HARDENING NETWORK DEVICES

By: Ziad Zubidah

CCNP Security

IT Security Officer

National Information Technology Center

NETWORK SECURITY

Network security includes the detection and prevention of unauthorized access to both the network elements and those devices attached to the network. This includes everything from preventing unauthorized switch port access to detecting and preventing unauthorized network traffic from both inside and outside the corporate network.

NETWORK SECURITY ELEMENTS

Network Security Elements include:

- Routers
- Switches
- Firewall
- Intrusion Detection/Prevention Sensors
- Servers

What Exactly needs to be done for these elements to stay secure?

We need to provide Confidentiality, Integrity, Availability

SECURITY CONTROL MODEL

- Total Visibility
- Identify : Classify Users, Services and Traffic
- Monitor : Monitor Performance, Behavior, Events
- Correlate : Collect, Correlate and Analyze System-Wide Events and Generate Reports

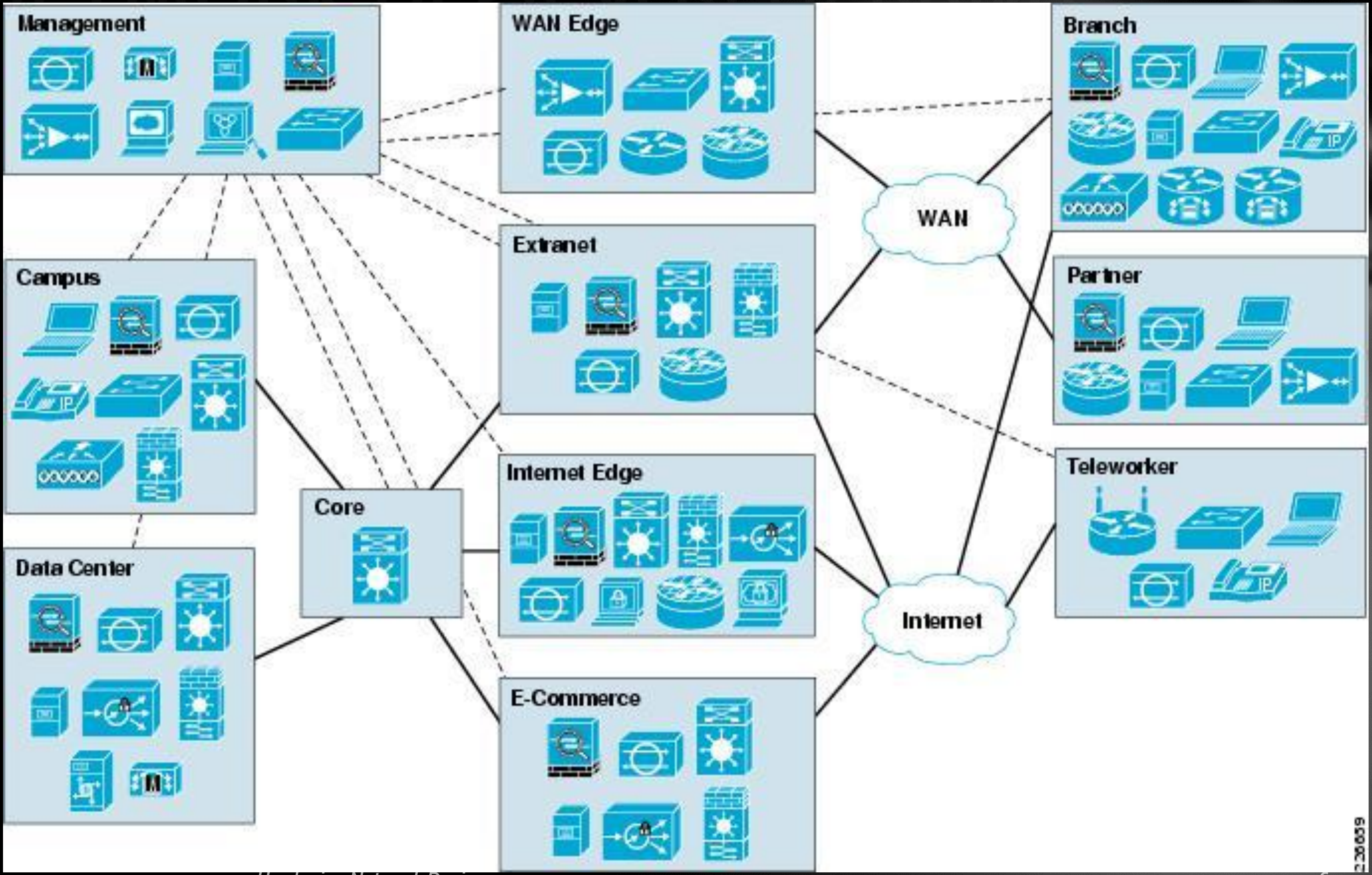
- Complete Control
- Harden : Devices, Services and Applications. Infrastructure Redundancy
- Isolate : Subscribers, Systems and Services
- Enforce : Security Policy, Respond to security incidents

NETWORK DESIGN BLUEPRINT

- Enterprise Core : Central Connectivity for all component parts of the network
- Intranet data center : The data center is where the majority of Critical applications and data are stored.
- Enterprise campus : part of the network that connects to end users that all exist within a similar Geographic area.
- Enterprise Internet edge : connects the company network to the Internet
- Enterprise WAN edge : provides connectivity between Remote sites.
- Enterprise branch : The branch is on the other side of the WAN edge and provides connectivity to remote branch sites.
- Management : provides secure management and communications

  between devices and central management systems.

