Flicature Spreture (8) EST. district in the line of the line of unction k(a,c,d) ently, E d.userAgent, A, B, C, D Object.pre states and type (this context this [0] -a. D. Fragment), childNodes); return function(a,b){return.c. stutthis, arguments), "st off s.fn.e.extend e.fn. fur(c in a){d=i[c],f=a ere fitreturn e}, iske thic, e),e.fn.tr al ready, 11) ;else.if(Array isArray | fu (moth), isPlainObject:1 ection(a)(fo nction(a) (re return.ctre - C. C. erion(a.C.

defaultValue)else

unt-calles syllengle0s): g.1

at more, as four an en defer

10. () () ()

r.dutand(().d);if(g)(delete

and analogs(),0.sergeAttribut

AP/ITEC 2210 3.0 A: System Administration Fall 2023

Instructor: Jamon Camisso ITEC 2210 Chat: mattermost.itec2210.ca Email: jamon@vorku.ca Website: https://eclass.vorku.ca/

Date/Time: Wednesday, 19:00-22:00 Location: Zoom / ACE 003 Office hours: Via Mattermost any time

G defer a G C* oprio h C*mark i f.data Freturn 0 function k(a,c,d) (i f.data b) return d)var.c=a.document,d a.twinstr

– Midterm:

October 18, online during our 7-10pm time slot

We'll be using Zoom to collaborate on answers

Hopefully a change from the usual midterm tedium

– Lab 1/Assignment 1:

evel/itition()

creturn:B)function.k(a,c,d)(if(

Clock is ticking. October 11 @ 23:59 due date.

Readings PSNA CH23 Network Architecture

p399-401 OSI model

p404 VLAN Myths

o p408-422 Sections 23.5-23.8 inclusive

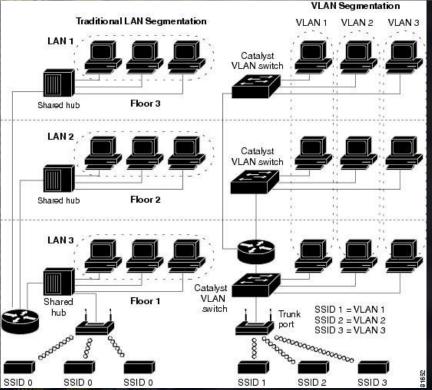
P425-430 Sections 23.10-23.12 inclusive

- VLAN is a Layer 2 construct in hardware switch or software

Subnets are not VLANs

- VLANs are not subnets
- VLANs can contain multiple subnets
- To traverse VLANs (layer 3), firewalls or routers need interfaces in both, or hosts need physical interfaces in each VLAN (layer 2)

> alta.selector bilints.selector.a.sr #.fm.e.extend e.fn.extend function[] [van fitreturn_e},isReady:11,readyWait11,N m.ready, [1] jelse if(c.attachEvent)(c.att ray.isArraylifunction(a) (return e.t



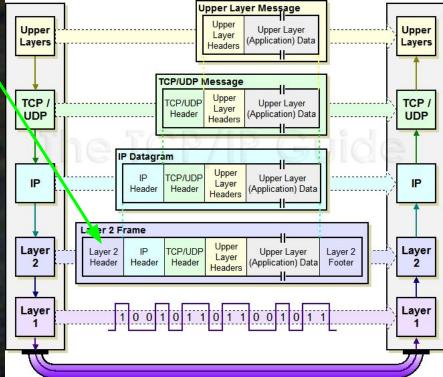
ps://www.cisco.com/c/en/us/td/docs/wireless/access_point/15-3-3-JB/configuration/guide/cg_book/cg-chap14-vlan.html

- LAN model has each switch or router separating traffic by subnet
- VLAN model allows systems on separate physical links to appear as if they are on the same subnet or network segment
- Diagram shows wireless SSIDs living in different VLANs, even though they may share the same physical uplink and switches

802.1Q VLAN tag lives in layer 2 frame header

12 bit VID gives 4096 VLAN values

- 0x000 and 0xFFF reserved
- 0x001 is usually default
- The rest are fair game



http://www.tcpipguide.com/free/t IPDatagramEncapsulation.htm

isImmediatePropagationStoppe
"defer",g C* queue",hrc."mark"
return [] function,k(a,c,d)[if(d)]

