAN.

Mitigate VLAN Attacks

- Configure the interface as a trunk link.

```
Switch(config-if)#
switchport mode trunk
```

- Prevent the generation of DTP frames.

```
Switch(config-if)#
switchport nonegotiate
```

- Set the native VLAN on the trunk to an unused VLAN.
  - Note: The default is VLAN 1.

```
Switch(config-if)#
switchport trunk native vlan vlan_number
```

Configuring Port Analyzer

SPAN

- Network traffic passing through ports or VLANs can be analyzed by using switched port analyzer (SPAN) or remote SPAN (RSPAN).
  - SPAN can send a copy of traffic from one port to another port on the same switch where a network analyzer or monitoring device is connected.
  - RSPAN can send a copy of traffic to a port on a different switch.
- SPAN is not required for syslog or SNMP.
  - SPAN is used to mirror traffic, while syslog and SNMP are configured to send data directly to the appropriate server.
  - SPAN does not mitigate attacks, but it does enable monitoring of malicious activity.

SPAN

- SPAN can be used to mirror traffic to another port where a probe or an IDS sensor is connected.
- SPAN is commonly deployed when an IDS is added to a network.
  - IDS devices need to read all packets in one or more VLANs, and SPAN can be used to get the packets to the IDS devices.

SPAN

- A SPAN session can be configured to monitor source port traffic to a destination port.

```
Switch(config)#
monitor session session_number source {interface interface-id [, | -]
[both | rx | tx]} | {vlan vlan-id [, | -] [both | rx | tx]}| {remote vlan
vlan-id}

Switch(config)#
monitor session session_number destination {interface interface-id [, | -
][encapsulation replicate] [ingress {dot1q vlan vlan-id | isl | untagged
vlan vlan-id | vlan vlan-id}]} | {remote vlan vlan-id}
```

Configuring SPAN – Example #1

- In this example, the existing SPAN configuration for session 1 is deleted, and then bidirectional traffic is mirrored from source Gigabit Ethernet port 0/1 to destination Gigabit Ethernet port 0/2, retaining the encapsulation method.

```
SW1(config)# no monitor session 1
SW1(config)# monitor session 1 source interface gigabitethernet0/1
SW1(config)# monitor session 1 destination interface gigabitethernet0/2 encapsulation replicate
```

Configuring SPAN – Example #2

- In this example the switch is configured to:
  - Capture the received traffic on VLAN 10.
  - Capture the transmitted traffic for VLAN 20.
  - Forward the output to interface Fa3/4.

```
SW1(config)# monitor session 1 source vlan 10 rx
SW1(config)# monitor session 1 source vlan 20 tx
SW1(config)# monitor session 1 destination interface FastEthernet 3/4
```

Verifying SPAN

- Use the **`show monitor session`** *`session-number`* command.

```
SW1(config)# show monitor session 1
Session 1
---------------
Type                              : Local Session
Source VLANs                      :
    RX Only                       : 10
    TX Only                       : 20
 Destination Ports                : Fa3/4
    Encapsulation                 : Native
          Ingress                 : Disabled
```

- In this example, all traffic received on VLAN 10 or transmitted from VLAN 20 is forwarded to FastEthernet 3/4.

Private VLAN Edge

PVLAN Edge

- The PVLAN Edge feature, also known as *protected ports*, prevents the forwarding of traffic (unicast, multicast, or broadcast) between protected ports.
- Data traffic cannot be forwarded between protected ports at Layer 2; only control traffic is forwarded because these packets are processed by the CPU and forwarded in software.
- All data traffic passing between protected ports must be forwarded through a Layer 3 device.
- Forwarding behavior between a protected port and a non-protected port proceeds as usual.
- The default is to have no protected ports defined.

Configuring and Verifying PVLAN Edge

- Use the **`switchport protected`** interface mode command to enable the PVLAN Edge feature.
- Verify the configuration with the **`show interfaces`** ***`interface_id`*** **`switchport`** command.

```
SW1# show interfaces gigabitethernet1/0/1 switchport
Name: Gi1/0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
<output omitted>
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL


Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled

<output omitted>
```

Layer 2 Best Practices

Layer 2 Security Best Practices

- Manage switches in secure a manner (SSH, out-of-band management, ACLs, etc.).
- Set all user ports to non-trunking ports (unless you are using Cisco VoIP).
- Use port security where possible for access ports.
- Use CDP only where necessary – with phones it is useful.
- Configure PortFast on all non-trunking ports.
- Configure BPDU guard on all non-trunking ports.
- Configure root guard on STP root ports.