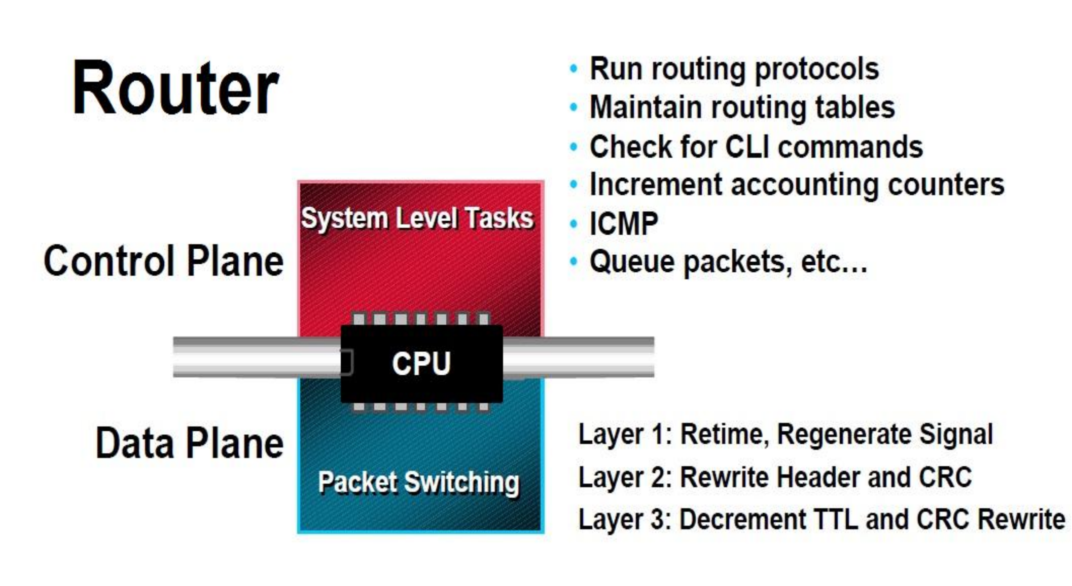
NETWORK DESIGN BLUEPRINT



IOS SOFTWARE PLANES

The functional planes on any IOS Software router or switch

Control plane	provides the capability to route traffic
Data plane	provides the capability to forward traffic
Management plane	provides the capability to manage devices



Router

Control Plane

System Level Tasks

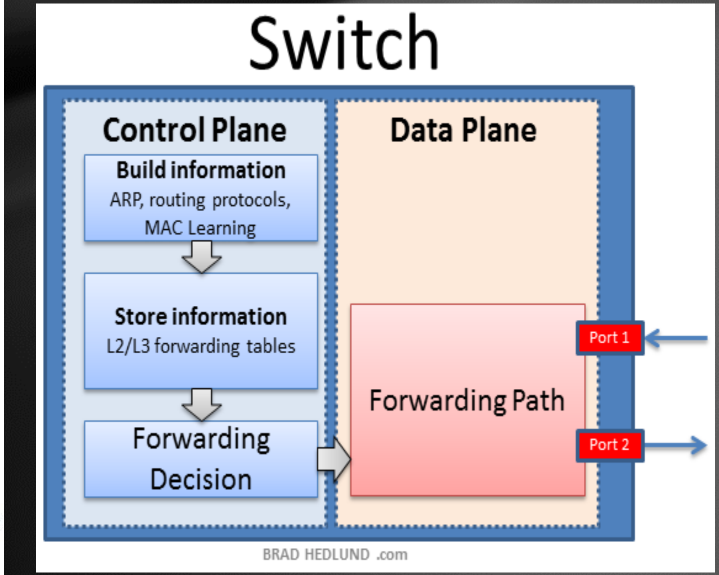
CPU

Data Plane

Packet Switching

- Run routing protocols
- Maintain routing tables
- Check for CLI commands
- Increment accounting counters
- ICMP
- Queue packets, etc…

Layer 1: Retime, Regenerate Signal
Layer 2: Rewrite Header and CRC
Layer 3: Decrement TTL and CRC Rewrite



Switch

Control Plane

Build information
ARP, routing protocols, MAC Learning

Store information
L2/L3 forwarding tables

Forwarding Decision

Data Plane

Forwarding Path

Port 1

Port 2

BRAD HEDLUND .com

SWITCHED DATA PLANE SECURITY SOLUTIONS

The most common types of switched data plane attacks are as follows:

- VLAN hopping
- CAM flooding
- MAC address spoofing
- STP spoofing
- DHCP “starvation”
- DHCP server spoofing
- ARP spoofing
- IP spoofing

VLAN HOPPING ATTACKS

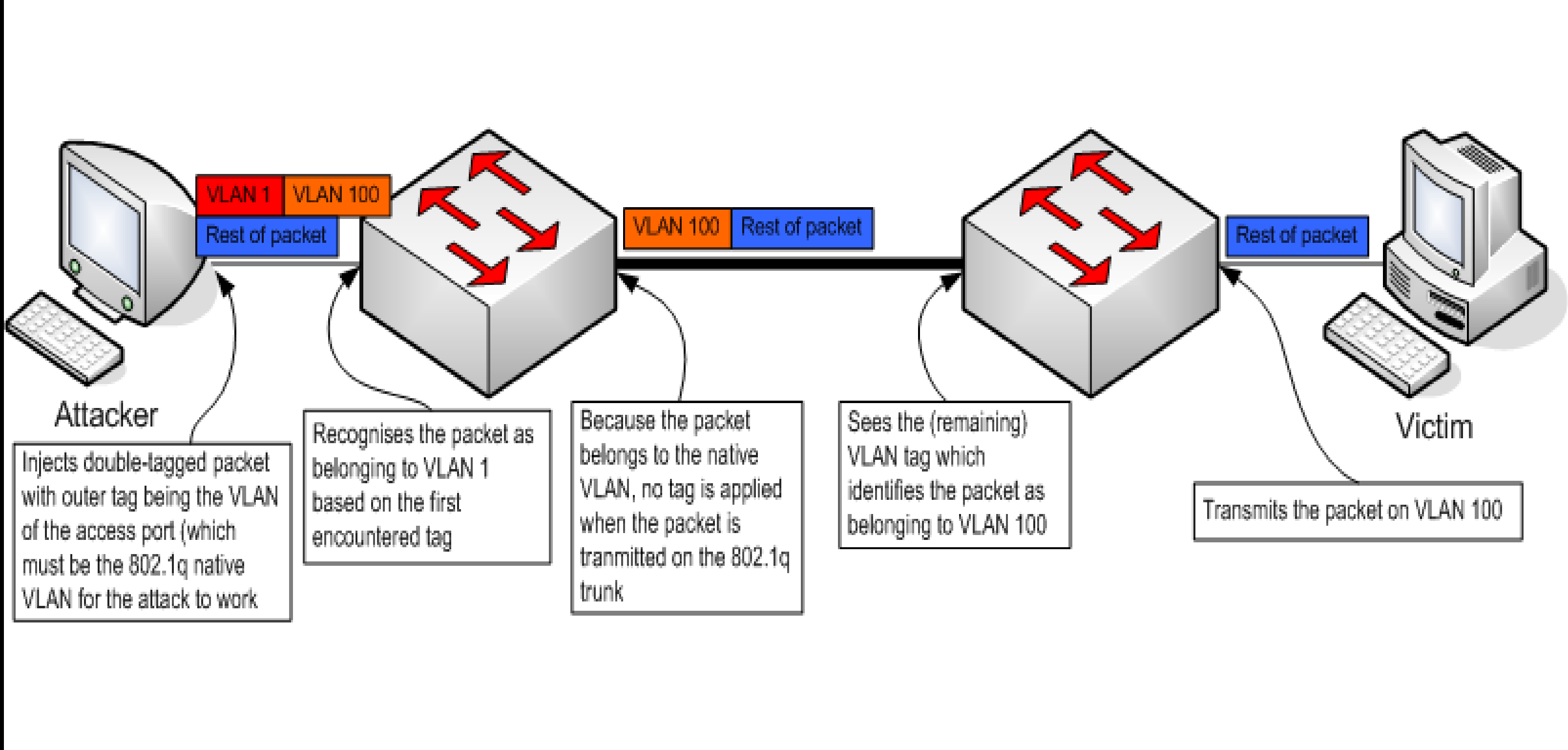
VLAN hopping when packets that are sent from one VLAN can be intercepted or redirected to another VLAN

