Campus High availability network - LAN
Construction of a Network with high Usability is one Kind of System Engineering

Construction of a network with high usability is a system engineering which requires full consideration of network structure, security, management, optimization and so on:

Ø In network planning stage, there is need to carefully analyze the user requirements and service pattern, pinpointing networks usability’s biggest effect on key points and connections

Ø In the network design stage, needs reasonably to plan the network architecture, provide redundancy design to the important connection points and links, uses the high usability technology, and give enough attention to the network security

Ø In network deployment stage, there is need to pay attention to the equipment software and hardware quality and the link quality

Ø After the network construction is completed, in maintenance stage, there is also need to use the appropriate network management tools to provide analysis for the network service traffic flow, and unceasingly optimized network, the improving the network usability level

Ø Moreover when doing the software and hardware edition upgrade and the new service deployment, it is needed to have a detailed plan beforehand, and prepare for emergency measures.
**Agenda**

- Enterprise network solution design guideline
- Recommend enterprise network design module
- Best practice for high availability network design
- Case study
Challenges for Enterprise Networks

How to manage/operate/control the network equipments located in different sites?

How to make easy network expansion without any network interruption? Upgrading to IPv6 network smoothly?

How to avoid single failure on the networks?

How to conciliate the different application with QOS technology? How to ensure the critical applications?

How to improve working efficiency in lowest TCO?
Best practice for network design

- Redundancy
  - No single point of failure
  - Load balance
Best practice for network design

Hierarchy

- Optimized network structure
- Strictly defined functions of each layer
- Easy and clear management
- Efficient troubleshooting
Best practice for network design

- Modularization
  - Convenient maintenance
  - Ease to scale
  - Confinement of failure area
Best practice for high availability design

Intranet/branch
- Internet
- WAN

Core
- S9500
- S7500

Aggregation
- S7500
- S5600

Access
- S5600
- S3610
- S5100
- S3100

IRF stack
- Star link
- Layer 3 to Desktop
- GE to Desktop

MS center
- Server farm
- IDC
Agenda

- Enterprise network solution design formula
- Recommend enterprise network design module
- Best practice for high availability network design
- Case study
Network Design Best Recommendations—Layer 3 to Desktop

Intranet/branch

Core layer

Aggregation

Access

Application

Full Layer 3 Network

Intrernet/branch

WAN

IDC

S3600

S7500

S9500

OSPF

Fast convergence of network failure

Through ECMP and redundancy you can realize load sharing and thus increase network usability

OSPF protocol for the entire Network, no need for layer 2 protocol, simplified configuration management

Broadcast domain is confined to the access ports, upper layers are not affected

Fast convergence of network failure

Test flow 1

Test flow 2

Tester

Tester
## Test Results

<table>
<thead>
<tr>
<th>Network Failure</th>
<th>Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access-Aggregation/Aggregation-Core Link failure/recovery</td>
<td>500ms</td>
</tr>
<tr>
<td>Aggregation Layer Equipment Failure</td>
<td>1sec</td>
</tr>
<tr>
<td>Core Layer Equipment Failure/ restart</td>
<td>1sec</td>
</tr>
<tr>
<td>Aggregation Layer dual MCU interchange</td>
<td>200ms</td>
</tr>
<tr>
<td>Aggregation link group failure/Recovery</td>
<td>&lt;1sec</td>
</tr>
<tr>
<td>Loading Hot patches to fix bugs</td>
<td>0</td>
</tr>
</tbody>
</table>

L3 to desktop

Detail test entries
Summary

• Redundancy link, nodes, devices, dual home design and real-time backup mechanism
• Triangle loop design and easy deployed ECMP
• Config OSPF correctly parameters such as LSA interval, interface linkdown interval, address distribute
• Propose L3 link connect between aggregation devices and config route entries summary and accelerate route entries convergence
• For small campus network(<50 nodes), only one OSPF area is enough, simplified configuration and ECMP support load balance
• For big campus network, deployed separate areas, deployed area 0 between core layer and aggregation layer. The aggregation device config as ABR, config NSSA area between access layer and aggregation layer
• Delivery route entries summary and route entries filter technology to limitation route entries
• OSPF deployed to access switch and deployed load balance with ECMP
• OSPF Area architecture support route summary and isolate failure areas
• Access switch deployed QOS technology and access policy improve LAN security
Network design best recommendation– L2 Access MSTP+VRRP

- **Internet**
- **WAN**
- **IDC**

**Core layer**
- MSTP prevents L2 loops while supporting link load sharing

**Aggregation**
- OSPF
- **VRRP**
  - VRRP master
  - STP root
  - VRRP backup
- S7500
- S9500

**Access**
- Access Equipment have low L3 functions requirements, price is relatively lower
- Can use VLAN for layer 2 user isolation, VLAN members communication is convenient
- Test flow 1
- Test flow 2

