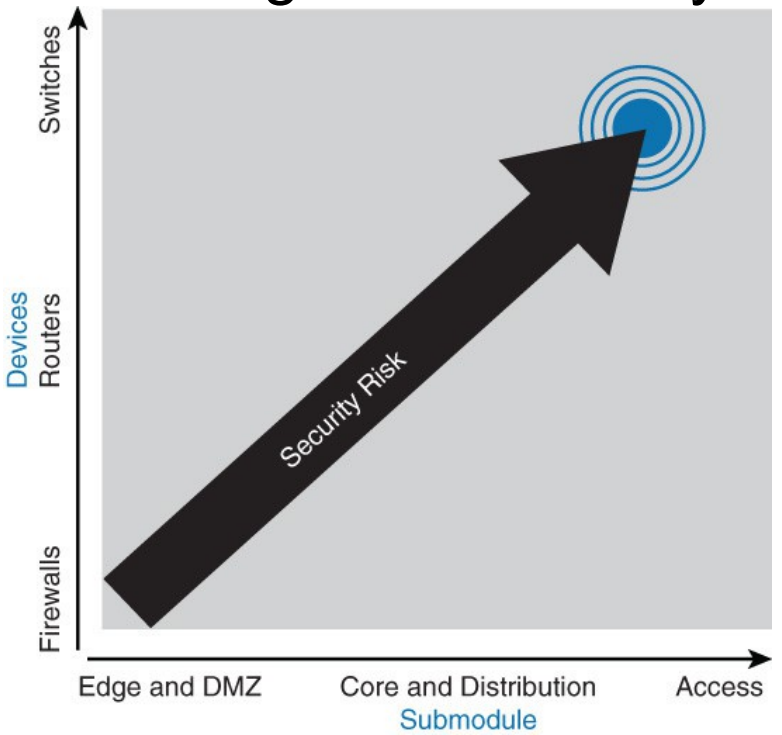
Chapter 10
Network Security
NET3011 – 17W

Network Security – Basics

- In this section, we'll try to focus on L2 aspects (mostly) that don't overlap (much?) with NET3007
- Years ago, the focus of network security was keeping the "bad guys" out (defenses facing outwards); now it's at least as important to protect against attacks originating from *within the network* (defenses facing inwards)
- We'll look at port security, storm control, securing VLANs, and a multitude of spoofing attacks
- Don't forget PVLANs! (Already covered at the beginning of the course.)

Security: Most Vulnerable Devices

- "Network security often focuses on edge routing devices and the filtering of packets based on L3 and L4 headers" FLG, p. 410
- "Campus access devices and L2 are largely unconsidered or an afterthought in most security discussions" FLG, p. 410
- Default security state:
  firewalls = block all, pass none, until configured differently;
  routers/switches = block none, pass all, until configured differently
- **"In the future, switches from Cisco will *not* be configured for open communication by default, but will have the features discussed in this chapter deployed to restrict communication unless explicitly allowed & configured."** FLG p. 411