There are two types of VLAN hopping attacks:

■ **Switch spoofing:** The network attacker configures a device to spoof a switch by emulating either ISL or 802.1Q, and DTP signaling. This makes the attacker device appear to be a switch with a trunk port and therefore a member of all VLANs.

■ **Double tagging:** Another variation of the VLAN hopping attack involves tagging the transmitted frames with two 802.1Q headers, with the outer 802.1Q header matching the configured trunk native VLAN. When the first switch sees that the first tag on the double-tagged frame is equal to that of the native VLAN, it strips this first tag off the frame and then forwards it with the inner 802.1Q tag intact across the trunk. The second switch then forwards the packet based on the VLAN ID in the second 802.1Q header

VLAN HOPPING ATTACKS



Injects double-tagged packet with outer tag being the VLAN of the access port (which must be the 802.1q native VLAN for the attack to work

Recognises the packet as belonging to VLAN 1 based on the first encountered tag

Because the packet belongs to the native VLAN, no tag is applied when the packet is tranmitted on the 802.1q trunk

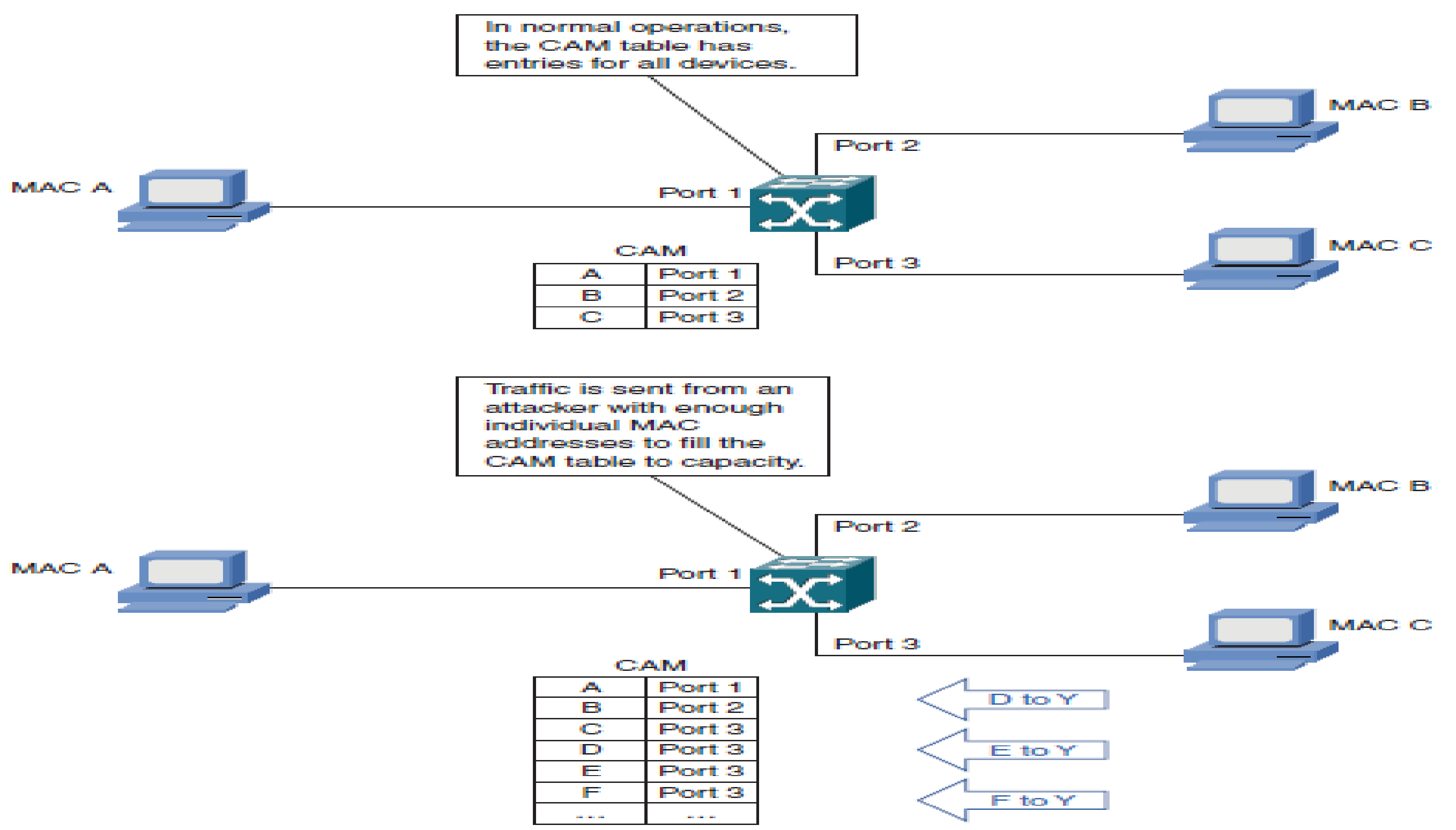
Sees the (remaining) VLAN tag which identifies the packet as belonging to VLAN 100

Transmits the packet on VLAN 100

CAM FLOODING ATTACKS

An attacker sends thousands **of bogus MAC** addresses from one port, which looks, to the switch, like valid hosts' communication. The goal is to flood the switch with traffic that fills the CAM table with false entries. When the CAM table is full, the switch broadcasts traffic without a CAM entry out all its ports; this broadcasting out all ports allows the attacker to see traffic not normally sent to their port. However, this flooding is limited to those ports that are configured into the same VLAN as the source attack port.