VLAN Security Best Practices

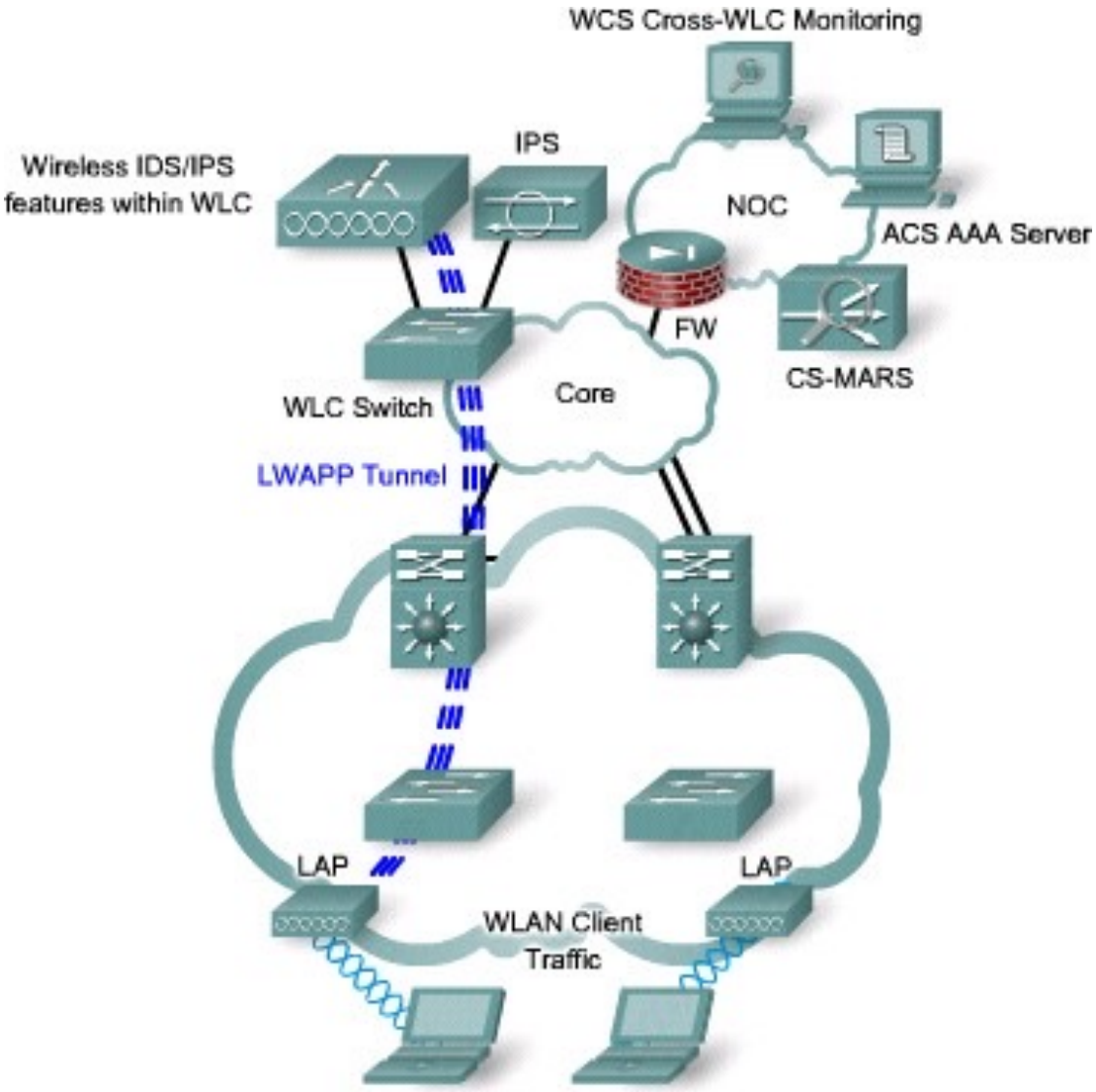
- Disable auto-trunking on user facing ports (DTP off).
- Explicitly configure trunking on infrastructure ports.
- Disable unused ports and put them in an unused VLAN.
- Use distinct VLAN assignments for management, native, user/data, voice, black hole, and private.
- Be paranoid – Do not use VLAN 1 for anything except for Layer 2 protocol control traffic.

Advanced Technology Security Considerations

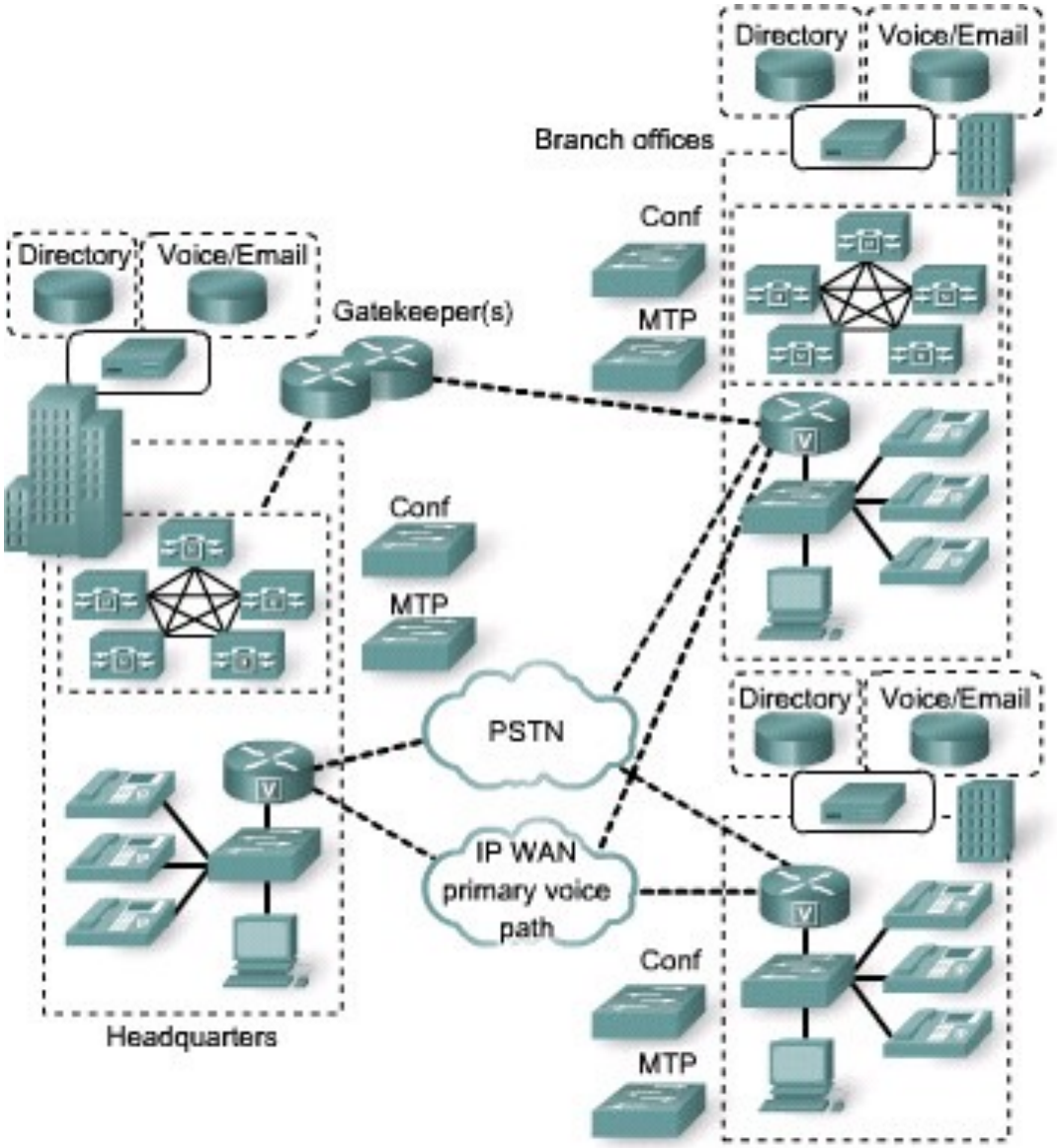
Modern Networks

- Converged networks have increasing challenged modern network design.
- New services to support include:
  - Wireless
  - VoIP
  - SANs