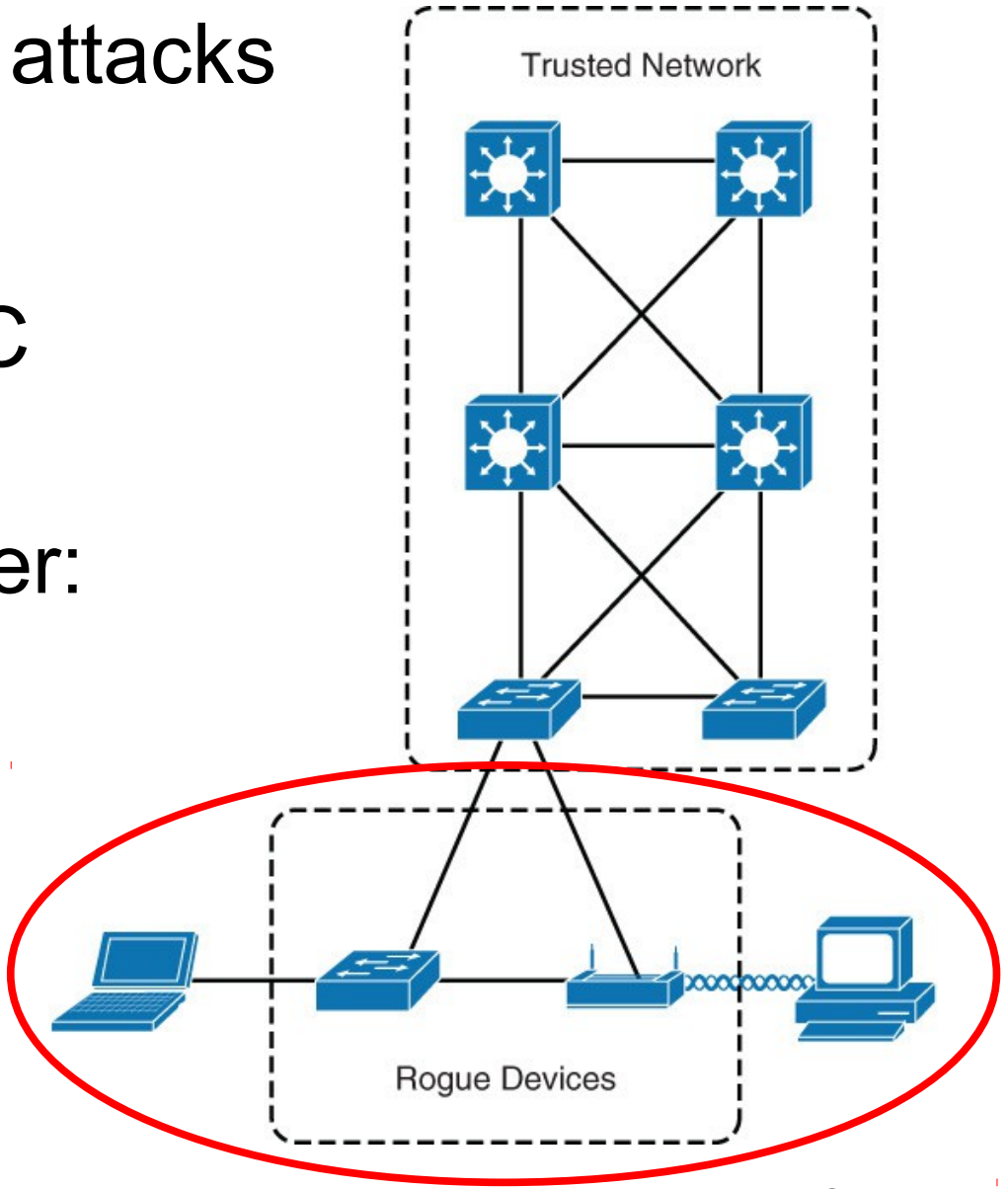
Security – Principles For Safety

- If it ever fails, the entire enterprise is exposed and vulnerable when relying solely on security established at the enterprise edge. It is better to have several layers of security before reaching internal resources (at L2).
- Public access for "external-only" resources can be a misnomer, since applications often require at least indirect access to enterprise resources.
- BYOD, wireless, and visitors all pose a significant threat as they allow attackers physical access. Relying on physical security isn't enough.
- Cloud architectures come with many new security risks; even with a (externally) secure cloud, attacks from within can compromise the cloud (ie. back doors).

Switch Security – Attack Vectors

- Rogue access is the root cause that can lead to several different kinds of attacks
  - rogue switch
  - rogue AP
  - rogue software on a PC
    (… or even a printer!)
- 4 categories we'll consider:
  - Device access attacks
  - VLAN attacks
  - MAC attacks
  - Spoofing attacks

  … all are based on L2
  (or L2 device) attacks



Security - Device Access Attack

- Scenario:
  - attacker tries to establish administrative access to a switch (… *or* a router, firewall, or other!)
- Countermeasures:
  - limit information available to attackers: disable CDP where not essential or intentionally used
  - prevent eavesdropping on credentials: never use telnet in a production network
  - use SSH with *long RSA keys*; use the latest version available on the device (e.g. SSH ver 1 has known weaknesses; upgrade the IOS?)
  - use ACLs to limit access to authorized stations

Extra: Minimal Cisco Config for SSH

Here's 5 steps for configuring a Cisco device for SSH:

1. Define credentials eg. a local account:
   (use Radius/Tacacs if you're willing to do more config)
   ```
   A(config)# username {user} secret {password}
   ```
2. Configure login authentication method
   ```
   A(config)# line vty {x}[y]
   A(config-line)# login local
   ```
3. Define the hostname:
   ```
   A(config)# hostname {node-name}
   ```
4. Define domain name:
   ```
   A(config)# ip domain-name {name.com}
   ```
5. Generate RSA keys:
   ```
   A(config)# crypto key generate rsa modulus {len}
   ```

