УДК 004.03.052

**Соловьев А.В.,**
**Майструк Д.В.,**
**Бондаренко В.Н.**, к.т.н.

# ОБЕСПЕЧЕНИЕ КАЧЕСТВА И БЕЗОПАСНОСТИ VOIP СВЯЗИ ПУТЕМ РЕОРГАНИЗАЦИИ КОРПОРАТИВНОЙ TCP/IP СЕТИ

**Национальный технический университет Украины «КПИ»**

*Рассмотрены проблемы, возникающие при внедрении и эксплуатации VoIP сетей. Предложены пути решения данных проблем при помощи реорганизации сети связи. Особое внимание уделено качеству, безопасности связи и снижению финансовых затрат.*

## *Введение*

Большинство современных организаций, будь-то коммерческие, государственные или любые другие, используют в своей работе локальные вычислительные сети (ЛВС) на базе протоколов сетевого уровня семейства *TCP/IP*. Развитие Интернет и *TCP/IP* сетей в общем дали мощный толчок к повсеместному внедрению *IP*-телефонии (*VoIP*). Технологии *VoIP* позволяют компаниям снижать затраты на телефонию как на этапе внедрения, так и на протяжении всего жизненного цикла инфраструктуры связи.

*IP*-телефония обладает множеством положительных качеств:

- дешевизна внедрения и эксплуатации;
- высокая скорость внедрения;
- обеспечение высокого качества передачи речи по сетям передачи данных;
- легкая интеграция с существующими сетями связи;
- возможность подключения к операторским сетям по различным стандартным протоколам;
- возможность использования внутренней нумерации, снижение затрат на телефонию в целом;
- развертывание на базе опорной *TCP/IP* сети;
- удобство администрирования и высокая надежность при эксплуатации.

Однако при попытке построения системы *IP*-телефонии на базе существующей *IP* сети без изменения ее структуры в большинстве случаев возникали проблемы, перечеркивающие все положительные стороны *VoIP*:

- несоответствие пропускной способности ЛВС и каналов передачи данных для корректной работы *VoIP* системы;
- отсутствие необходимого уровня безопасности при использовании недорогого оборудования и подверженность *VoIP* системы внутренним атакам;
- сложность администрирования *VoIP* оборудования.

Работа посвящена анализу перечисленных проблем и их решению с минимальными затратами финансовых ресурсов. При этом в качестве базового протокола *VoIP* связи рассматривается наиболее динамично развивающийся в корпоративном секторе открытый протокол *SIP* [1].

## *Рост трафика в корпоративных сетях*

Популярность технологий облачных вычислений, сетевых средств хранения данных, развитие и распространение всевозможных Интернет ориентированных медиа сервисов, увеличение количества сетевых устройств, необходимых одному сотруднику, привели к взрывообразному росту трафика в корпоративных ЛВС (так называемая «проблема лавины данных»). Кроме того, увеличение количества устройств создает проблему широковещательных штормов, что может парализовать работу сети.

Закон Мура, ранее описывавший развитие микросхем, удивительно точно описывает изменения в современных ЛВС. Удваивающаяся мощность сетевых вычислительных устройств позволяет обрабатывать и хранить вдвое большие объемы данных, а с учетом снижения стоимости – ведет к их повсеместному внедрению и росту генерируемого ими трафика в два раза за год [2]. Вместе с тем, рост скорости каналов передачи данных отстает от роста генерируемого трафика на 30–50% [3]. Эти два фактора приводят к перегрузкам сети и, как следствие, к увеличению задержек и потерям пакетов, что критично для *VoIP*.

Согласно стандарту *ITU G.114* задержка при передаче речи от абонента к абоненту до 250 – 300 мс считается удовлетворительной, при задержке более 400 мс использование *VoIP*

связи не имеет смысла. На графике (рис. 1) показана экспертная оценка качества связи в зависимости от задержки при передаче речи [4].

Максимальная задержка при кодировании голосового сигнала для современного оборудования не превышает 60 мс, исходя из этого – время прохождения пакетов в сети для комфортной работы *VoIP* не должно превышать 120 мс. Чтобы добиться таких и меньших значений задержки в больших ЛВС, где голосовой и весь остальной трафик не разделяются и обрабатываются совместно, требуются значительные финансовые затраты на дорогостоящее оборудование.

### Безопасность и шифрование в SIP

Протокол *SIP* имеет множество неоспоримых преимуществ, таких как:

- открытость;
- невысокая стоимость оборудования;
- удобство администрирования и развертывания;
- низкие тарифы, поддержка множеством операторов. Однако в стандартном виде этот протокол не обеспечивает шифрования.

*SIP* – (*Session Initiation Protocol* – протокол установления сеанса) используется только для терминирования звонков и определяет способ согласования между клиентами открытия канала обмена данными на основе транспортного протокола передачи трафика реального времени (или другого), чаще всего *RTP*. В корпоративных сетях, где вопросы безопасности стоят не на последнем месте, необходимо шифровать не только сам разговор (*RTP*), но и сеанс инициализации звонка (*SIP*), содержащий *DTMF*, номера, имена абонентов и пр.

