Network Maintenance (Network Separation and Merging)

Topics :

Define scenario  
Define problem  
Design scheme  
Documentation (ppt, doc)

Ref:

Acm communication

Ac computing

iEEE computing & communication

Then there are packet shapers which are centred on providing visibility, control, and acceleration. Visibility, so that you are able to see everything on the network -- revealing the source of any network problems; control, to set policies that reflect priorities; and acceleration of the performance in which data is delivered -- done by compression.

**Advanced Discovery**  
Network monitoring and troubleshooting products discover devices by monitoring traffic and by actively querying hosts. Once discovered, they usually provide the most thorough information possible in terms of: DNS name, NetBIOS name, SNMP name, IPX name, and address.

Real-time remote monitoring and problem discovery makes it easy and economical to extend your knowledge and expertise across your network. Some software uses a Web browser interface to monitor distant sites directly from your desktop. With some products you can run multiple sessions at any one time.

**Reporting Software**  
This is an important consideration. Reporter software will transform collected network performance data into usable documents. Some software packages can even draw you a map of your entire network. You can document collisions, utilisation, and errors, and publish them in a variety of formats -- including HTML and PDF.

Software maintenance   
Hardware maintenance   
Network maintenance   
Managed services   
Disaster recovery management

Session key management in spontaneous network

First scenario : To find a way to share some different session key  
Find a way to let the application choose user

Second scenario : having 2 networks and merging

- Proposal (problem)

Given the scenario described above, the problem we wish to face is the

management of security issues when two or more spontaneous networks merge

together, and when a spontaneous network is partitioned in two or more groups

of users, each one using its own network. In the case of networking established

using "spontaneous VPN" (i.e. a VPN among nodes, built using a shared session

key), the basic problem is how to manage session keys when two networks merge,

in order to build a new VPN in a transparent way for users and applications,

and how to have independent networks when subsets of users choose to leave the

original network. To provide a full transparency also other aspects, such as

naming, addressing and authentication, have to be considered.

- Scenarios

1. Multiple session key sharing :

Let us say that we have 2 spontaneous network which have their own TEK

(Trafic Encryption Key) used for encrypting all messages in one communication

session. A session key will be chosen randomly for every spontaneous network.

Then every user of the first network is able to decrypt first network communications,

but not second network communications and vice-versa. When the 2 networks will merge,

we have to find a way to share the session keys without loosing in security. Do we create

a new session key ? Do we choose one of the key or do we merge the 2 session keys ?

Normally, key must be distributed securely before encryption can be used in order to get

a secure network. But in this case, communication has already been started before merging

the 2 networks. All these questions and issues will consist on our first scenario and will

need to be brainstorm ...

2. Mutliple spontaneous network merging :

When having two distinct spontaneous network, question is how can we merge these one into

only one network without loosing any information ? Of course, our goal is to recover all the

information of the 2 previous networks like shared folders, communications, data, etc.

- References

Establishing trust in pure ad-hoc networks

Asad Amir Pirzada, Chris McDonald

January 2004 ACSC '04: Proceedings of the 27th Australasian conference on

Computer science - Volume 26 , Volume 26

(ACM Portal)

Spontaneous networks: Trust in a world of equals

Gilaberte, R.L.; Herrero, L.P.;

Networking and Services, 2006. ICNS '06. International conference on

16-18 July 2006 Page(s):42 - 42

(IEEE Xplore)

Friends and foes: preventing selfishness in open mobile ad hoc networks

Miranda, H.; Rodrigues, L.;

Distributed Computing Systems Workshops, 2003. Proceedings. 23rd International

Conference on

19-22 May 2003 Page(s):440 - 445

(IEEE Xplore)

On the design of spontaneous networks using a P2P approach and Bluetooth

Cano, J.; Cano, J.-C.; Manzoni, P.; Ferrandez, D.;

Computers and Communications, 2005. ISCC 2005. Proceedings. 10th IEEE

Symposium on

27-30 June 2005 Page(s):125 - 130

(IEEE Xplore)

Spontaneous networking: an application oriented approach to ad hoc networking

Feeney, L.M.; Ahlgren, B.; Westerlund, A.;

Communications Magazine, IEEE

Volume 39, Issue 6, June 2001 Page(s):176 - 181

(IEEE Xplore)

Security management for ad-hoc networked resource-limited mobile devices

Sedov, I.; Speicher, S.; Cap, C.;

Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th

Volume 5, 26-29 Sept. 2004 Page(s):3262 - 3266 Vol. 5

(IEEE Xplore)

Implicit merging of overlapping spontaneous networks [mobile ad hoc networks]

Legendre, F.; de Amorim, M.D.; Fdida, S.;

Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th

Volume 4, 26-29 Sept. 2004 Page(s):3050 - 3054 Vol. 4

(IEEE Xplore)

Spontnet: experiences in configuring and securing small ad hoc networks

Feeney, L.M.; Ahlgren, B.; Westerlund, A.; Dunkels, A.;

Networked Appliances, 2002. Liverpool. Proceedings. 2002 IEEE 5th International Workshop on

30-31 Oct. 2002 Page(s):102 - 106

(IEEE Xplore)

A multiway merging network

De-Lei Lee, Kenneth E. Batcher

Ref : http://www.springerlink.com/content/f072n85t7q5n6757/

Websites :

http://en.wikipedia.org/wiki/Session\_key

http://en.wikipedia.org/wiki/Session\_%28computer\_science%29

http://www.cytoscape.org/cgi-bin/moin.cgi/Advanced\_Network\_Merge\_and\_ID\_Mapping