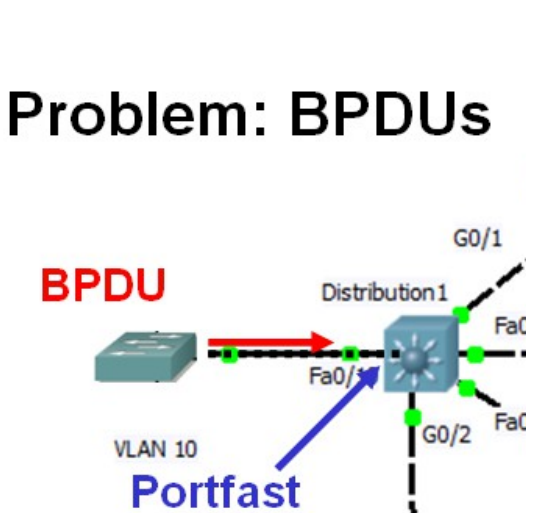
min = 1024
better = 2048
best = 4096
(but slow)

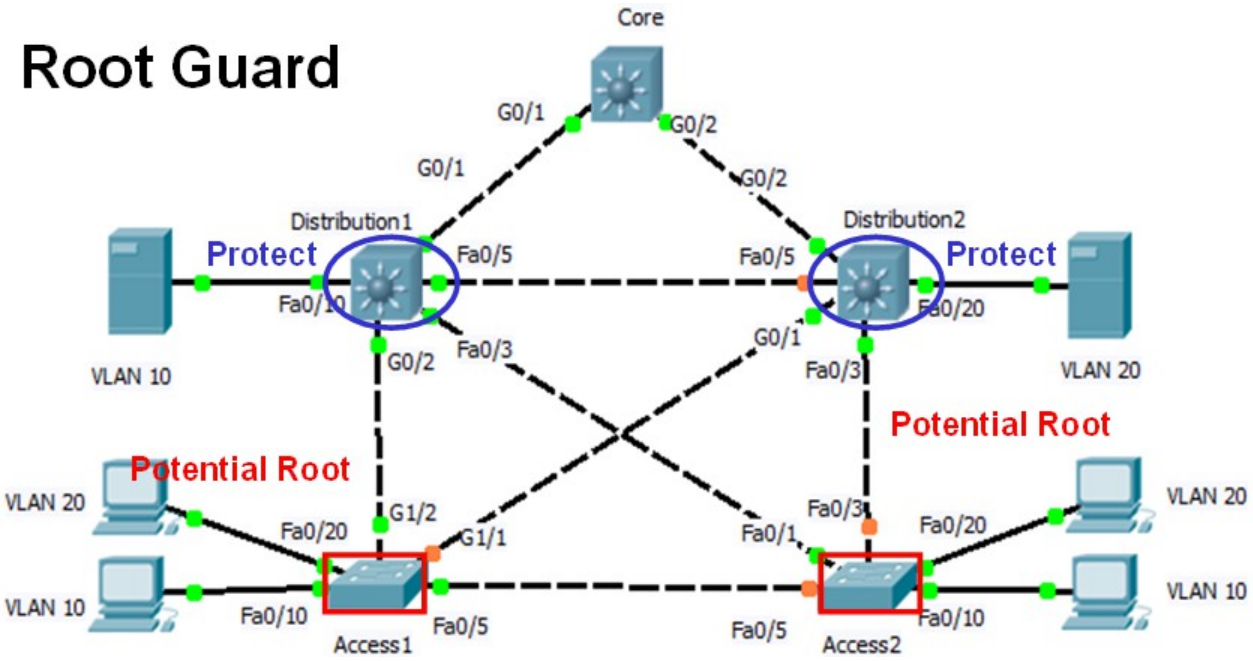
Switch Security – VLAN Attacks

- VLAN attacks come in two forms:
  - switch attack / switch spoofing attack
  - VLAN hopping attack
- We won't cover VLAN hopping attack:
  - based upon double-tagged VLAN frames; ("illegal" in a campus network; okay for an ISP!) check textbook if you're interested in details
  - unable to find evidence that it still exists
  - may only exist in older hardware & IOS versions
- Primary defenses against switch (spoofing) attack: BPDU guard, root guard, access ports, manual trunk config
- VLAN ACLs (VACL) + Storm Control provide extra protection
- *Don't forget* about protection from Private VLANs!