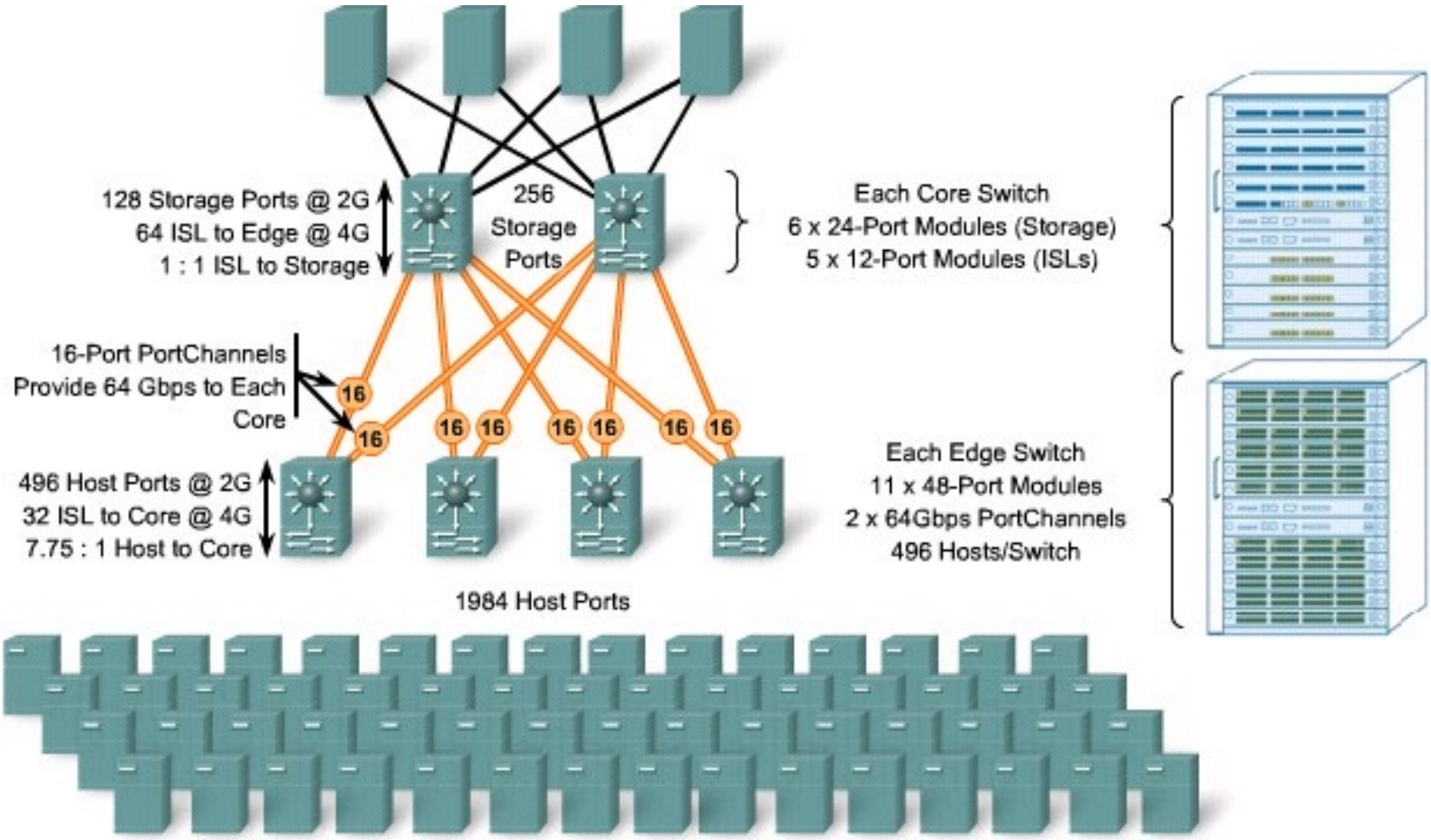
Wireless Networks



VoIP Networks



SAN Networks



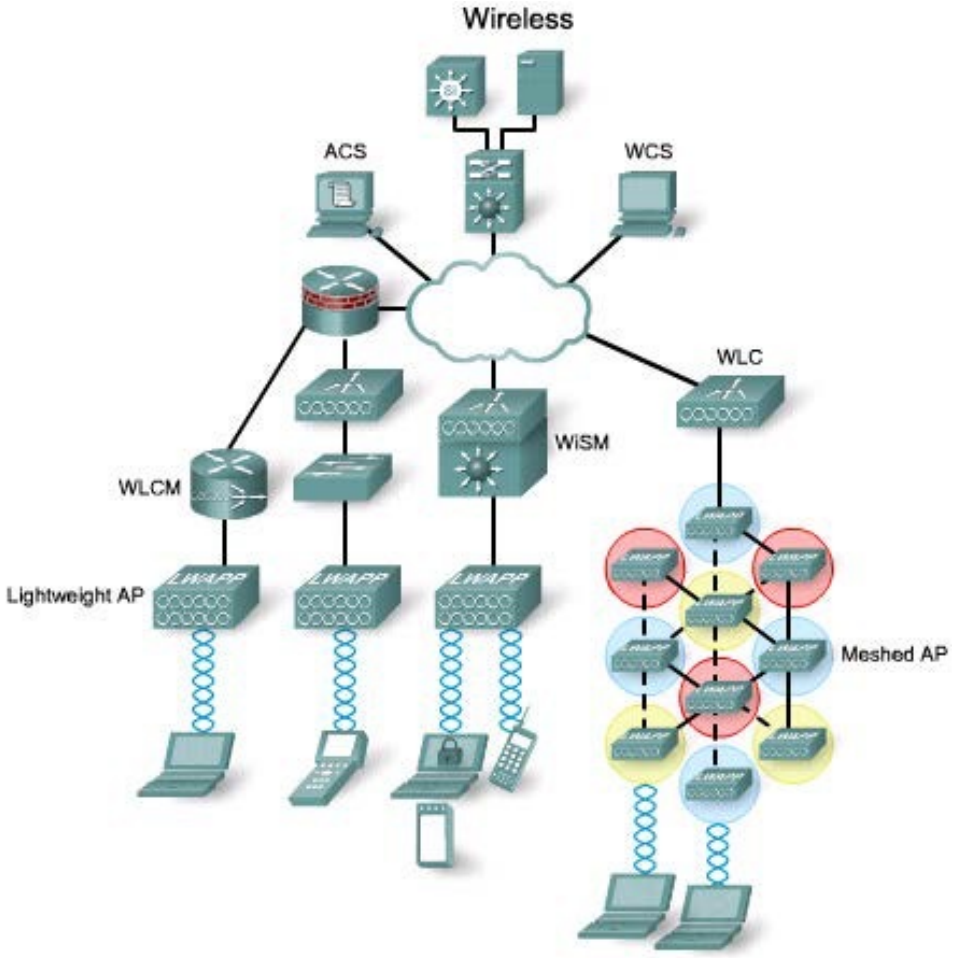
Wireless Networks

Wireless Deployments

- Autonomous
  - Each access point must be individually configured.
- Infrastructure (Lightweight)
  - Modern enterprise wireless now include:
    - Lightweight APs
    - Wireless LAN controllers (WLCs) to manage APs
    - Wireless Control System (WCS) to support wireless applications

Lightweight Wireless

- Lightweight APs depend on wireless LAN controllers (WLCs) for their configurations.
- WLCs are responsible for system-wide wireless LAN functions, such as:
  - Security policies
  - Intrusion prevention
  - RF management
  - QoS
  - Mobility
- Wireless Control System (WCS) are used to help support wireless applications.



Wireless

- An infrastructure-integrated approach has a number of benefits:
  - A single user identity and policy simplifies user management and protects against unauthorized access.
  - Proactive threat and intrusion detection capabilities detect wireless attacks and prevent them.
  - Comprehensive protection safeguards confidential data and communications.
  - Collaboration with wired security systems enables a superset of wireless security functionality and protection.

Wireless Attack Methods

- Wireless attack methods can be broken up into three categories:
  - Reconnaissance
  - Access attack
  - Denial of Service (DoS)