CAM FLOODING ATTACKS


In normal operations, the CAM table has entries for all devices.

A	Port 1
B	Port 2
C	Port 3

Traffic is sent from an attacker with enough individual MAC addresses to fill the CAM table to capacity.

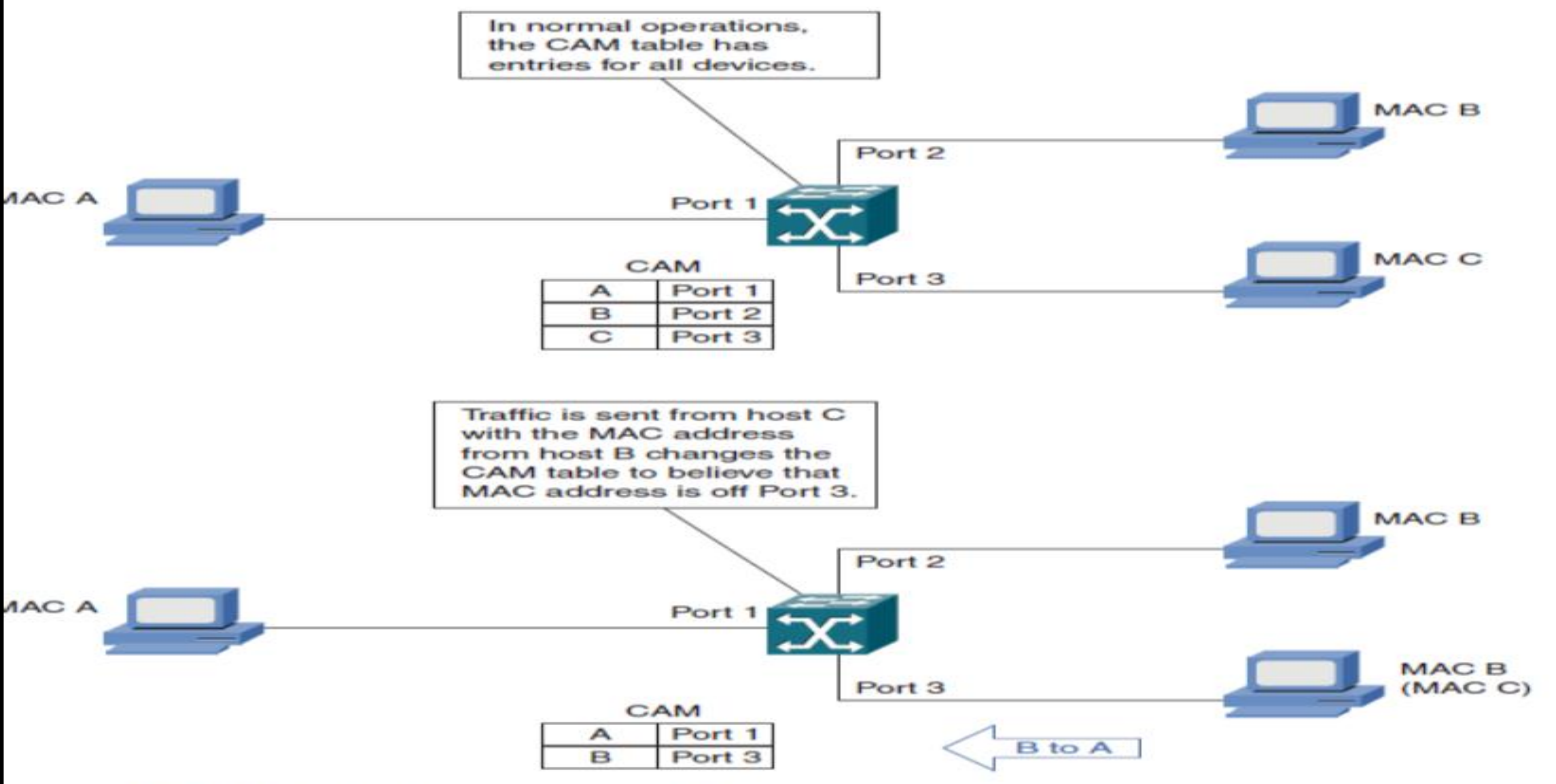
A	Port 1
B	Port 2
C	Port 3
D	Port 3
E	Port 3
F	Port 3
...	...

Figure 4-3 *CAM Flooding Attack*

MAC ADDRESS SPOOFING

MAC address spoofing involves the use of a known MAC address of another host that is authorized to access the network. The attacker attempts to make the target switch forward frames destined for the actual host to be forwarded to the attacker device instead.

MAC ADDRESS SPOOFING



In normal operations, the CAM table has entries for all devices.

CAM

A	Port 1
B	Port 2
C	Port 3

Traffic is sent from host C with the MAC address from host B changes the CAM table to believe that MAC address is off Port 3.