VLAN Attacks – Taking Over Root

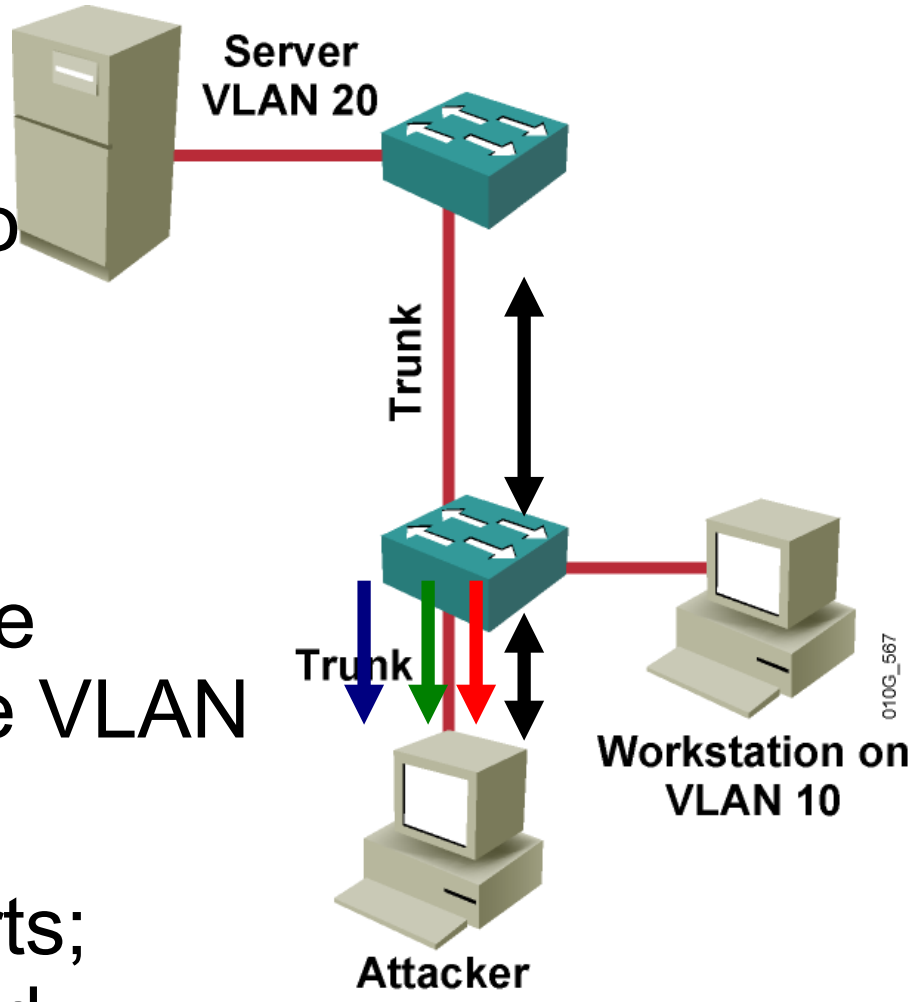
- Scenario: Become the Root Bridge by sending (real or emulated on a PC) BPDUs, causing security breaches and/or DoS:
  – all traffic flows towards the (new) Root Bridge
  – slower access layer links may be overloaded
- Countermeasure: BPDU guard and Root guard





VLAN Attacks – Pulling Trunk Traffic (1)

- Scenario: Use either a real switch or a PC to spoof a switch:
  – both can negotiate a trunk
- Attacker then gains access to data on all VLANs carried on the negotiated trunk
- Management traffic (or other sensitive traffic) was only safe because it was on a separate VLAN … not any more!
- Countermeasure: access ports; manually configure trunks and allowed VLANs



VLAN Attacks – Pulling Trunk Traffic (2)

- Assigning an access VLAN is **not** sufficient

```
Sw(config)# interface range fa 0/11 - 15
Sw(config-if-range)# switchport access vlan 10
Sw(config-if-range)# end

Sw# show interface fa 0/11 switchport
Name: Fa0/11
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: ????
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 10 (Accounting)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
```

VLAN Attacks – Pulling Trunk Traffic (3)

- Configuring access mode ensures no trunking!

```
Sw(config)# interface range fa 0/11 - 15
Sw(config-if-range)# switchport access vlan 10
Sw(config-if-range)# switchport mode access
Sw(config-if-range)# end

Sw# show interface fa 0/11 switchport
Name: Fa0/11
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 10 (Accounting)
```

VLAN Attacks – Pulling Trunk Traffic (4)

- Configure all non-trunk ports as access ports so that trunking cannot be negotiated
- Additionally, place all unused ports:
  – in the shutdown state
  – in Blackhole VLAN which is only for unused ports

```
Sw(config)# interface range fa 0/11 - 15
Sw(config-if-range)# switchport access vlan 10
Sw(config-if-range)# switchport mode access
Sw(config-if-range)# end

Sw(config)#interface range fa 0/16 - 17
Sw(config-if-range)# shutdown
Sw(config-if-range)# switchport mode access
Sw(config-if-range)# switchport access vlan 999
```