Наиболее простым и универсальным в использовании механизмом шифрования является построение *IPsec* туннеля от конечной точки включения (например, *IP* АТС офиса) до центрального софт свича организации. Использование *IPsec* увеличивает скорость канала, необходимую для удовлетворительной работы *VoIP*, на 30 – 50%, а также увеличивает временные задержки прохождения пакетов. Данный недостаток этого метода шифрования не позволяет его использовать в условиях, описанных в предыдущем разделе.

Другим способом шифрования является связка протоколов *SRTP+TLS*. *SRTP* (*Secure Real-time Transport Protocol* – безопасный протокол передачи данных в реальном времени) является версией протокола *RTP* с поддержкой *AES* шифрования. Использование протокола *SRTP* не увеличивает объём передаваемых данных. Существует версия *SRTP* с использованием метода обмена ключей по алгоритму Диффи-Хелмана (алгоритм, позволяющий двум сторонам получить общий секретный ключ, используя незащищенный от прослушивания, но защищённый от подмены канал связи) [5]. Эта версия протокола называется *ZRTP*, но она является коммерческой, что противоречит условию минимальных финансовых затрат.

Для шифрования *SIP* сообщений можно использовать *SIPS* (протокол *SIP* с шифрованием сигнального трафика на транспортном уровне с применением *TLS* (*Transport Layer Security* – безопасность транспортного уровня – криптографические протоколы, обеспечивающие защищенную передачу данных между узлами *TCP/IP* сети)). Данная связка является наиболее удачной, но пока не поддерживается большим количеством оборудования, а закупка нового противоречит условию минимальных финансовых затрат.

При построении системы *VoIP* связи на базе имеющийся *IP* сети без ее реорганизации, возникает серьезная проблема защиты от несанкционированного доступа к *VoIP* оборудованию (центральный софт свитч, *IP* АТС, *IP* телефоны и пр.) из корпоративной сети. Так как *SIP* софт свитч не требует высокой производительности аппаратного обеспечения сервера, на котором работает, то при наличии свободного доступа из корпоративной сети, он может быть выведен из строя простой *DDoS* атакой внутренней ботнет сети.

### Развертывание и администрирование систем VoIP связи

Развертывание полноценной системы *VoIP* связи с поддержкой всех функций и использованием *Ethernet IP* телефонов чаще всего не требуется и связано с большими финансовыми затратами. Построение такой системы оправдано лишь при планировании офиса «с нуля», выделении отдельной *IP* сети для *IP* телефонов и четком понимании задач системы голосовой и видео связи в конкретной организации.

К сожалению, в Украине часто наблюдается ситуация использования дорогостоящего оборудования *VoIP* связи (например, *Cisco UC Phone 7965*, *Cisco 2911 Voice Bundle*) для решения тривиальных задач голосовой связи между абонентами. Такие задачи можно решить с на-

много меньшими финансовыми затратами при сохранении качества связи.