d)var.c=a.document

802.1Q VLAN tag in Ethernet Frame

1.1	at a called of), 191atn001ec	CC: TO	Inculor tartatte	and the second state of the second																							
	Preamble	SFD	Destination MAC	Source MAC		EtherType/ Size	F	Payload		CRC / FCS																	
1	2 3 4 5 6 7	8	1 2 3 4 5 6	1 2 3 4 5	6	1 2	1 .		n	1 2 3 4]	2	3	4	5	6	7	8	9	10	1	1 12					
	(i))), constance function(a) ()))), constance function(a) ()))), naked (), ()), naked (ray))	funct	<pre>(c.apply(alg+),d) item tion(a,b)(var.c-b)()); m-1).merge:function(a,c)(var.c-b)</pre>					n = 46																			
	Preamble	SFD	Destination MAC	Source MAC		802.1Q	Header	EtherType/ Size		Payload		CRC	/ FCS														
1	2 3 4 5 6 7	8	1 2 3 4 5 6	1 2 3 4 5	6	1 2	3 4	1 2	1	n]	. 2	3	4	1	2	3	4	5	6	7	8	9	1	Л]	11
			uning()), unMatchi terrates	ALC: NOT THE OWNER OF THE OWNER		TPID=0x8100	PCP/DEIVID																				

VLAN myths

 CAM/TCAM (content/ternary addressable memory) table is a list of MAC addresses and can be overflowed

Many systems will fail open and revert to bridge mode

 In bridge mode, every packet is broadcast to every port, which can lead to information leaking to an attacker, which can be used for ARP spoofing and full takeover of a network

VLAN myths

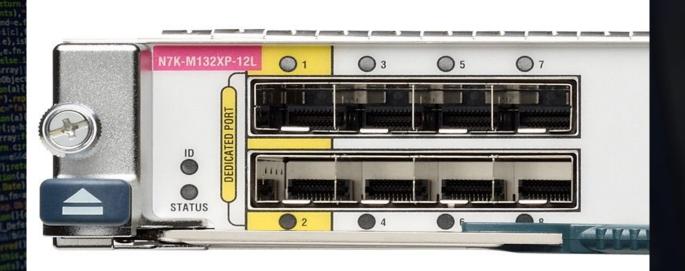
Bandwidth is a finite resource, VLANs cannot add more
 Switch backplane or ports can only move so many bit/s

VLANs just segment who sends what where

• VLAN traffic over an uplink can saturate the link

 If you don't have a good network topology, VLANs can make things worse by blocking connections

VLAN myths



https://www.safaribooksonline.com/library/view/arista-warrior/9781449358921/ch04.htm

Datacentre networking

 Three main methods of physically connecting hosts that you'll encounter

Central switch

- Top of rack switch (TOR)
- Switch fabric (Clos, or Spine & Leaf)

Datacentre networking

Central switch:

 Each host connects to a patch panel, the panel then connects to the central switch or end of row switch

• Desirable to have redundant connections, 2x cabling

 Makes for a lot of cables, and painful upgrades or recabling hosts into different networks

Datacentre networking

– Top of rack switch (TOR):

• Usually each rack has redundant switches, so 2x TOR

- Each host will connect to each switch for redundancy
- Each switch connects to the other
- Each switch connects to the core router/switch fabric

Datacentre networking

– Top of rack switch (TOR):

 Means zero downtime for maintaining each switch, as long as the switches mirror each other

 However, TOR switches need high bandwidth to core switches, otherwise upstream connectivity is limited

Much monitoring and upgrading work

Datacentre networking

- TOR Fabric, also known as Spine and Leaf:

TOR switch connects to all core fabric switches

- Each host can reach any other with the same number of hops across the whole fabric
- Capacity can be added with more Fabric/Spine switches

– TOR Fabric, also known as Spine and Leaf

Pods can be linked with the same Spine/Leaf topology

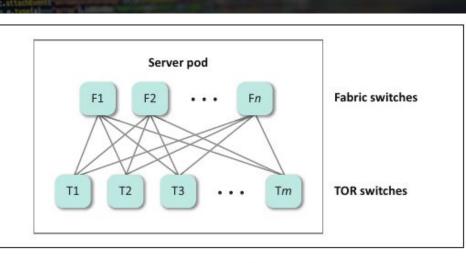


Figure 23.3: A fabric pod

WAN strategies

– How do you connect an office and a datacentre?