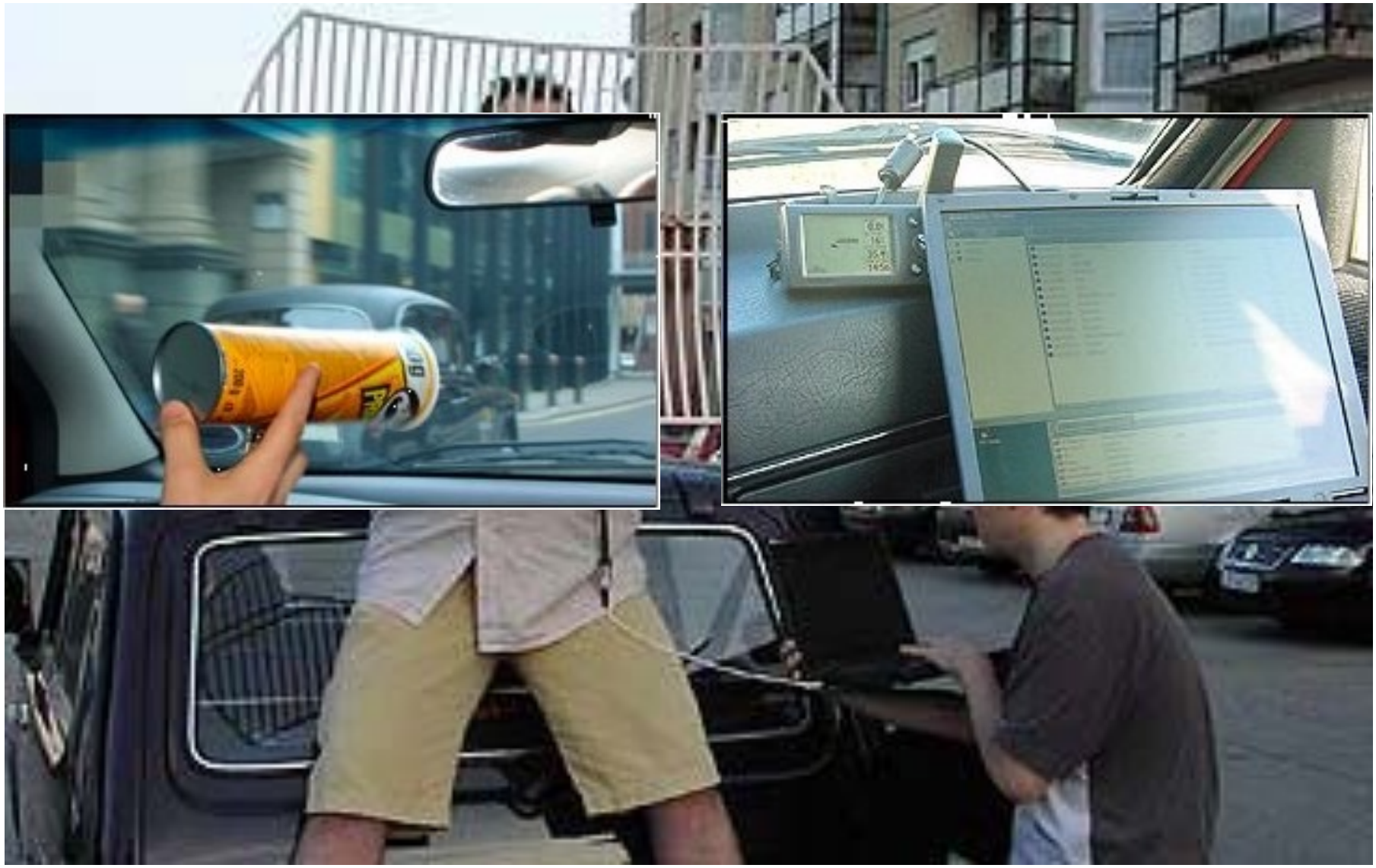
Wireless Hacking Tools

- Network Stumbler software finds wireless networks.
- Kismet software displays wireless networks that do not broadcast their SSIDs.
- AirSnort software sniffs and cracks WEP keys. (If you're still using WEP– you're in big trouble anyway!)
- CoWPAtty cracks WPA-PSK (WPA1).
- ASLEAP gathers authentication data.
- Wireshark can scan wireless Ethernet data and 802.11 SSIDs.

Reconnaissance

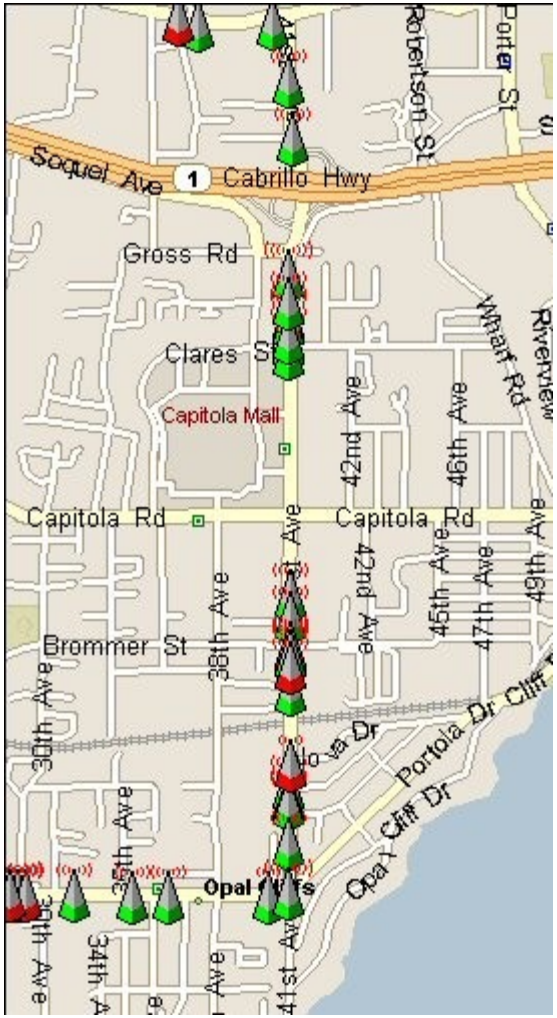
- Reconnaissance is the unauthorized discovery and mapping of systems, services, or vulnerabilities.
  - Also known as information gathering.
  - Not usually illegal, but is illegal in some countries.
  - Similar to a thief scouting a neighborhood for unsecure homes.
  - Usually precedes an actual access or DoS attack.
  - Often called wardriving.