VLAN Attacks – Pulling Trunk Traffic (5)

- Configure all trunk ports
  - as "on," rather than negotiated
  - with native VLAN different from any data VLANs
  - specify the allowed VLANs carried on the trunk

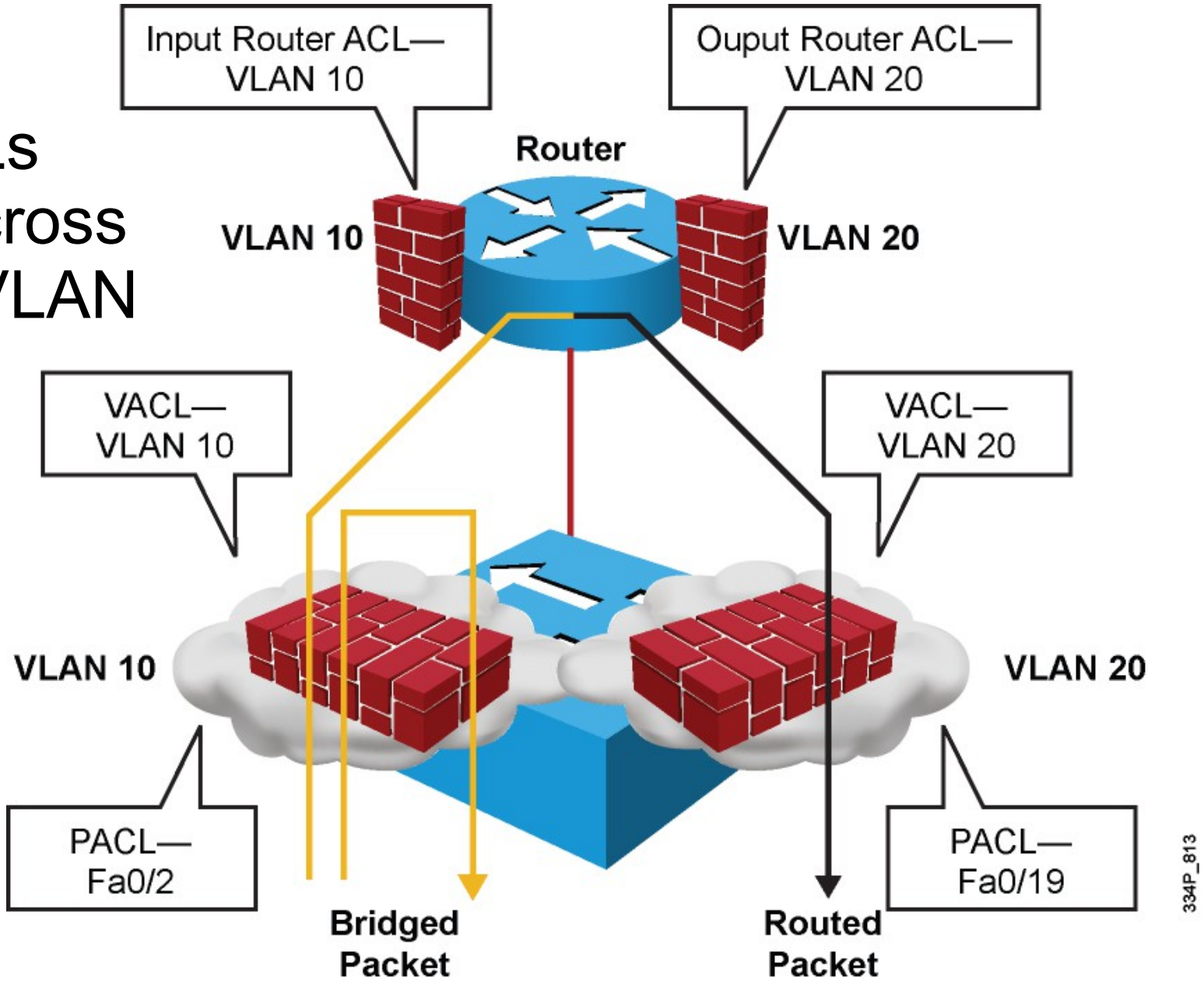
```
Sw(config)# interface gig 0/1
Sw(config-if)# switchport mode trunk
Sw(config-if)# switchport trunk native vlan 2
Sw(config-if)# switchport trunk allowed vlan 2,10,20
```

- Is there a possible security issue or benefit from specifying:

  `switchport nonegotiate` ?