**Application**
- Tester
- Tester

**VLAN 10**
- VLAN 20
Network Design Best Recommendations-Layer 2 deployment

- VLAN
- MSTP
- VRRP
- Loop back-detection
- BPDU Guard
- STP edge port

- MAC and ARP limit
- STP Root guard
- Broadcast storm control
- Dual home connected
- DLDP
## Test Result

<table>
<thead>
<tr>
<th>Network Failure</th>
<th>Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access-Aggregation link failure/Recovery</td>
<td>&lt;1sec</td>
</tr>
<tr>
<td>Aggregation Layer equipment failure</td>
<td>3sec</td>
</tr>
<tr>
<td>Aggregation layer equipment switchover to the main equipment</td>
<td>500ms</td>
</tr>
<tr>
<td>Aggregation layer-core layer link failure/recovery</td>
<td>&lt;1s</td>
</tr>
<tr>
<td>Core layer equipment failure</td>
<td>&lt;1s</td>
</tr>
<tr>
<td>Single Link failure (start DLDp)</td>
<td>2s</td>
</tr>
</tbody>
</table>

**VRRP and MSTP**

**Detail test entries**
Summary

• Redundancy and trunk link
• Chassis switch full redundancy
• Deployed OSPF on aggregation and core layer
• Deployed STP and VRRP on access and aggregation device
• Access switch deployed secure and control policy improve LAN security
• DLDP detect link states
Network Design Best Recommendations-3 – Access and Aggregation IRF

- **Intranet/branch**
  - IRF allows easy expansion and has cost advantage compared to box type equipment.

- **Core layer**
  - 10G RPR provides 50ms failure recovery guarantee.
  - Distributed link aggregation provides load balancing between the equipment, and assures link failure protection.

- **Aggregation**
  - IRF access provides high access port density and load sharing, and simplified management.
  - Distributed forwarding mechanism improves forwarding capacity.

- **Access**
  - OSPF

- **Application**
  - Test flow 1
  - Test flow 2

- **Tester**
## Test results

<table>
<thead>
<tr>
<th>Network Failure</th>
<th>Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Stack group: single switch Addition/removal</td>
<td>&lt;1s</td>
</tr>
<tr>
<td>Access Stack group single equipment failure</td>
<td>&lt;5s</td>
</tr>
<tr>
<td>Access-Aggregation Stack group internal single link failure/recovery</td>
<td>&lt;300ms</td>
</tr>
<tr>
<td>Aggregation-core stack group internal single link failure/recovery</td>
<td>&lt;500ms</td>
</tr>
<tr>
<td>Core layer equipment failure</td>
<td>1s</td>
</tr>
</tbody>
</table>

### Detail test entries

IRF
Summary

• Deployed to campus or university network
• Ringed stack connect every devices
• Deployed OSPF to access layer
• Uplink use DLA to support availability uplink
• Stacked switch can support unitive upgrade as one chassis device
• Access switch deployed QOS technology and access policy improve LAN security
Network Design Best Recommendations IV – L3 Gigabit to Desktop

Entire Network cost is relatively high, satisfies many service types’ non-blocking switching.

Many kinds of broads within Chassis device.

Flat L2 network architecture, easy configuration and management.

Gigabit L3 access, can satisfy every service bandwidth requirements.

Entire Network cost is relatively high, satisfies many service types’ non-blocking switching.

Test flow 1
Test flow 2

Application
Intranet/branch
Core layer
Access

Tester
Tester

Internet
WAN
IDC
### Test Result

<table>
<thead>
<tr>
<th>Network Failure</th>
<th>Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access –Core layer link failure/recovery</td>
<td>&lt;700ms</td>
</tr>
<tr>
<td>Core layer equipment failure</td>
<td>&lt;700ms</td>
</tr>
<tr>
<td>Core layer equipment reboot</td>
<td>&lt;1s</td>
</tr>
<tr>
<td>Core layer equipment main control broad switch over</td>
<td>&lt;50ms</td>
</tr>
</tbody>
</table>

Detail test entries

2 layer high bandwidth
Summary

- Deployed to high throughput, shorten latency, fast forwarding requirements environment.
- Chassis switch full redundancy with abundant interfaces and broad.
- Flat network and OSPF deployed to whole network
- 2 Layer architecture and fast convergence
- Easy deployed, management, scale
- Access switch deployed QOS technology and access policy improve LAN security
Agenda

- Enterprise network solution design formula
- Recommend enterprise network design module
- Best practice for high availability network design
- Case study
Best practice technology recommendation 1
- Right redundant design

Aggregation and core device commend hot standby design and dual uplink.

