Проектирование системы безопасности приватной компьютерной сети

Апанович Денис Алексеевич
Крымский федеральный университет имени В.И. Вернадского
Таврическая академия
факультет математики и информатики
кафедра информатики (группа 602-И)

e-mail: apanovichtatyana@mail.ru

В работе рассматривается задача, которая стоит перед проектировщиком локальной сети, стремящимся уменьшить вероятность блокировки перетоков информации.

1. Виртуальные частные компьютерные сети

Путём замены одного из компьютеров большой («глобальной») компьютерной сети на роутер малой («локальной») компьютерной сети можно получить «подсеть». Рекурсивно можно построить разветвлённый односвязный нециклический граф и получить древовидную топологию. Итак, если роутер звездообразной сети A состоит в сети B, сеть A считается «подсетью» сети B. При этом возможны два подхода:

- IP-адресация участников древовидной сети «сквозная», т. е., каждый участник древовидной сети, независимо от глубины, на которой он находится, виден из корневой сети.

- Участникам подсети A_1 разрешается иметь такие же IP-адреса, как участникам независимой от A_1 подсети A_2. При этом участники подсетей A_1 и A_2 не видны из корневой сети.

В силу ограниченности множества всевозможных IP-адресов, приходится использовать второй подход («виртуальные» подсети). При нём для прокладки пути через маршрутизаторы необходимо грамотно построить таблицы маршрутизации. Основные принципы коммутирования будут изложены в следующем пункте.

2. Коммутационные сети Клоза

Определение 1. *«Матричным коммутатором» размерности — $m \times n$ назовём набор выключателей, коммутрирующих m входов с n выходами. Математической моделью «матричного коммутатора» является бинарная матрица* $\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & & & \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$, *где* $\forall i = \overline{1, m} : \forall j = \overline{1, n} : a_{ij} \in \{0, 1\}$.

Пример «матричного коммутатора» — программируемая микросхема ПЗУ, где каждая точка коммуникации — плавкий предохранитель. При программировании необходимые предохранители программатор прожигает выборочно с помощью высокого напряжения, а при считывании с помощью низкого напряжения можно определить, в какой точке коммуникации какое состояние предохранителя. Легко видеть, что ёмкость такой микросхемы составляет $m \cdot n$ бит:

Утверждение 5. *Количество всевозможных состояний матричного коммутатора размерности $m \times n$ составляет $2^{m \cdot n}$.*

Определение 2. *Кроссбаром (англ. "Crossbar") размерности $m \times n$ назовём «матричный коммутатор» размерности $m \times n$, выполняющий следующие условия:*

- *Запрещается один и тот же вход одновременно подключать к нескольким разным выходам.*
- *Запрещается к одному и тому же выходу одновременно подключать несколько разных входов.*
- *Каждый вход должен иметь возможность подключиться к какому-нибудь выходу. Отсюда следует, что количество входов не должно превышать количество выходов ($m \leq n$).*

Утверждение 6. *Количество всевозможных состояний кроссбара $m \times n$ составляет $\dfrac{n!}{(n-m)!}$ (при условии, что все входы куда-то подключены).*

Определение 3. *Пусть имеется r «входящих» кроссбаров. Каждый имеет размерность $n \times m$. Столько же «исходящих» кроссбаров размерности $m \times n$ (таким образом, имеем $r \cdot n$ входов и столько же выходов). Пусть имеется также m кроссбаров «среднего яруса», каждый из которых имеет размерность $r \times r$. Все эти кроссбары соединим по схеме рис. 1. Полученную сеть назовём «сетью Клоза».*