VLAN Attacks – VACLs (1)

- VLAN ACLs operate across an entire VLAN



VLAN Attacks – VACLs (2)

- Simple configuration of port ACLs:

```
Sw(config)# access-list 100 permit ip 10.1.9.0 0.0.0.255 any
Sw(config)# mac access-list extended BACKUP_SERVER
Sw(config-ext-mac)# permit any host 0000.1111.4444

Sw(config)# interface fa0/1
Sw(config-if)# ip access-group 100 in  !ONLY in possible
RTR(config)# interface fa0/1
RTR(config)# ip access-group 100 in
RTR(config-if)# ip access-group 100 out !in/out possible
Dev(config)# line con 0
Dev(config-line)# access-class 100 in   !in/out possible
```

- As you already know, port ACLs always end with an implicit "deny all" !

VLAN Attacks – VACLs (3)

- VACL has similar, but not entirely identical structure:

```
Sw(config)# access-list 100 permit ip 10.1.9.0 0.0.0.255 any
Sw(config)# mac access-list extended BACKUP_SERVER
Sw(config-ext-mac)# permit any host 0000.1111.4444
```

```
Sw(config)# vlan access-map XYZ 10
Sw(config-map)# match ip address 100
Sw(config-map)# action drop
Sw(config-map)# vlan access-map XYZ 20
Sw(config-map)# match mac address BACKUP_SERVER
Sw(config-map)# action drop
Sw(config-map)# vlan access-map XYZ 30
Sw(config-map)# action forward
```

```
Sw(config)# vlan filter XYZ vlan-list 10,20
```

- Like ACLs, they always end with an implicit "deny all"

VLAN Attacks – VACLs (4)

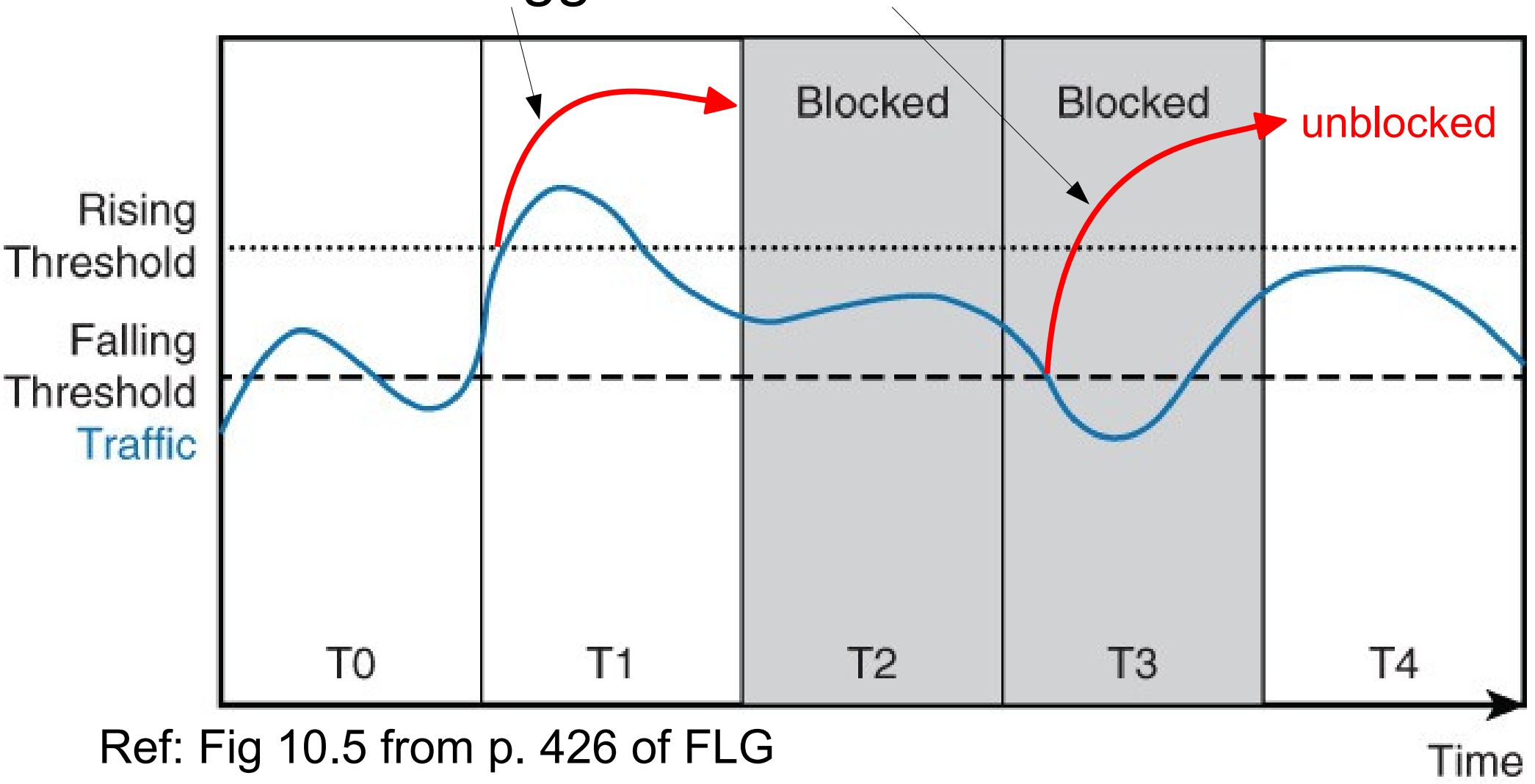
- The applicability / restrictions on ACLs, Port ACLs, and VACLs in Cisco implementation is fairly detailed, and covered on p.424-425, 448-450:
- Some key points:
  - "*An instance of an ACL that is mapped to a L2 port is called a PACL. An instance that is mapped to a L3 port is called a [RACL]* "
  - "*A MAC ACL is not applied to IP, MPLS, or ARP messages*"
  - "*The PACL feature does not affect L2 control packets such as CDP, VTP, DTP, and STP received on the port.*" (Really? Recall UDLD triggering!)
  - "*PACLs can be configured on a LAG interface but not on its ... members.*"
  - "*In port prefer mode, PACLs take effect and override the effect of other ACLs. This mode is the only mode allowed when applying [a] PACL on a trunk.*" … "*The one exception to this rule is when the packets are forwarded in the software due to an exception to hardware forwarding. The route processor then applies the ingress [RACL] regardless of the PACL mode.*" https://www.youtube.com/watch?v=v77SF4TFUoM
- "VACLs, [RACLs], and PACLs work together seamlessly; **however, care must be taken when engineering these filtering techniques together.**"
- Now, try to make sense of Q22 in the Ch 10 Review Questions!

