LECTURE 5: Open Shortest Path First
Guest lecture by Dr. Mukul Goyal
DATE: wed, 06,August, 2003, Notes by P. Pallavi

TOPIC: Current research directions in OSPF

Introduction:

OSPF:

1. OSPF stands for Open Shortest Path First
2. OSPF is an interior Gateway Routing Protocol.This means that "it is used for finding routing with in an autonomous system"
3. It is basically a link-state routing protocols
4. It works in three stages

Sending hello packets for finding adjacencies

Flooding Link State Advertisement (LSA)

Synchronization of Link State Database and shortest path calculation

## CURRENT RESEARCH DIRECTIONS IN "OSPF" :

1. Fast convergence to topology changes in OSPF protocol
2. Traffic engineering with OSPF
3. Graceful restart

Fast convergence to topology changes in OSPF protocol:

Convergence process: This is defined as detecting the topology change as early as possible and make the routing table adapt to the new topological changes. So the steps are

1) Detecting topology change
2) Generate LSAs
3) Flooding the LSAs through out the network.
4) SPF calculations on receiving the new LSAs

When we call a topology change?

1. If a router comes up or
2. If a router goes down or
3. If a link is established or
4. If a link is broken

Detecting topology change:

In topology changes, good events (router comes up or link establishment etc) do not cause any problem. So good events can wait. But bad events must be detected fast. There are two techniques for fast detection.

Hello protocol

Hardware detection

Hello protocol:

It is a default technique.

In this technique, we use a parameter called router dead interval that is 3 or 4 multiples of hello interval. If a router doesn't receives a hello message from a router with in this dead interval then it assumes that the router is dead.

Drawback of using hello protocol for failure detection is that the router has to wait for a long time to check for a failure.normally, The dead interval time is in between 30 to 40 ms, which is a problem in VoIP.

1) We can decrease the router dead interval time. But the problem with this is cause of " False Alarms".

False alarms: Suppose we decreased dead interval time to milli seconds range. Then if the packet arrives just after the dead interval time because of congestion in network. Then the router is assumed to be down causing a false alarm and this process goes on causing a global catastrophe.

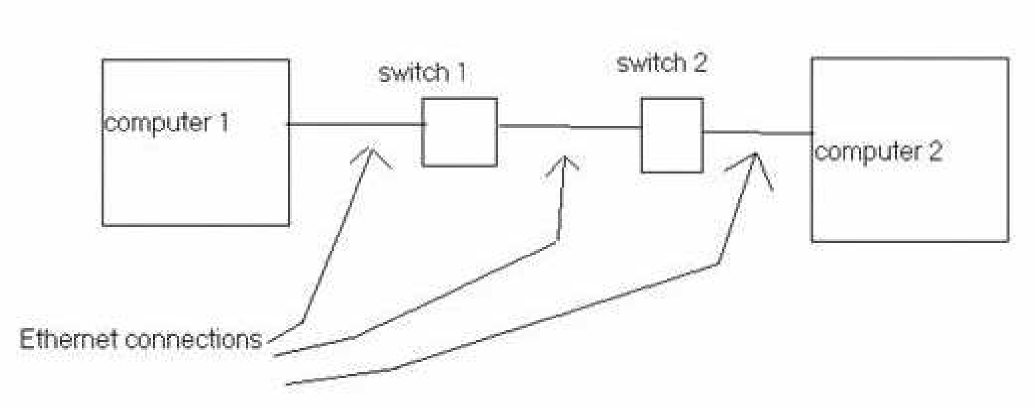
This can be avoided if the hello packets are prioritized.

2) The other alternative is to minimize the hello interval time. But, The hello protocol has to do many works like forming adjacencies along with failure detection. So, it is too complicated.so,it is better to use a light weight protocol dedicated to failure detection. This protocol is called " Heart beat protocol"

Heart beat protocol: In this, small packets are transmitted frequently across neighbors. To further reduce the hello/heart beat protocol interval, we can use line cards to process them. so OSPF process don't bother about them. But it has a drawback that the OSPF process and line cards are independent.so,it may continue its work even when the OSPF process crashes.

Hardware Detection: In this, lower level protocols indicate the failure to the OSPF process. Eg:Optical links

But hardware detection is not always possible. For eg: if two systems are connected by an Ethernet connection that contains two switches in between them as shown below.



Then it is not possible to detect a failure if the link between switch1 and computer1 fails.

LSA Generation:
A router has to generate LSA as fast as possible. But, no router can generate an LSA faster than a second.
Flooding LSAs:
LSA flooding is reliable. It means that a router that receives a LSA sends an acknowledgement. But, The bad implementation in OSPF is that, a router floods only after calculating SPF.eg: Cisco routers forward 1 LS update packet per 30ms.
If there is a loss of LSA, the LSA s are retransmitted only after 5 sec.so there are two techniques to optimize the flooding

Intelligent flooding

Flooding handled by line cards.

SPF calculations on receiving new LSAs: SPF calculation consumes more time. Two parameters are used here.

1. SPF Delay
2. SPF hold time

SPF delay: It is the delay between first new LSA and the resulting SPF calculation. It is normally 5 seconds.
SPF hold time: It is the delay between successive SPF calculations. It is normally 10 seconds in Cisco routers.

It is better to take SPF hold time larger if there are frequent changes. But if there are no changes then it is better to make SPF hold time less.so, what we have to do is initially take SPF hold time as less value and keep on doubling the value if there are frequent changes till its value equal to 10 ms.
SPF calculation time (According to Dijkstra’s algorithm) = O(L logN)
Log is of base 2
Where L=Number of links
N=Number of nodes
Let us take some examples to find the impact of network topology on convergence process.

Full mesh N*N

Then SPF calculation time N*N logN

Where log is of base 2.
Partial mesh 10*N

Then SPF calculation time 10*N*log N

Where log is of base 2.

It is better to use incremental SPF technique to minimize the convergence process time.

Traffic engineering with OSPF:It is defined as performance optimization of operational networks with the main focus on minimizing over-utilization of capacity when other capacity is available in the network.
The question is " can we achieve traffic engineering goals with OSPF?"
The answer is to some extent.
Type 10 opaque LSA contains the following TE information regarding different links.

Traffic engineering metric

Maximum bandwidth

Maximum reserved bandwidth

Unreserved bandwidth

Administrative group

Generation of new TE LSAs not be more frequent than 1 per 5 sec
Graceful Restart:

Graceful restart is very important when a router went temporary down because of some hardware or software upgrade. In this case it is better to have routing and forwarding processes separately. So that the routing process can tell all routers that it is going down for few amount of time and it will come back soon. Then the forwarding process may be allowed to forward data provided that there are no loops or back holes.

-