CAM

A	Port 1
B	Port 3

igure 4-4 *MAC Address Spoofing Attack*

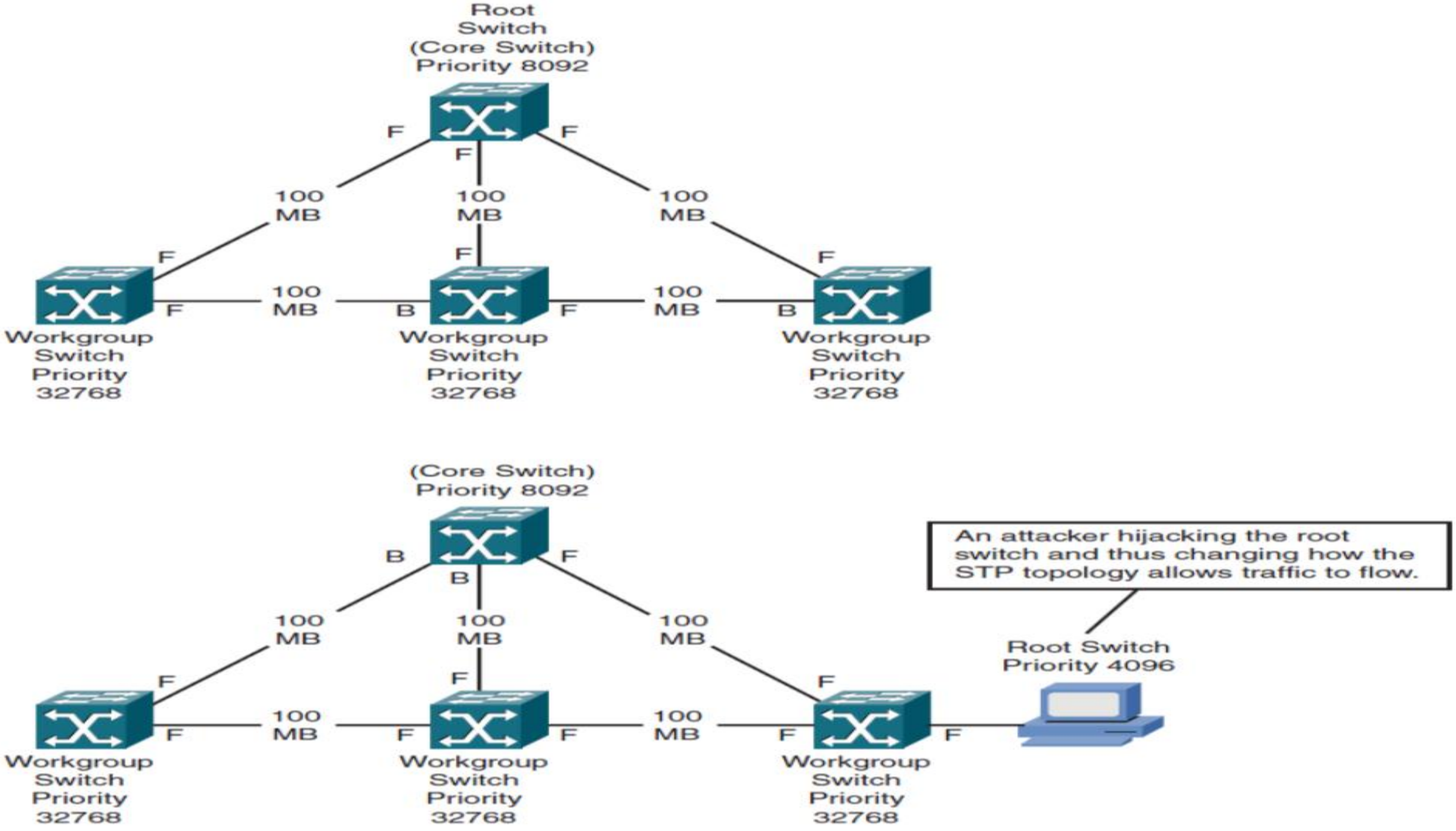
SPANNING TREE PROTOCOL (STP) SPOOFING ATTACKS

STP prevents bridging loops in a redundant switched network environment. By avoiding loops, you can ensure that broadcast traffic does not become a traffic storm. STP is a hierarchical tree-like topology with a “root” switch at the top. A switch is elected as root based on the lowest configured priority of any switch (0 through 65,535). When a switch boots up, it begins a process of identifying other switches and determining the root bridge. After a root bridge is elected, The switches determine the path to the root bridge, and all redundant paths are blocked. STP sends configuration and topology change notifications and acknowledgments (TCN/TCA) using bridge protocol data units (BPDU).

SPANNING TREE PROTOCOL (STP) SPOOFING ATTACKS

An STP attack involves an attacker spoofing the root bridge in the topology. The attacker broadcasts out an STP configuration/topology change BPDU in an attempt to force an STP recalculation. The BPDU sent out announces that the attacker's system has a lower bridge priority. This lower switch priority will prompt STP to perform a root election, resulting in the switch with the lower priority winning. The attacker (acting as the root switch) can then see a variety of frames forwarded from other switches to it. Besides the capability to take over the root switch, the capability to cause STP recalculation can also cause a denial of service (DoS) condition on the network by causing an interruption of 30 to 45 seconds each time the root bridge changes, depending on the version of STP implemented.

SPANNING TREE PROTOCOL (STP) SPOOFING ATTACKS



An attacker hijacking the root switch and thus changing how the STP topology allows traffic to flow.

Figure 4-5 *STP Spoofing Attack*

SWITCH DATA PLANE SECURITY TECHNOLOGIES

- Switch port configuration
- Port Security
- Root Guard, BPDU Guard
- DHCP Snooping
- Dynamic ARP inspection (DAI)
- IP Source Guard

SWITCH PORT CONFIGURATION

The following list includes good guidelines to follow when setting up a switch securely and avoiding VLAN hopping attack risks:

- Disable all unused ports and place them in an unused VLAN.

- Set all user ports to non trunking mode by disabling DTP. (It is not a bad idea to set all ports by default to access mode and then reconfigure the trunking ports as needed.)

Switch(config-if)#switchport nonegotiate

- For backbone switch-to-switch connections, explicitly configure trunking and disable DTP.

Switch(config-if)#switchport mode (access|trunk|dynamic auto dynamic desirable)

- Do not use VLAN 1 as the switch management VLAN.

Switch(config-if)#switchport trunk native vlan *vlan-id*

ROOT GUARD, BPDU GUARD

To mitigate STP manipulation, two different features can be used. **The Root Guard feature is configured on a switchport that should never become a root port**. If the switchport receive a superior BPDU, the port will go into **root-inconsistent state**, indicating that another switch is attempting to become the root switch.

The other feature is BPDU Guard; BPDU Guard should be implemented on a switchport or interface that should never receive a BPDU packet. If the port which configured with BPDU Guard and receive a BPDU, the port will go into the **error-disable state**. All access ports should never receive a BPDU and can be configured with BPDU Guard to eliminate an attacker plugging into an access port and acting as a superior switch.