Wardriving



Wardriving

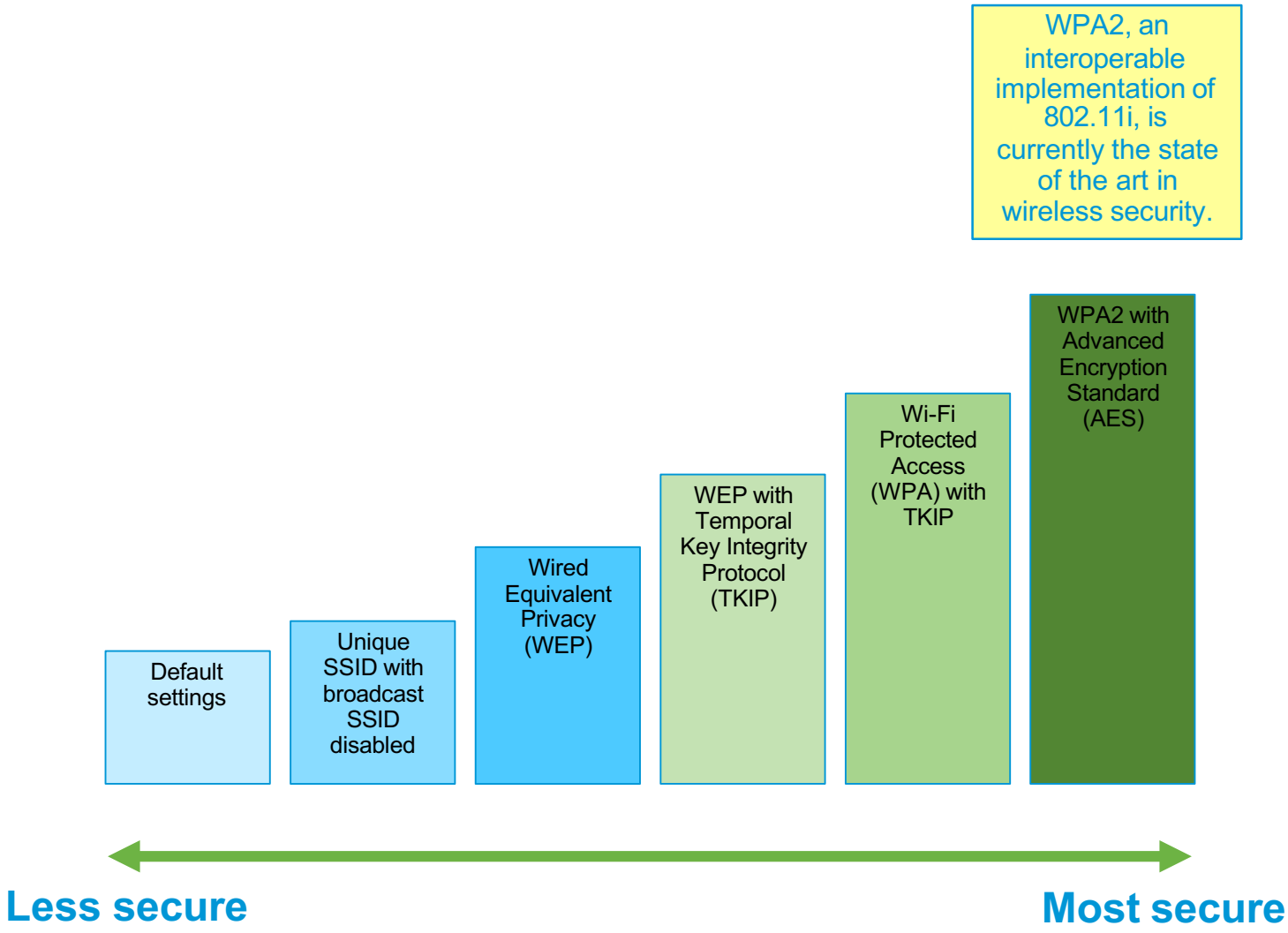
Wardriving Maps



Reconnaissance

- Commercial wireless protocol analyzers like AiroPeek (by WildPackets), AirMagnet, or Sniffer Wireless can be used to eavesdrop on WLANs.
  - Free protocol analyzers like Ethereal or tcpdump fully support wireless eavesdropping under Linux.
- Utilities used to scan for wireless networks can be active or passive.
  - Passive tools, like Kismet, transmit no information while they are detecting wireless networks.

Securing Wireless



Securing Wireless

- Keep several security considerations in mind:
  - Wireless networks using WEP or WPA/TKIP are not very secure and are vulnerable to hacking attacks.
  - Wireless networks using WPA2/AES should have a pass phrase of at least 21 characters.
  - If an IPsec VPN is available, use it on any public wireless LAN.
  - If wireless access is not needed, disable the wireless radio or wireless NIC.
- Deploying a wireless solution should absolutely require WPA2/AES together with authentication handled by a centralized authentication server.

VoIP Networks

VoIP

- The success in data networking has led to its adaptation to voice traffic.
- VoIP has become popular largely because of the cost savings over traditional telephone networks.