Complex redundant design will waste more links resource and bring routing protocol calculate complexity.
Best practice technology recommendation 2 – Ethernet link trunk

Benefit for link trunk

- **improve bandwidth**
  - 4 link looked like 1 link

- **traffic load balance within consists of links**

- **links backup each other, improve availability**

Fault recovery within 500ms
Best practice technology recommendation 3 – ECMP (Equal Cost Multi Path)

Device load balance at L2-L3 traffic to avoid drop packets on single link when deployed ECMP.
Best practice technology recommendation 4 - GR (Graceful Restart)

Separated control panel and forwarding panel
OSPF GR/RFC 4167, ISIS GR/RFC 3847, LDP GR/RFC 3036
BGP GR / draft……
Best practice technology recommendation 5 -
- Virtual Router Redundancy Protocol

- Configure several VRRP groups, load balance the traffic.
- By adjusting the network node priority, VRRP master node can be controlled.
- Set hello packet interval on the master for shorten switch time.
- The device keep traffic stability and avoid unnecessary broken within un-occupy model.
- The device avoid frequently switch through config delay interval in occupy model.
- Config uplink monitor is commended.
Best practice technology recommendation 6 – detect one way communication

DLD--Device Link Detection Protocol

Normal Condition, through Hello\Echo packet exchange build the neighboring relation between equipments.

When the port R fails, can not receive signal, it goes down at once.

Device sent announce a special DLD packet after port unable. The opposite port receive the packet and then DLD down.

DLD detect within 2 seconds!
Best practice technology recommendation 7 – Hot patch function.

Without reset device, fixed software bugs and upgrade software version. Administrator control fixed processing through Load/Active/Deactive/Run/Delete commands.
Best practice technology recommendation 8 -- Smart Link

Smart Link, L2 protocol, shift and recover within 200 ms

Smart Link: L2 protocol, shift and recover within 200 ms

- Redundant uplink group with port 1 and port 2
- Port 1 forwarding packets and port 2 backup in generally.
- Port shift and forwarding packets with 200ms when port 1 unable.

Smart Link + Monitor Link:
- Private technology
- Down link change to down state when uplink down.
- Cooperative between up device port and down device.
Best practice technology 9 -- Intelligent Resilient Framework

IRF
(Intelligent Resilient Framework)

Advantage of IRF technology
- High reliability, reduce single point failure effect.
- High performance,
- Distributed L2/L3 protocol processing.
- High management configuration, works like a Fabric
- One time software upgrade inside the stacked group.
- Hot swappable
IRF - Recommend ring stack

Recommend ring stacking to improve availability and load sharing with stack cable.

String stacking easy bring single failure when the single stack cable failed.
Best practice technology recommendation 10–Resilient Packet Ring

Mid & Small campus network – recommended dual core backup model

Large campus & high reliable network- RPR core ring network group.
RPR (Resilient Packet Ring) is a kind of hardware-based protection ring technology.

**Characteristic:**
- Reversed dual-ring topology
- Internal and external ring can transmit data frame and control frame
- Internal and external control frame contain data frame control information from different ring

**Advantage:**
- Hardware fast protection, recovery time <50ms
- Work in physical layer, compatible to upper layer protocol
- Plug and play, outstanding expansibility
- Fairness algorithm increase bandwidth utilization
- QoS guarantee
Best practice technology recommendation 11 – RRPP

In the ring network condition, through the complete software innovation realization H3C proposed RRPP (Rapid Ring protection Protocol) technology.

- RRPP ring
- RRPP control VLAN
- Main node, Transition node
- Main port, slave node
- Polling mechanism
- Notice mechanism for link state change
- Failure recovery mechanism
Agenda

- Enterprise network solution design formula
- Recommend enterprise network design module
- Best practice for high availability network design
- Case study
ICBC is PRC’s biggest state-owned commercial bank, with 18,000 business networks, 100 overseas branches and thousands of agents all over the world.

ICBC has 2 data centers, the data centre in Shanghai is for processing and operation, the one in Beijing is for backup and recovery. In 2005, a first level branch data centre was established in each province to realize province to headquarters data centralization. The first level branch data centre consolidates the whole province’s access services servers, OA servers, aggregation service platform, gateway platform, etc, with high requirements for performance, reliability, service segregation and security. H3C has constructed 18 of the provincial data centres.
The project deployed S9512, S7500 and S5624P switches and AR46 routers.
S5624P supports IRF and PoE.
University of Malaya is a most renowned university in Malaysia. The university applies technology to drive the studies and management to create a first-class teaching environment.

H3C solutions not only can satisfy the requirements for converged network for Voice and Video over IP, but also offer rich functionalities and security. The backbone network migrated seamlessly from 155Mbps to 10GE, giving many new applications and hotspots for the 750-acre campus.
25 S3628EIs are deployed at the office level to provide access for PC and IP phones, providing PoE for the IP phones.

IRF stacking technology is used to provide resiliency, performance and expandability for the network access.

Voice VLAN functions provide high quality of service for voice calls.