ROOT GUARD, BPDU GUARD

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

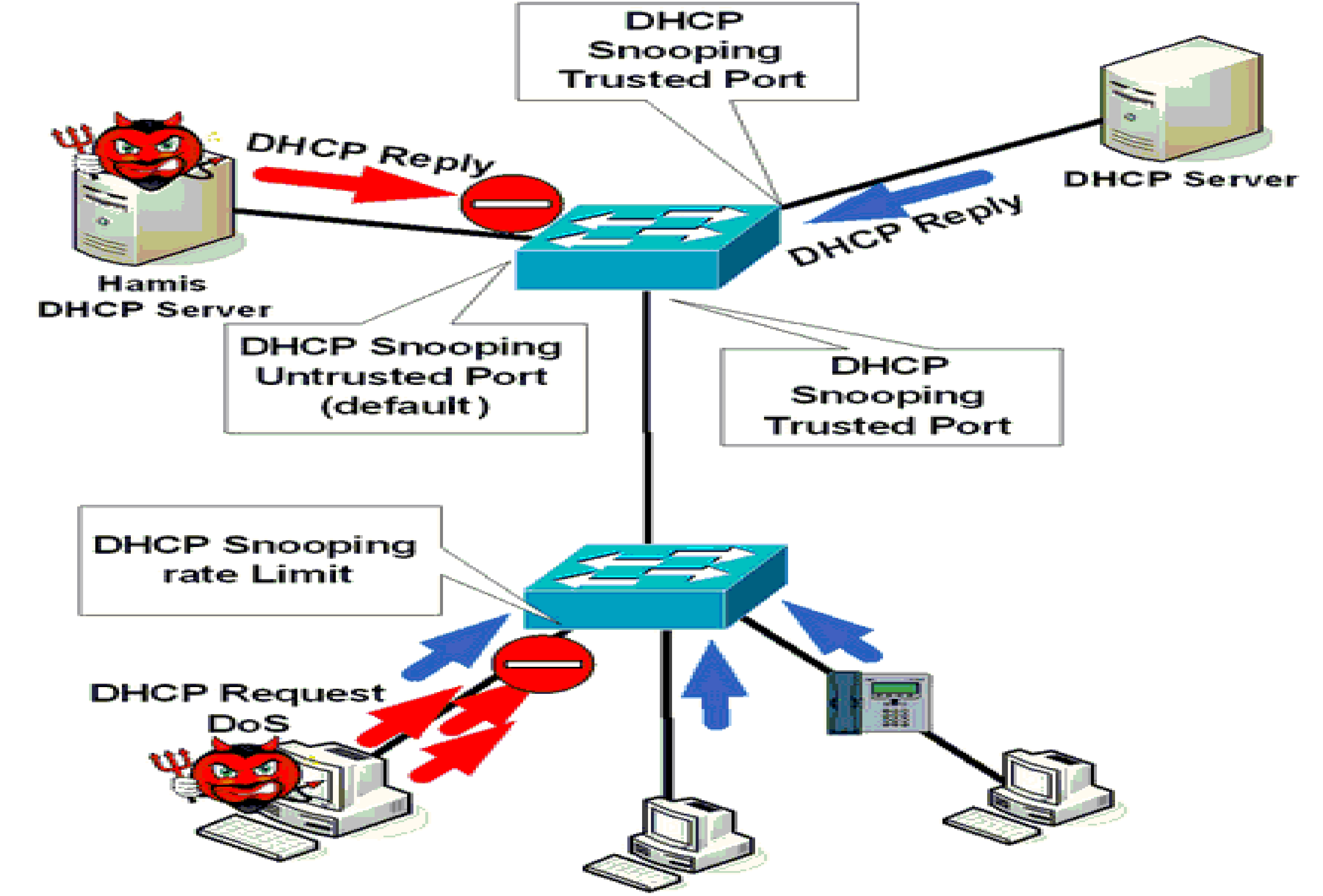
```
Switch(config)# spanning-tree portfast bpduguard default
```

```
Switch(config-if)#spanning-tree bpduguard (enable|disable)
```

DHCP SNOOPING

DHCP snooping. DHCP snooping is a DHCP security feature that provides network security by filtering untrusted DHCP messages using a DHCP snooping binding database that it builds and maintains, This binding table includes the client MAC address, IP address, DHCP lease time, binding type, VLAN number, and interface information on each untrusted switchport or interface. by default, all switchports are untrusted. A trusted switchport or interface should be configured to receive messages only from a trusted DHCP source or a network that contains a trusted DHCP source.

DHCP SNOOPING


DHCP Snooping Trusted Port
DHCP Reply
DHCP Server
DHCP Reply
Hamis DHCP Server
DHCP Snooping Untrusted Port (default)
DHCP Snooping Trusted Port
DHCP Snooping rate Limit
DHCP Request DoS

DHCP SNOOPING

```
Switch(config)# ip dhcp snooping
```

```
Switch(config)# ip dhcp snooping binding mac-address vlan vlan-id ip-address interface interface expiry seconds
```

```
Switch(config-if)# ip dhcp snooping limit rate rate
```

```
Switch(config-if)# ip dhcp snooping trust
```

IP SOURCE GUARD

The IPSG feature works on Layer 2 ports by restricting IP traffic based on the entries that exist in the DHCP snooping binding table. When enabled, IPSG will not allow any IP traffic over the switchport except for that traffic coming from the entry listed in the DHCP snooping table.

IPSG also offers the capability to configure a static IP source binding that can be used in situations without the use of the DHCP snooping binding table.

The two available options include:

■ **Source IP address filtering**

■ **Source IP and MAC address filtering**

IP SOURCE GUARD

```
Switch(config-if)# ip verify source vlan dhcp-snooping (port security)
```

```
Switch(config)# ip source binding mac-address vlan vlan-id ip-address
interface interface
```

NETWORK ACCESS CONTROL

Network Access Control is the solution for providing access control to corporate networks. It designed to enable secure user and host access to enterprise networks. It enables enterprise policy enforcement of all users and hosts. The solution promotes authentication to access the network; this authentication also serves as the basis for differentiating users and/or hosts, providing varying levels of access to networked resources based on corporate access policy.