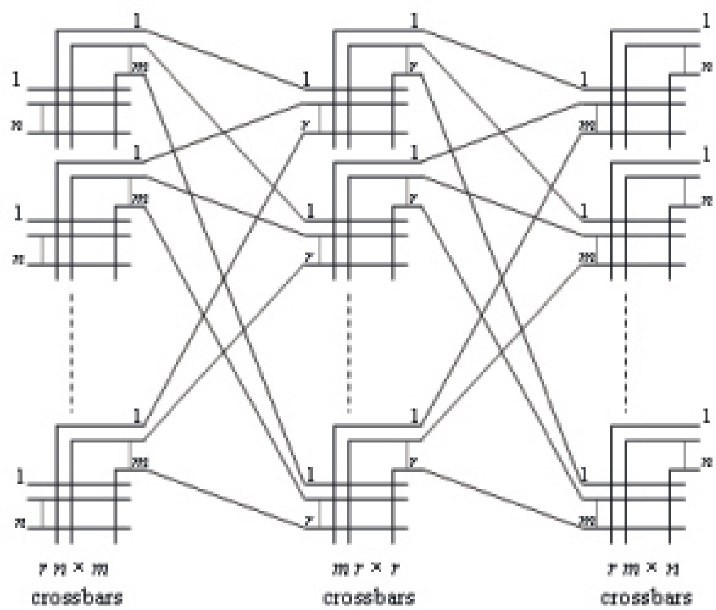

Рис. 1. Сеть Клоза

Смысл в построении сетей Клоза заключается в том, что сеть Клоза имеет меньшее количество точек коммутации по сравнению с аналогичным «одноядерным» кроссбаром.

Пример 1. *Рассмотрим кроссбар размерности* 2×2. *Количество возможных состояний составляет, согласно утверждению 6, лишь* $\dfrac{2!}{0!} = 2! = 2$ *(параллельное коммутирование и перекрёстное коммутирование), между тем, количество точек коммутации составляет* $2 \cdot 2 = 4$.

Иными словами, для того, чтобы переключаться между двумя состояниями кроссбара 2×2 $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ и $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, необходимо манипулировать 4 перемычками. При большем количестве входов и выходов этот недостаток кроссбара будет всё ощутимее:

Утверждение 7. *Количество точек коммутации в сети Клоза* $2 \cdot r \cdot m \cdot n + m \cdot r^2 = (2 \cdot n + r) \cdot r \cdot m$. *Между тем, аналогичный кроссбар имел бы размерность* $r \cdot n \times r \cdot n$, *при этом содержал бы* $(r \cdot n)^2$ *точек коммутации.*

Определение 4. *Сеть Клоза называется «строго неблокирующей», если свободный вход входящего кроссбара всегда может быть соединён со свободным выходом исходящего кроссбара без необходимости перекоммутации уже существующих соединений.*

Следующий вывод составляет основу классической статьи [1]:

Теорема 1. *Достаточное условие для того, чтобы сеть Клоза являлась «строго неблокирующей», можно записать формулой:*

$$m \geq 2 \cdot n - 1. \tag{2.1}$$

Определение 5. *Сеть Клоза называется «условно неблокирующей» или «неблокирующей при перекоммутациях», если свободный вход входящего кроссбара всегда может быть соединён со свободным выходом исходящего кроссбара при допущении перекоммутации уже существующих соединений*

Очевидно, что если сеть Клоза является «строго неблокирующей», она является и «условно неблокирующей», но достаточное условие для того, чтобы сеть Клоза была «условно блокирующей», много мягче условия (2.1): $m \geq n$.

Определение 6. *Если* $m < n$, *то сеть Клоза называется «допускающей блокировки».*

Список литературы

[1] Clos, Charles A study of non-blocking switching networks // Bell System Technical Journal. — 1953. — №32 (2). — 406–424 pp.

[2] Philipp Hall On Representatives of Subsets // Journal of the London Mathematical Society. — 1935. — №10. — 26–30 pp.

[3] Желваков Б.Б. *Архитектура корпоративных информационных систем. Учебное пособие.* – С.-П.: Государственный инженерно-экономический университет, кафедра Информационных систем в экономике, – 2012 – С. 622.