  - Traditional telephone networks users pay a flat monthly fee for local telephone calls and a per-minute charge for long-distance calls.
  - VoIP calls are placed using the Internet with users paying a flat monthly fee which is huge for international calls.

VoIP Advantages

- VoIP service providers charge up to 50% less than telecom.
- Feature rich environment can increase productivity.
- Features include Find Me/Follow Me, Remote Office, Click-to-Call, Outlook integration, unified voice mail, conference calling, and collaboration tools.
- Move, add, and change costs are much less.
- Ongoing service and maintenance costs can be lower.
- Many VoIP systems require little or no training for users.
- Mobile phone charges decrease as employees use softphones.
- Telecommuting phone costs are decreased.
- VoIP enables unified messaging.
- Encryption of voice calls is supported.
- Fewer administrative personnel are needed for answering telephones.

VoIP Components

Call Agents

Provides call control for IP phones, Call Admission Control (CAC), bandwidth control and management, and address translation.

Cisco Unified Communications Managers and Cisco Unified Communications Manager Business Edition both function as the call agents.

Multipoint Control Unit (MCU)

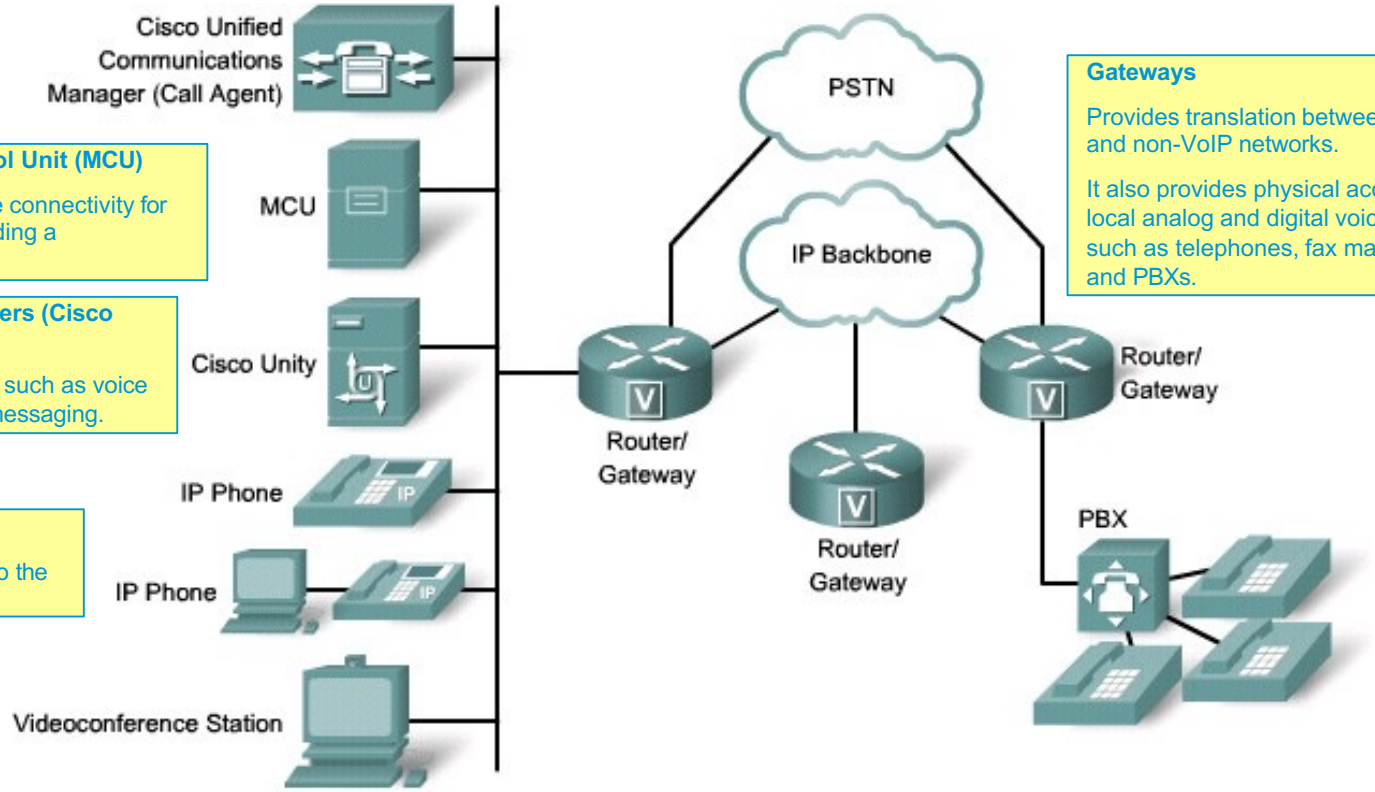
Provides real-time connectivity for participants attending a videoconference.