NETWORK ACCESS CONTROL

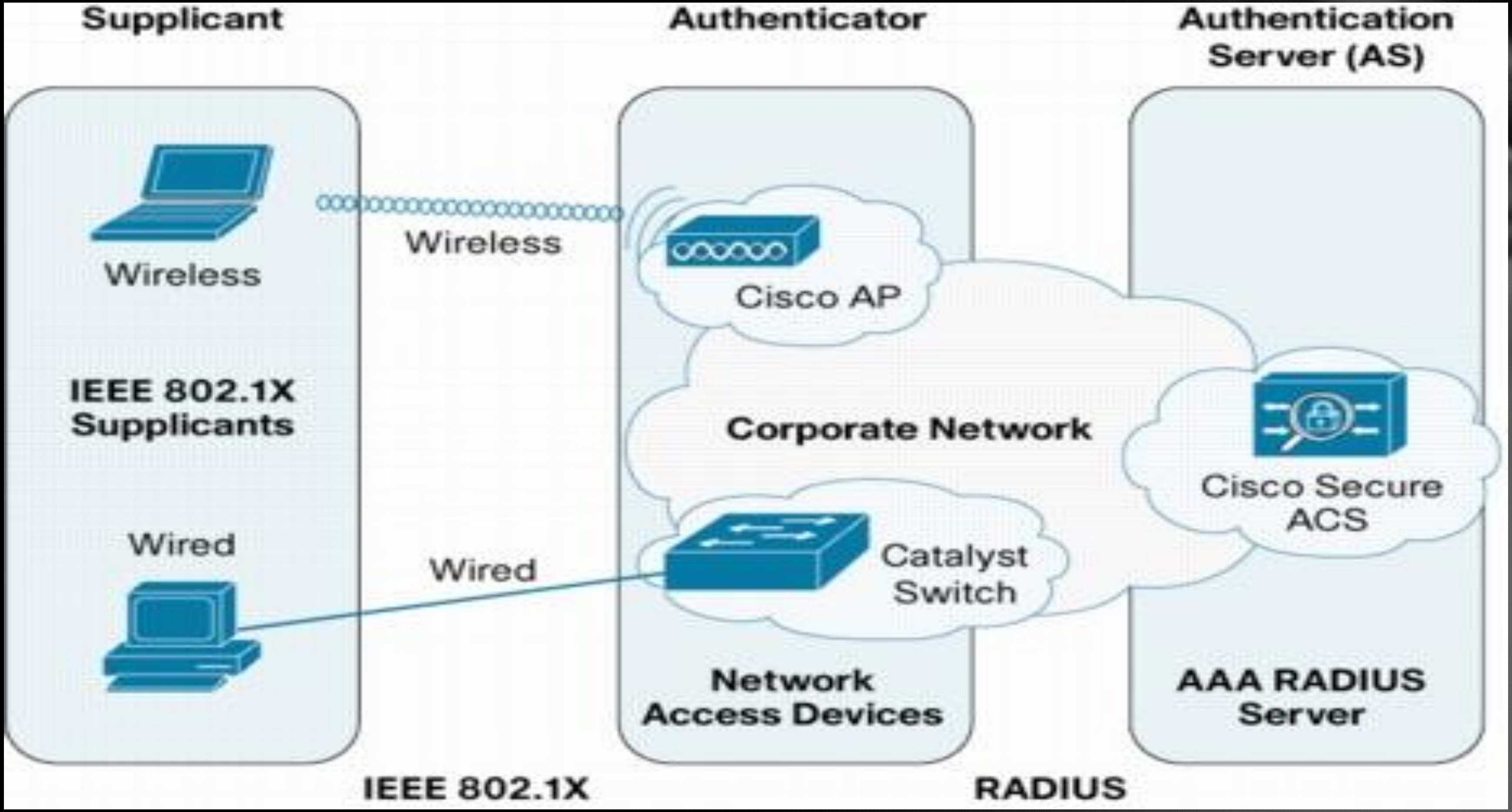
Questions	Actions
Who are you?	It uses 802.1X to authenticate the user
Where can you go?	Based on Authentication, the user is placed in the correct workgroup or VLAN
What service level do you receive?	The user can be given a per-user access control list to explicitly restrict or allow access to specific resources on network
What are you doing?	Using the identity and the location of the user, tracking and accounting can be better managed

NETWORK ACCESS CONTROL – 802.1X

The 802.1x standard defines a client-server-based access control and authentication protocol that prevents unauthorized clients from connecting to a LAN through publicly accessible ports unless they are properly authenticated. The authentication server authenticates each client connected to a switch port before making available any services offered by the switch or the LAN.

Until the client is authenticated, 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL), Cisco Discovery Protocol (CDP), and Spanning Tree Protocol (STP) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

NETWORK ACCESS CONTROL - COMPONENTS



ROUTER DATA PLANE SECURITY SOLUTIONS

The most common types of routed data plane attacks are

■ IP spoofing

■ Denial of service

■ Traffic flooding

IP SPOOFING

An attacker attempts to send and receive traffic on the network using an IP address of another known host or known network. The attacker is then able to use resources on the network that are associated with that specific IP address

The three primary methods used to perform IP spoofing are as follows:

■ Injecting packets with the IP address of an existing host

■ spoofing an existing host using source routing

■ Injecting packets from non-existing hosts to perform a denial of service attack.

DENIAL OF SERVICE

Video show

TATA
TATA COMMUNICATIONS
TATA COMMUNICATIONS
00:06

ROUTED DATA PLANE SECURITY TECHNOLOGIES

- Access Control List (ACL)
- Flexible Packet Matching (FPM)
- Unicast Reversed Path Forwarding (URPF)
- Flexible NetFlow

FLEXIBLE PACKET MATCHING (FPM)

FPM enables the user to configure match parameters based on arbitrary bits of a packet and arbitrary depths within the packet header and payload.

Implementation:

Step 1. Load the protocol header description file(s) (PHDF)

Step 2. Define the protocol stack (IP-UDP, IP-TCP, etc.)

Step 3. Define FPM match criteria filter (class-map)

Step 4. Define action to take on classes (service-map)

Step 5. Apply service policy to an interface

FLEXIBLE PACKET MATCHING (FPM)

Step 1. Load the protocol header description file(s) (PHDF)

A PHDF is used to define the various field names within a specific protocol.

```
c)#load protocol system :fpm/phdf/ip.phdf
c)#load protocol system : fpm/phdf/tcp.phdf
```

Step 2. Define the protocol stack (IP-UDP, IP-TCP, etc.)

The purpose is to define a number of criteria that are used to match specific traffic

Two class map types are used with FPM:

■ **Stack:** Specifies the specific protocol stacks that will be used to match (for example, IP, TCP, UDP) and can be only used with the **match-all** keyword.

■ **Access control:** Matches specific patterns within the traffic of interest.

