6.1 Link Aggregation:

Multiple links between two switches. Put more physical links into one logical link. Can be used in enterprise network. Two modes:

1. Manual Mode

=interface Eth-trunk 1

=interface GigabitEthernet0/0/1

=eth-trunk 1

=interface GigabitEthernet0/0/2

=eth-trunk 1

For layer3 (router) :

=undo portswitch

=ip address .. .

=display interface eth-trunk 1

1. LACP Mode-> Link aggresgation control protocol. Negotiate using LACP protocol. If three physical links. Two will be acive. One will be backup.

All the links must have same speed

6.2 VLAN Principal: Devide end points in separate broadcast domains in the same network

VLAN Ethernet frame;(Tagged)

|DMAC|SMAC|TAG|TYPE|DATA|FCS

TAG ->

TPID(2b, 0x8100) | PCP | DEI | VLAN ID(2b)

In hybrid system : whe should configure three: Tagged, untagged, pvid(port vlan id)

Assignment method -> Port based, mac, ip, protocol, policy based (combining all )…

=vlan 10 , =vlan batch 2 to 3

=display vlan

=interface …

=port link-type trunk/access

\*\*

=vlan 2

=port GigabitEthernet….

\*\*

=Interface

=port default vlan 3

=port trunk allow-pass vlan 2 3

=port link-type hybrid

=port hybrid pvid vlan 3 //untagged receiving will be for vlan 3

=port hybrid untagged vlan 3 // sending

Configurign hybrid interface :

=Port link-type hybrid

=port hybrid untagged vlan 2 to 3 // remove the tags before sending to host

Voice vlan => higher priority

=vlan 2

=interface …

=voice-vlan 2 enable

=voice-vlan mode auto

=quit

=voice-vlan mac-address (mac) mask (mask)

6.3: InterVLAN Routing:

Communicating between differerent VLAN. Ways:

1. External router
2. Layer 3 switched

Between switch and router, multiple logical links but one physical link. Called single arm routing

Switch-host : access link

Switch-router : Trunk link

On switch two vlans.

Router:

=interface GigabitEthernet0/0/1.1

=dot1q termination vid 2

=ip address 192.168.2.254 24

=arp broadcast enable

=interface GigabitEthernet 0/0/1.2

=dot1q termination vid 3

=ip address 192.168.3.254 24

=arp broadcast enable

Layer 3 switch = switch + router

=interface vlanif 2

=ip address 192.168.2.254 24

=interface vlanif 3

=ip address 192.168.3.254 24

7.1 HDLC AND PPP: WideArea network

In LAN : Ethernet, In WAN : HDLC, PPP

Serial Signaling:

Async: 1 byte per signal. Every byte has a start and a stop bit

Sync: |Flag|Data|Flag

DCE(Data circuit terminating equipment) -> DTE (Data Terminal Equipment)

|Flag|Address|Control(Type of the frame -> Information(Huawei))|Information|FCS|Flag(Stop)

Types of frames(Control):

1. I (Information)
2. S (Superversory)
3. U(Unnumbered)

= interface serial 1/0/0

=link protocol hdlc

= ip address (ip)

\*

=ip address unnumbered intaface loopback 0

PPP protocol(Point to point protocol)

Components:

1. PPP Encapsulation method
2. LCP -> Link control protocol (Data link )
3. NCP -> Netwrok control protocol. (used for negotiating)

Frame:

|Flag|address|Control|Protcol|Information|Flags

Information -> LCS-> |Code|Identifier|Length|Data

Data -> LCP Configuration Option format -> |Type|length|Data|

LCP Negotiation packet types:

1. Configure Request
2. Ack
3. Nak. Recognized all parameters but not accept
4. Reject. Not recognized all parameteres

Parameter for LCP negotiation:

1. Maximum receive unit default(1500)
2. Authentication protocol. Default(No auth)
3. Magic number. Default(Enable) -> to loop detection

=Interface serial ..

=link-protocol ppp

=ip address ….