VLAN Attacks – Storm Control (1)

- Another form of attack is achieved simply by flooding and saturating a link: DoS by sheer volume of traffic
- Cisco provides protection by setting individual limits on max permissible unicast, broadcast, or multicast traffic
- Can respond by dropping excess frames (default), sending an SNMP trap, or shutting down the port
- As with GLBP, triggering and releasing the protection is based on rising and falling levels
- Cisco peculiarities:
  - "some switches consider multicast traffic as broadcast"
  - do not configure it on members of a LAG ("unsupported")
  - "configured percentage levels are only approximate and actual enforced level might differ"

VLAN Attack – Storm Control (2)

- Illustration of trigger and release levels



Ref: Fig 10.5 from p. 426 of FLG

- *What other protocol has similar hysteresis controls*?!

VLAN Attack – Storm Control (3)

- "behavior of storm control differs between [Cisco] software versions and hardware models."
  – May trigger/release in 1 sec intervals
  – May trigger *immediately*
- Unfortunately, storm control is per port and *not differentiated per VLAN* (so a cross-VLAN attack!)

MAC Attacks – Basics

- Switches turn into hubs if their MAC address table overflows; examine limits with "show sdm prefer"
- MAC address limits are *not* per VLAN but per switch
- Consider the consequences to a single switch, and then *to all upstream switches*, and then for accessing traffic off the prescribed VLAN.
  What two generic kinds of attacks are possible?
- Can choose limit on number of MAC addresses on a per-port basis
- Can choose how those MAC addresses are determined, and how long they stay registered
- Can choose severity of action

MAC Attacks – Countermeasures (1)

- Remember: on Cisco switches *must* enable port security *separately from describing it* !!
- Default number of MAC addresses per port = 2
  Reason for that value is 1 (VoIP phone) + 1 (PC)
- Limits for access layer switches should be much smaller than for higher layer switches (2K - 16K)
- MAC addresses can be:
  – learned normally / dynamically
  – statically configured (not often used)
  – learned in a "*sticky*" manner
  – retained "forever", except that aging can be configured for the first two categories
- Sticky MAC addresses are one of two commands that pro-actively modify the running config (Save it?!)