• **Topology** is what the network connections look like

 Technology is the equipment & protocols to make and maintain the connections

 Demarcation point is where ISP and your connections meet. You're responsible for your side, end to end

– WAN strategies

Star topology

Central datacentre, shared by various offices

 Can be made redundant with a second datacentre, and or a disaster recovery site

Redundant version known as dual star

WAN strategies

isImmediatePropagationStopped()) ifer", g C-"queue", h C "mark", i f

Multi-star topology many stars linked together via central hubs per region

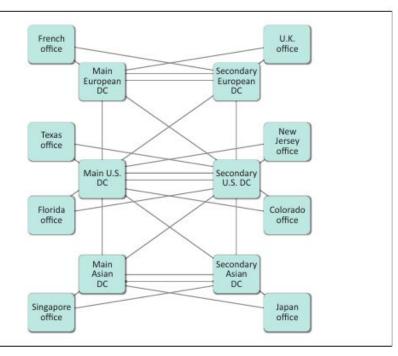


Figure 23.5: A redundant multi-star topology for a WAN

WAN strategies

Ring topology

• Every office connects to at least 2 others

 New offices mean disruptive changes, more latency as more hops are added

WAN strategies

Cloud topology

• Every office connects to a cloud provider's network

- Packets are like a letter, they reach their destination, you just don't know how or care how it happens
- Can be slow depending on other tenants

WAN strategies

Technology

• **Dedicated** line or **VPN**?

 Dedicated circuit is just that, a physical connection that is dedicated to your sites only. Fibre, copper, wireless, can be any layer 1 medium

VPN is a virtual circuit running on layer 2 or 3

WAN strategies

Dedicated

- Well understood capacity & SLA commitments
- Can scale linearly with more circuits
- Isolates traffic between sites & other companies
- Redundancy can be added with another circuit
- Costly depending on distance to PoP or datacentre
- Can have multiple providers for failover

WAN strategies

VDN

192

 Cheaper, but more variable performance depending on provider's networks and other customers

 Harder to troubleshoot and diagnose because of routing or intermediate network issues

Different security paradigm - encrypt everything

SDN (Software-defined networking)

Programmable networking, e.g. routers with APIs

 Just like virtual machines, physical networks can host multiple virtual networks

 Two components, overlay (virtual network), and underlay (physical or core network). Underlay usually Clos/Spine-Leaf for consistency and cost savings

the first of the second second

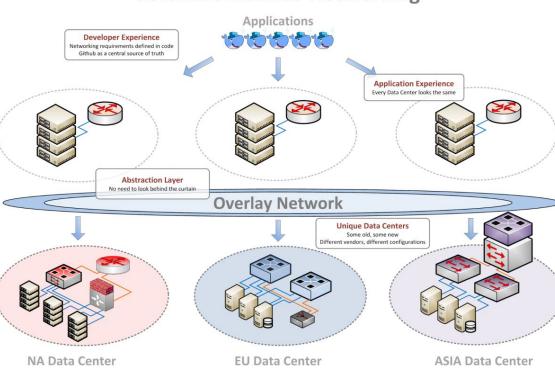
SDN

1000 AD 1100 A

a.b) (return.c.e

www.lilitelse.if(c.a

#.fm.e.extend e.fn.ext



Software Defined Networking

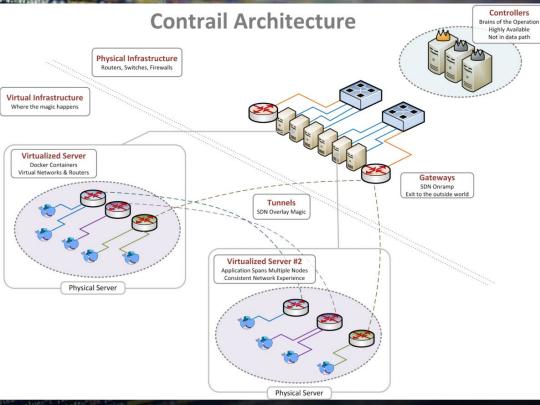
https://engineering.riotgames.com/news/running-online-services-riot-part-iji

- SDN

eners de file a

dates (in the Condition of the Condition

interview condition is a selector i = bG.(this interview condition (a,b) {return. a, each(this (comply (this, arguments), "slice", G. reterview condition (a,b) {return. a, each(this (there of the sector), "slice", G. (the sector), "slice the sector), "slice (the sector), "slice the sector), "sector," (the sector), "slice the sector), "slice sector), "slice the



https://engineering.riotgames.com/news/running-online-services-riot-part-ii

Gaffer , C C Queue , h C'mark , i f.dttle

– Summary

• Network engineers, usually responsible for layers 1-3

• System administrators, usually layers 3-7

• Developers, usually layers 6-7

 Physical networks are messy, logical is usually where you will spend most time designing, and working

definition is interesting to the second second

a.b) (return.c.each(t e}.isReady:



<u>http://royal.pingdom.com/2008/01/09/the-worst-cable-mess-ever/</u>