Authentication mode ->

1. PAP (plaintext)
2. CHAP. (Challenge, Response, Success/faulre). MD5 calculation is used

IPCL is NCP for configuring IP(Static address negotiation): Help to dynamically assign ip address

Authonticator:

=loca-user (user) password cipher (pass)

=local-user (user) service type ppp

=interface serial ..

=link protocol ppp

=ppp authentication mode pap

=ip address (ip)

Authenticated:

=Interface serial …

=link-protocol ppp

=ppp pap local-user (user) password cipher (pass)

=ip address (ip)

=debugging ppp pap all

7.2 PPPOe

PPPoe = PPP(has authentication) + Ethernet(faster)

Host-> Router -> DSL Model -> DSLAM -> PPPoe Server

PPPoe packets:

1. PADI-> initiation (Broadcast)
2. PADO-> discovery offer (Unicast)
3. PADR -> Active Directory session request(unicast)
4. PADS -> Actove directory session confirmed
5. PADT -> Discovery terminate

Packet size negotiation

Ethernet| PPP|PPPoe|IP|TCP|Data|FCS|

Dialar interface:

=dialer rule

=dialer rule 1 ip permit

=quit

=interface dialer 1

=dialer user enterprise

=dialer-group 1

=dialer bundle 1 (to link physical and the logical interface)

=ppp chap user (use)

=ppp chap password cipher (pass)

=ip address ppp-negotiate

=Interface Gigabitethernaet 0/0/1

=pppoe-client dial-bundle-number 1 on-demand

=quit

=ip route static 0.0.0.0 0 dialer 1

8.1 -> Address Translation

Ipv6 length = 128 bits

Static NAT, dynamic NAT -> Both are one to one translation

Port translation, Easy IP -> no need to multiple public ip address/port

Static conf:

=interface GigabitEthernet 0/0/1

=ip address (ip of the inside host)

=interface serial

=nat static global (outgoing ip) inside (inside ip)

Dynamic conf:

=Nat address-group 1 (public ip 1) (public ip 2) // ip from ip1 to ip2

=Acl 2000

=rule 5 permit source (private network) (subnet)

=quit

=interface serial

=nat outbound 2000 address-group 1 no-pat

Easy IP:

=Acl 2000

=rule 5 permit source (private network) (subnet)

=quit

=interface serial

=nat outbound 2000

For server:

=interface GigabitEthernet 0/0/1

=ip address (ip of the inside host)

=interface serial

=nat server protocol tcp global (outgoing ip) www inside (inside ip) (inside port)

PAT => PORT address translation

8.2 ACL (Access control list)

Used to filter routes

|  |  |  |
| --- | --- | --- |
| Type | Ranges | Parameter |
| Basic | 2000-2999 | Source IP |
| Advanced | 3000-3999 | Source des ip. Protocol, port |
| L2 ACL | 4000-4999 | MAC |

=ACL 2000

=rule 5 deny source (ip) (mask)

=rule 10 permit source any

Conventions -> rule gap should be 5

=interface GigabitEthernet 0/0/0

=traffic-filter acl outbound 2000

=display acl 2000

Advanced ->

=acl 3000

=rule deny tcp source (source ip) (source sub) (dest ip) (deest sub) destination-port eq 21

8.3 AAA (Authentication, Authorization, Accounting)

Protocols : RADIUS, HWTACAS

Authentication -> On a router NAS(Network access server)-> some username and password

Authorization -> group based roles

Device group(public, private) -> User group(Admin, staff) -> time -> privilege

Accounting a user -> Login time, up time, username, upload/download speed

AAA domains -> help to manage user/groups

=local-user (name) password cipher (pw)

=authentication-scheme auth1

=authentication-mode local

=quit

=authorization-scheme auth2

=authorization-mode local

=domain (name)

= authentication-scheme auth2

= authorization-scheme auth2

8.4 IPSec VPN.

TCP/IP protocol doesnot ensure security

Ipsec tunnel between enterprise branch and headquarter. Internet is not secure

Ipsec vpn is an architecture

Combination of two protocols:

AH(Authentication Header) => MD5, SHA1, SHA2

Encryption => DES, 3DES, AES

ESP => Auth+encry

(SA)Security association => Local address, remote address, SPI inbound/outbound, key , proposal

Encapsulation mode =>

1. Transport

AH:

IP|AH|TCP|DATA

ESP:

IP|ESP|TCP|DATA|ESP TRAILER|ESP AUTH => IP is not authenticated

AH+ ESP => All is authenticated

1. Tunnel -> new IP header. If we want to hide from the internet

Vpn establishment

Ensure reachability => Identify interesting traffic (ACL) => ipsec proposal (ACL + proposal together) => Create ipsec policy => apply policy to interface

=ip route static … .

=acl 3000

=rule 5 permit ip source (source)

=ipsec proposal tran1

=esp authentication-algorithm sha1

// default mode tunnel

=ipsec policy P1 10 manual

=security acl 3000

=proposal tran1

=tunnel remote (ip)

=tunnel local (ip)

=sa spi outbound esp 54321

=sa spi inbound esp 12344

=sa string key outbound esp simple Huawei

=sa string key inbound esp simple huawei

\*

=interface …

=ipsec policy P1

ACL => match accept/deny. Otherwise normally forward without encryption

8.5 GRE(Generic routing encapsulating) VPN

Problem with ipsec is -> unable to multicast (site to ite), only allow static route

Multicast protocol -> OSPF, video

GRE protocol to encapsulate multicast packet.

Ipsec -> encrypt + auth

GRE help to extend hops.

RIP has limitation of hops. Max 16

IPsec over gre or gre over ipsec

GRE -> |DATALINK|IP|GRE header(has optional key)|IP/IPX|Payload|

=interface tunnel 0/0/1

=ip address 40.1.1.1 24

=tunnel-protocol gre

=source (ip)

=destination (ip)

=quit

=ip route static (ip) tunnel 0/0/1

=keepalive period 3

9.1 SNMP -> Simple network management protocol -> monitor

Communication between NPM(Network managementstation) and devices

NMS like a software on the server

3 versions:

1. V1. Has trap(UDP port : 162)
2. V2c: getbulk request. One request all info
3. V3 : more secured

=snmp-agent

=snmp-agent sys-info version v2c

=snmp-agent trap enable

=snmp-agent trap source GigabitEthernet 0/0/1

10.1 IPv6

IPV6 header format:

|version|traffic class |flow level|

|payload length|next header|hop limit|

Source address

Destination address

Extension header can be used. Which will not be required for every packet -> Fragment, Ipsec

Larger ipv6 can be condensed into smaller ones by using double colon

2000::/3 -> global internet

FE80::/10 -> link local unicast address

FF00::/8 -> multicast

Global unicast

Globa routing prefix(48) susubnet id(16) interface id(64)

Link local

(1111111010) (10 bits) (0) (54 bits) interface id(64)

Multicast

1(8 bit) flags(4 bits) scope (4 bits) group id(112 bits)

FF02::1 -> All nodes, FF02::2 -> All routers

Anycast:

Same IP for 2 servers. One server is down, another is backup

No need for DHCP -> Stateless address auto configuration

Router solicitation(client) -> RA(Router Advertisement -> Sending prefix of the network)(Router)

Interface id generator -> Prefix from MAX(24 bits, 7th bit = 1) || FFFE( 16 bits) || suffix from mac

DAD -> Duplicate address detection

NS(Neighbour Solicitation) -> Neighbour Advertisement => To check supplicate IP

10.2 IPV6 routing -> RIPng , OSPF v3 , ISIS, BGP4+

If more hosts in the same link are neighbours. No need to be in same network. Router id must be configured manually (OSPF 3)

For authentication -> IPV6 extention header (OSPF 3)