Application Servers (Cisco Unity)

Provides services such as voice mail and unified messaging.

IP phones

Provide IP voice to the desktop.



Gateways

Provides translation between VoIP and non-VoIP networks.

It also provides physical access for local analog and digital voice devices, such as telephones, fax machines, and PBXs.

Videoconference Station

Provides access for end-user participation in videoconferencing.

The station contains a video capture device for video input and a microphone for audio input.

VoIP Protocols

VoIP Protocol	Description
H.323	ITU standard protocol for interactive conferencing; evolved from H.320 ISDN standard; flexible, complex
MGCP	Emerging IETF standard for PSTN gateway control; thin device control
Megaco/H.248	Joint IETF and ITU standard for gateway control with support for multiple gateway types; evolved from MGCP standard
SIP	IETF protocol for interactive and noninteractive conferencing; simpler but less mature than H.323
RTP	IETF standard media-streaming protocol
RTCP	IETF protocol that provides out-of-band control information for an RTP flow
SRTP	IETF protocol that encrypts RTP traffic as it leaves the voice device
SCCP	Cisco proprietary protocol used between Cisco Unified Communications Manager and Cisco IP phones

VoIP Security Considerations

- VoIP communication occurs over the traditional data network which means that the same attacks can affect voice communication.
- VoIP specific attacks include:
  - Unauthorized access to voice resources
    - Voice systems, user identities, telephone configurations, voice-mail messages (intercept them), voice-mail greeting, Voice ports (shut them down), and voice-routing parameters
  - Compromise network resources (specifically protocol vulnerabilities)
  - Eavesdrop
  - DoS attacks
    - Network resource (bandwidth) overload, host resource starvation, and out-of-bounds attacks (using illegal packet structure and unexpected data)

VoIP Spam = SPIT

- SPIT are high-volumes of unsolicited and unwanted bulk messages broadcast to the enterprise users.
  - Bulk calls are also difficult to trace, they can be used for fraud, unauthorized use, and privacy violations.
  - Up to now, VoIP spam is infrequent, but it has the potential to become a major problem.

Authenticated Transport Layer Security (TLS) stops most SPIT attacks, because endpoints only accept packets from trusted devices.

Vishing (Voice Phishing)

- Uses telephony to glean information, such as account details directly from users.
- For example:
  - Victims receive an phishing email from PayPal asking them to verify their credit card details over the phone.
  - People who call enter their credit card number using the keypad.
  - Once entered, perpetrators steal money from the account of their victims.

Toll Fraud

- Is the theft of long-distance telephone service by unauthorized access to a PSTN trunk (an outside line) on a PBX or voice-mail system.
- Toll fraud is a multibillion-dollar illegal industry, and all organizations are vulnerable.
- Theft can also be defined as the use of the telephony system by both authorized and unauthorized users to access unauthorized numbers, such as premium rate numbers.
- Use Cisco Unified Communications Manager such as dial plan filters, partitions, or Forced Authorization Codes (FACs).

SIP

- SIP is a relatively new, but increasingly popular protocol that offers little inherent security.
- Examples of hacks for SIP include:
  - Registration hijacking, which allows a hacker to intercept incoming calls and reroute them.
  - Message tampering, which allows a hacker to modify data packets traveling between SIP addresses.
  - Session tear-down, which allows a hacker to terminate calls or carry out a VoIP-targeted DoS attack by flooding the system with shutdown requests.

VoIP Security Solutions

- Create a voice VLAN.
- Configure firewalls to inspect voice protocols to ensure that SIP, SCCP, H.323, and MGCP requests conform to voice standards.
- Use IPsec VPNs using either DES or 3DES encryptions.
- On the IP Phones, disable unnecessary services, disable default usernames, allow only signed images to be installed, and support secure management protocols.

SAN Networks

Storage Area Networks (SANs)

- Network and server downtime costs companies large sums of money in business and productivity losses.
  - At the same time, the amount of information to be managed and stored is increasing dramatically every year.
- A SAN is a specialized network that enables fast, reliable access among servers and external storage resources.
  - A storage device is not the exclusive property of any one server.
  - They are shared among all networked servers as peer resources.
- A SAN does not need to be a physically separate network.
  - It can be a dedicated subnet that carries only business-critical I/O traffic such as reading / writing a file from / to a disk, between servers and storage devices.
  - For example, it will not carry general-purpose traffic.