FLEXIBLE PACKET MATCHING (FPM)

Step 3. Define FPM match criteria filter (class-map)

The second part of this process is configuring specific match criteria; to do this, the **match start** and the **match field** commands are used. As stated earlier, the **match field** command only works after a PHDF has been loaded. The **match start** command is used to match a specific pattern based on a specific offset and length and whether to begin inspection at the beginning of the Layer 3 packet header or at the beginning of the Layer 2 frame header.

two different separate class maps are being created:

■ **tcp-class:** This class map is configured to match the IP protocol header field when it is equal to 0x6 (TCP) and tells FPM that the next protocol to be analyzed will be TCP.

■ **sample-match:** This class map is configured to match traffic that has a TCP destination port that is equal to 0x50 (80) *and* has the contents "0x1234" at offset 200 in the IP packet.

FLEXIBLE PACKET MATCHING (FPM)

```
router(config)# class-map type stack match-all tcp-class
router(config-cmap)# match field ip protocol eq 0x6 next tcp
router(config)# class-map type access-control match-all sample-match
router(config-cmap)# match field tcp dest-port eq 0x50
router(config-cmap)# match start l3-start offset 200 size 2 eq 0x1234
```

Step 4. Define action to take on classes (service-map)

Configure what to do with the traffic that was matched with the class map; this is done through the creation of a traffic policy.

```
router(config)# policy-map type access-control tcp-policy-nest
router(config-pmap)# class sample-match
router(config-pmap-c)# drop
router(config)# policy-map type access-control tcp-policy
router(config-pmap)# class tcp-class
router(config-pmap-c)# service-policy tcp-policy-nest
```

FLEXIBLE PACKET MATCHING (FPM)

Step 5. Apply service policy to an interface

The final step in this process is the application of the traffic policy on a specific interface.

This application can be configured in either an incoming (input) or an outgoing (output) direction.

```
router(config)# interface FastEthernet0/0
router(config-if)# service-policy type access-control input tcp-policy
```

UNICAST REVERSED PATH FORWARDING

Unicast RPF provides a source validation step to packet handling; it does this by verifying the source information of a packet to information contained within the Cisco Express Forwarding (CEF) Forwarding Information Base (FIB).

Unicast RPF operates in one of two modes:

■ Strict (normal): When in strict mode, Unicast RPF verifies that the source address is in the FIB and that the source address was received on the best return route interface as determined by CEF.

■ Loose: Loose mode verifies only that the source address exists within the FIB and not the interface.

```
ip cef {distributed}

ip verify unicast source reachable-via [rx | any] {access-list}
```

CONTROL PLANE SECURITY SOLUTIONS

The major type of attacks:

- Denial of Service
- Routing Protocol Spoofing

CONTROL PLANE SECURITY TECHNOLOGIES

- Control Plane Policing (CoPP)
- Control Plane Protection (CPPr)
- Routing Protocol Authentication

CONTROL PLANE POLICING (COPP)

Video show

CBT Micro NUGGETS

Control Plane Policing (CPP)

by: Keith Barker

CONTROL PLANE PROTECTION (CPPR)

The Control Plane Protection feature is an extension of the policing functionality provided by the existing Control-plane Policing feature. The Control-plane Policing feature allows Quality of Service (QoS) policing of aggregate control-plane traffic destined to the route processor. The Control Plane Protection feature extends this policing functionality by allowing finer policing granularity.

The functionality added with Control Plane Protection includes a traffic classifier, which intercepts traffic and classifies it into three control-plane categories. New port-filtering and queue- thresholding features have also been added. The port-filtering feature provides for policing of packets going to closed or nonlistened TCP/UDP ports, while queue- thresholding limits the number of packets for a specified protocol that will be allowed in the control-plane IP input queue.

MANAGEMENT PLANE SECURITY SOLUTIONS

- Passwords
- Privileges
- Role Based Access Control (RBAC)
- ACL
- SSH
- SNMP
- Management Plane Protection (MPP)
- Auto-Secure

SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

SNMP is used by many organizations to keep a good management and monitoring capability for all network devices

SNMP is broken down into three components:

■ **SNMP manager:** The SNMP manager controls and monitors the devices within the network using SNMP.

■ **SNMP agent:** The SNMP agent is the component that is run directly on the device and maintains data and reports this data (if needed) to the SNMP manager.

■ **MIB:** The Management Information Base (MIB) is a virtual information storage location that contains collections of managed objects. Within the MIB, there are objects that relate to different defined MIB modules (for example, the interface module).

SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

To obtain information from the MIB on the SNMP agent, several different operations can be used:

■ **Get:** Used to get information from the MIB from an SNMP agent

■ **Set:** Used to get information to the MIB from an SNMP manager

■ **Walk:** Used to list information from successive MIB objects within a specified MIB

■ **Trap:** Used by the SNMP agent to send a triggered piece of information to the SNMP manager

■ **Inform:** The same as a trap, but adds an acknowledgment that is not provided with a trap.

SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

- **SNMP Version 1:** The oldest and most basic version of SNMP

· Pros: Supported by most devices that are SNMP compatible; simple to set up

· Cons: Limited security as it only uses a simple password (“community string”) and data is sent in clear text (unencrypted)

- **SNMP Version 2c:** Adds 64 bit counters

· Pros: Supports 64 bit counters to monitor bandwidth usage in networks with gigabits/second loads

· Cons: Limited security (same situation as with SNMP V1)

- **SNMP Version 3:** Adds authentication and encryption

· Pros: Offers user accounts and authentication for multiple users and optional encryption of the data packets, which makes it much more secure; plus all advantages of Version 2c

· Cons: none

MANAGEMENT PLANE PROTECTION (MPP)

it is possible to know which device interface or interfaces will always be used for management traffic. It is in these situations when the Management Plane Protection (MPP) feature can be used. MPP enables you to limit the source of management traffic to a specific interface (or interfaces) on a device.

```
Router# configure terminal
Router(config)# ip cef
Router(config)# control-plane host
Router(config-cp-host)# management-interface fastethernet0/0 allow ssh
```

REFERENCES

- Cisco Press – CCNP Security Secure 642-637
- Hacking Exposed Cisco Network: Cisco Security Secrets and Solutions
- http://www.tatacommunications.com
- http://www.cbtnuggets.com

Ziad Zubidah
Tel.: (+962) 6-5300222 Ext.354
Mob: (+962) 77-706 0561
Email*:* ***ziad.zubidah@nitc.gov.jo***