=ipv6

=ospfv3

=ipv6 enable

=ipv6 address fe80::1 link-local

=ospfv3 1 area 0.0.0.0

=ipv6 enable

=ipv6 address 2001:1::1/64

=ospfv3 1 area 0.0.0.0

10.3 DHCPv6

To get an IP ->

1. Stateless addresss auto configuration
2. DHCPv6 (stateful -> all the parameters are obtained along with)

Use UDP port 547(server), 546(client) to communicate

Client -> RS -> router -> RA(Router Advertisement)(if M = 1 && O = 1 use DHCP) -> client

Client will use linklocal address to communicate with DHCP server

If the client and server are not on the same link, use DHCP relay

FF02::1:2 this maulticast address will be used for all the DHCP servers and relays

Client -> Solicit (request ) -> Server -> Advertisement (address, dns, other params)-> Client ->

DUID -> DHCP Unique Identifier. Each host and server has unique ID.

To get DUID, 2 ways -> 1. LL(Link layer) 2. LLT(Link layer Timestamp)

=dhcpv6 duid ll

=dhcpv6 pool pool1

=address prefix 3000::/64

=excluded-address 3000:1/64

=dns-server 3000::1/64

=dns-domain-name Huawei.com

\*

=ipv6

=dhcp enable

=interface …

=ipv6 address 3000::1/64

=dhcpv6 server pool1

11.1 MPLS Basic Priniciple: Multiprotocol Label Swithing -> to speed up the data forwarding.

Two plan :

1. Control plan
2. Forwarding plan(Data plan)

ATM -> Asynchronous transfer mode

MPLS => Ip forward + ATM -> You don’t need to check IP header

Only to check label table and forward data

First router = ingress. Last router = egress

Companies purchase MPLS vpn from ISP

MPLS TE -> Traffic engine -> Control traffic to make a balance

LER => Label Edge router => First and the last router

LSR => Label Switch router => routers in the middle

LSP => Label switch Path => Tunnel

Control Plan :

1. Routing protocol => to learn and build ip routing table
2. IP Routing Table => help to build IP Forwarding table, in egress
3. Label distribution protocol => to build label forwarding table

Data plan:

1. IP Forwarding table => if doesn’t need to go tunnel
2. Label forwarding table

Layer 2 frame mode encupsaltion:

Frame Header | MPLS Header | IP Header | Payload

MPLS Header (32 bits):

Label | EXP | S | TTL

if S == 1 => Bottom of the stack. Pop

Forwarding process:

1. FESC: Forwarding Equivalence class => group by same destination
2. NHLFE:Next hop label forwarding entry => 3 oparation:
   1. Push -> Ingress
   2. Pop -> Egress
   3. Swap -> Middle

=display mpls lsp include 10.2.0.0 24 verbose

ILM => Incoming label map

11.2 : SR Basic principal : Segment Routing

LDP is a protocol to distribute label in MPLS

LDP uses local label switching -> problem

LDP has 11 type of protocol package. Which is slow and consume lot cpu. Only support shortest IGP Path, TE is not supported

RSVP is better -> 8 types packets -> consume cpu -> for load balancing a lot of work. Has to configure individually

Traditional network -> control + Forwarding -> high bandwidth

Revolutionary SDN Network -> Control(High performance) is separated in another hardware. Router only do the forwarding. Not compatable with existing

Incremental SDN Network: Controller have some part of control plans. Mix of traditional and revolutionary

11.3 : SR:

SR Domain : Set of nodes

Segment : Node, prefix(destination), adjacent

SID -> Segment ID

SRGB -> Segment Routing Global Block: Pool of segment ID

Segment List : Sorted SID, prefix SID, adjacent SID

SID and node ID are different. SID means Segment id. The id of link between two routers

Node id is the id of a router.

Forwarding technology can be based on node id, segment id or both.

To learn SID and node ID they use IS-IS

BGP LP collects all the SIDs to the controller

Controller uses PCEP technology to calculate the path from source to dest

Controller uses NETCONF too provide calculation to source

SR\_TE : Strict explicit path. Where source knows full path from source to dest

Loos explicit path : not all the node/segment in the destination path is mentioned. Use IGP to calculate the not-mentioned node.