Storage Area Networks (SANs)

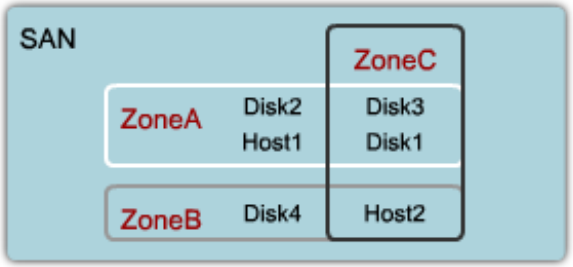
- Cisco SAN solutions provide a preferred means of accessing, managing, and protecting information resources across a variety of SAN transport technologies.
- For example:
  - Fiber Channel
  - Fiber Channel over IP (FCIP)
  - Internet Small Computer Systems Interface (iSCSI)
  - Gigabit Ethernet
  - Optical network

SAN Transport Technologies

- Fiber Channel:
  - The primary SAN transport for host-to-SAN connectivity.
  - Fiber Channel networks provide a serial transport for the SCSI protocol.
  - Uses a world wide name (WWN) to uniquely identify each element.
- iSCSI:
  - Maps SCSI over TCP/IP and is typically used in the LAN.
  - Leverages existing IP networks to build and extend SANs by using TCP/IP to transport SCSI commands, data, and status between hosts or initiators and storage devices or targets, such as storage subsystems and tape devices.
  - Uses a logical unit number (LUN) which is a 64-bit address as a way to differentiate individual disk drives within a common SCSI target device such as a disk array.
- FCIP:
  - Popular SAN-to-SAN connectivity model that is used over the WAN or MAN.
  - SAN designers can use the open-standard FCIP protocol to break the distance barrier of current Fiber Channel solutions and enable interconnection of SAN islands over extended distances.

Fiber Channel Zoning

- Partitioning the Fiber Channel fabric into smaller subsets is called Fiber Channel Zoning.
  - If a SAN contains several storage devices, one device should not necessarily be allowed to interact with all the other devices in the SAN.
- Zoning rules:
  - Zone members see only other members of the zone.
  - Zones can be configured dynamically based on WWN.
  - Devices can be members of more than one zone.



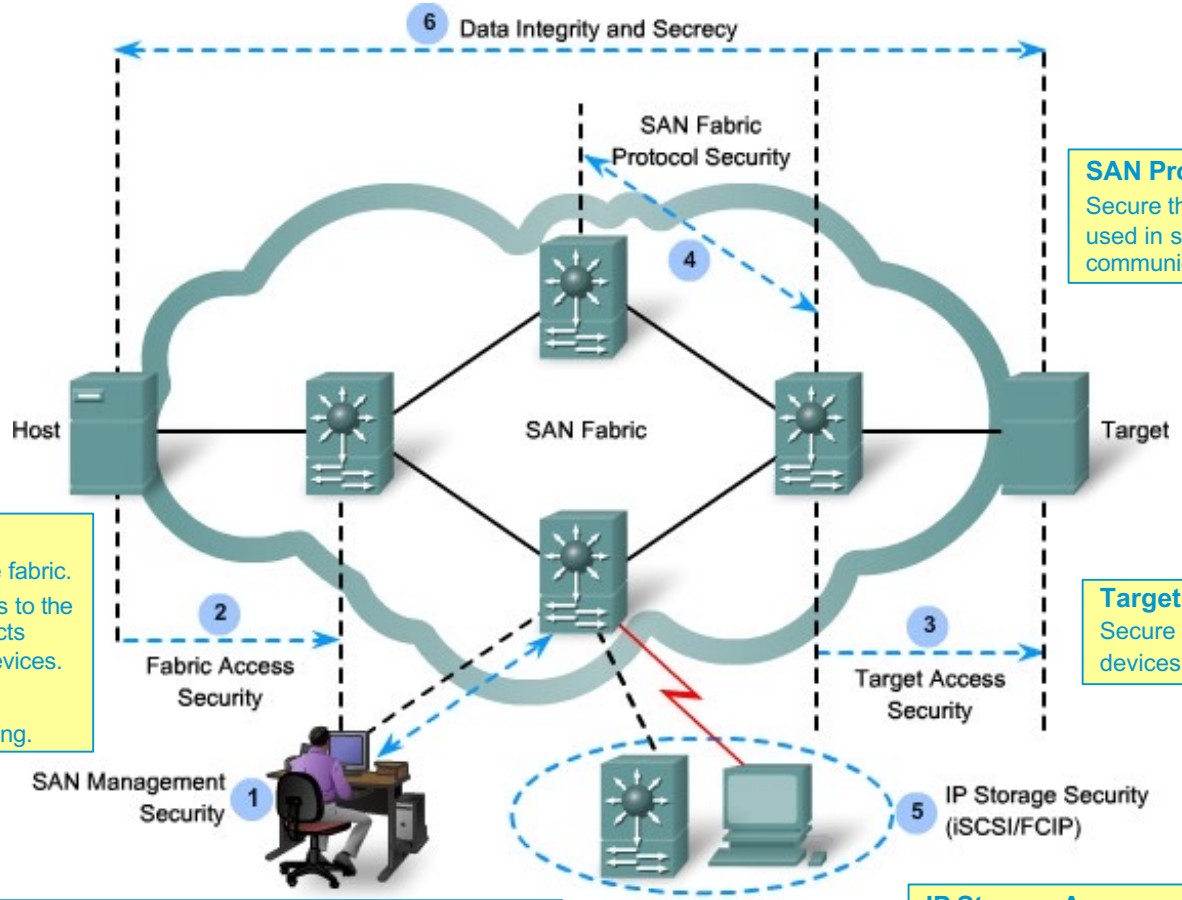
Note that devices can be members of more than 1 zone.

VSANs

- A virtual storage area network (VSAN) is a collection of ports from a set of connected Fiber Channel switches that form a virtual fabric.
  - Originally developed by Cisco but now an ANSI standard.
  - VSANs strongly resemble VLANs.
- VSANs utilize hardware-based isolation, meaning that traffic is explicitly tagged across inter-switch links with VSAN membership information.

Six Critical Areas for SAN Security

Data Integrity and Secrecy:
Encrypt data as it crosses networks as well as when stored on disks.



SAN Protocols:
Secure the protocols that are used in switch-to-switch communication.

Fabric Access:
Secure access to the fabric.
The SAN fabric refers to the hardware that connects servers to storage devices.
Use VSANs and zoning.

Target Access:
Secure access to storage devices (targets).

SAN management:
Secure the management services that are used to administer the SAN.

IP Storage Access:
Secure FCIP and iSCSI.