MAC Attacks – Countermeasures (2)

Severity of response has multiple levels:

- Protect: simply discard frames from excess ("invalid") MAC addresses
- Restrict: discard frames from each excess MAC **and** register event by (1) increment counter, and (2) send SNMP trap
- Shutdown: err-disable the port, log an error message, and send SNMP trap

(Conveniently, severity increases in alphabetical order)

Spoofing Attacks – Basics

- This course covers three spoofing attacks involving L3 addressing:
  – DHCP server spoofing
  – IP address spoofing
  – ARP spoofing
- It is vitally important that you understand the frame and packet header details and IP operation in order to understand these attacks
- Countermeasures are all founded on DHCP snooping, to build a trusted database mappings between port, MAC address, and IP address
- DHCP snooping splits "broadcast" traffic into two (three?) different categories, such that one category is flooded in a restricted manner (not completely broadcast anymore!)

DHCP Server Spoofing – Bad News

- How does DHCP work (i.e. what is the sequence?)
- How can you create a DoS attack against DHCP?
- What are the consequences of malicious GW, DNS, TFTP server, or other settings?
- Who needs to receive which messages?
- What is an indication of illegitimate (spoofed) messages?
- Like most security measures, once DHCP snooping is enabled, ports are considered restricted unless configured as "trusted"
- Invalid traffic received on a port causes a port shutdown
- DHCP snooping is enabled *globally*, but must be applied to specific *VLAN*s, and relevant *ports* marked as trusted or rate-limited

IP Address Spoofing – Stolen Identity

- Reflected DoS service attacks are based on spoofing the source IP address; replies are sent to a victim/target address, thereby overwhelming it
- Cisco's countermeasure is IP Source Guard:
  - DHCP snooping *must* be enabled
  - initially, *all* traffic except for DHCP is denied
  - only when DHCP is complete, the switch automatically creates and installs a (per port) PACL with the appropriate source IP address (Careful: could possibly exhaust TCAM limitations!)
  - can additionally require that the source MAC address also be validated via DHCP
  - static entries can be provided for printers, servers, and other similar resources

ARP Spoofing – Where's My Server?

- ARP Spoofing can potentially negate all the previous spoofing protections: how *does a device reach other resources*?
- Countermeasure is Dynamic ARP Inspection (DAI)
  - DHCP snooping *must* be enabled
  - Like most security measures, once DAI is enabled, all ports (in a VLAN) are considered restricted and ARP responses are inspected, except for ports configured as "trusted"
  - can be even more restrictive by ensuring L2 and ARP header MAC addresses match (live demo?)
  - DAI is enabled per *VLAN*, and relevant *ports* marked as trusted

Cisco-isms: DHCP Snooping Issues

- By default, Cisco switches *change* DHCP client packets when DHCP snooping is enabled:
  add Option 82 info while leaving the GW addr = 0
- By default, Cisco DHCP servers and/or relay-agents *reject* DHCP client packets containing Option 82 info with a GW addr = 0.0.0.0
- Solutions include:
  - force the DHCP server to accept these types of request packets (as per lab 10.1)
    ip dhcp relay information trust-all
  - stop snooping switch from adding Option 82 info:
    no ip dhcp snooping information option

Refs: https://brbccie.blogspot.ca/2013/03/dhcp-snooping-and-option-82.html
https://www.cisco.com/en/US/docs/ios/12_4t/ip_addr/configuration/guide/htdhcpre.html#wp1092711

Security – Best Practices

1. Secure passwords: enable ~~password~~ secret; console password; service password-encryption; AAA
2. Useful system banners: banner MOTD, banner login
3. Secure vty access: ACLs; disable telnet; SSH with *long RSA keys* (>1024 bits)
4. Secure web access: disable HTTP; HTTPS only if necessary; use ACLs
5. Secure SNMP: disable write access unless specifically needed; use SNMPv3 with authentication
6. Secure unused ports: hard-configured in access mode **and** placed in blackhole VLAN **and** shutdown
7. Secure CDP: disable it on all access ports unless needed (e.g. Cisco VoIP)
8. Secure STP: BPDU guard; root guard; avoid BPDU filter unless necessary
9. Port security: limit # of MACs on access ports; activate *shutdown* mode; rate-limit violation notices
10. Use DHCP snooping + extensions to protect against spoofing (DHCP, IP, ARP)
11. Secure trunks: disable DTP & manually configure trunks; restrict allowed VLANs; use VLAN ACLs ("VACL")

Reminder

- These slides are *not* intended to capture all details (i.e. CLI configuration & verification); they are only intended to capture and present the concepts!
- You are responsible for *reading* the textbook to gain the knowledge (memorization) and understanding (apply the knowledge)