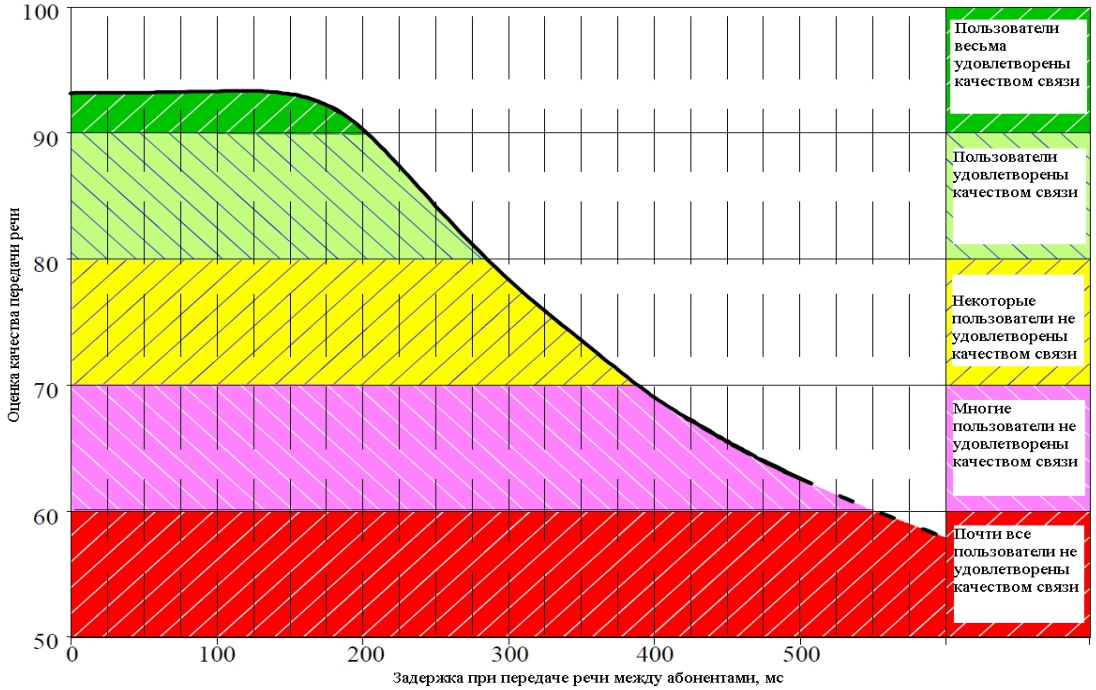


Рис. 1. Зависимость удовлетворения пользователей качеством связи от задержки

При наличии действующей системы аналоговой телефонной связи, наиболее простым и быстрым вариантом подключения офиса к существующей *VoIP* системе организации является замена аналоговой АТС на цифровую с поддержкой SIP, что не приводит к кардинальным изменениям в аналоговой телефонной и *IP* сетях. В таком случае не требуется физический монтаж опорной *IP* сети от станции к абоненту и закупка дорогостоящих *IP* телефонов; используются аналоговые телефоны, подключенные с помощью имеющегося телефонного распределительного провода к *IP* АТС. Единственным условием для корректной работы такой системы является соответствующий требованиям по скорости и задержкам канал передачи данных от *IP* АТС к центральному софт свичу организации.

Сопоставим затраты на организацию *VoIP* системы, требования к которой приведены в табл. 1. Применение *IP* АТС (*Samsung OS-707MA*), модулей расширения *(KP-AP4-WMG+SIP*), системных телефонов с поддержкой *SIP* (*Samsung OfficeServ*, *ERICSSON-LG*, *Siemens HiPath*) снизит расходы на развертывание и дальнейшее обслуживание системы *VoIP* связи (табл. 3) *более чем в два раза* по сравнению с решением *Cisco* (ядро *Cisco 2911 VoiceBundle, PVDM3-16, UC LicensePAK*; модуль расширения *Cisco Four-port Voice Interface Card – FXO (Universal)),* затраты на реализацию которого приведены в табл. 2.

Однако, в случае использования имеющейся *IP* сети для построения *VoIP* системы, централизованное администрирование (например, из головного офиса) такой системы усложняется различной адресацией, различными принципами маршрутизации и разделения сетевого трафика в имеющихся сетях объектов (филиалов, офисов, производственных предприятий). Учитывая вышеизложенное, приходим к необходимости реорганизации имеющейся *IP* сети для обеспечения качества и безопасности *VoIP* связи.

*Таблица 1.*

Требования к *VoIP* системе

| |
|---|
| 4 Входящие аналоговые линии |
| 4 входящие цифровые линии |
| 1 уровневый *IVR* (4 канальный автооператор) |
| 4 системных телефона (2 связки директор/секретарь) |
| Возможность использования стандартных аналоговых телефонов (до 20 шт.) |

*Таблица 2.*

Затраты на *VoIP* систему на базе ядра *Cisco*

| *Cisco* | Наименование | Кол-во | Цена, грн. с НДС | Сумма, грн. с НДС |
|---|---|---|---|---|
| Ядро | *Cisco 2911 Voice Bundle, PVDM3-16, UC License PAK* | 1 | 19000,00 | 19000,00 |
| Модули расширения | *Cisco Four-port Voice Interface Card - FXO (Universal)* | 1 | 5480,00 | 5480,00 |
| Аппараты (директор/ секретарь) | *Cisco UC Phone 7965, Gig Ethernet, Color* | 4 | 3750,00 | 15000,00 |
| Аппараты (аналоговые) | Шлюз для аналоговых телефонов, 8 | 2 | 2225,00 | 4450,00 |
| Дополнительные расходы | Блок питания для *Cisco UC Phone 7900 series* | 4 | 280,00 | 1120,00 |
| Работы по настройке | | 1 | 13500,00 | 13500,00 |
| | | | | 58550,00 |

### *Реорганизация корпоративной IP сети с учетом требований VoIP*

Рассмотрим построение *TCP/IP* сети организации, состоящей из одного центрального офиса, который является ядром сети, и двух зависимых филиалов. Данный пример легко экстраполируется на сети любого размера.

На рис. 2 представлена карта сети, которая поможет разобраться с нюансами разделения сетей центрального офиса и филиалов. Основной идеей, используемой для решения описанных проблем *VoIP*, является разделение сетей на канальном уровне (*Level 2*) с помощью коммутаторов второго уровня (*L2* коммутаторы, стоимость которых начинается от 800 грн.) с поддержкой *VLAN* (*Virtual Local Area Network*).

*VLAN* – это логическая ("виртуальная") локальная компьютерная сеть, представляющая собой группу хостов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному домену, независимо от их физического местонахождения.

*Таблица 3.*

Затраты на *VoIP* систему на базе ядра *Samsung*

| *Samsung* | Наименование | Кол-во | Цена, грн. с НДС | Сумма, грн. с НДС |
|---|---|---|---|---|
| Ядро | *Samsung OS-707MA* | 1 | 8486,40 | 8486,40 |
| Модули расширения | *KP-AP4-WMG+SIP* | 4 | 753,60 | 3014,40 |
| Аппараты (директор/ секретарь) | *SMT-i3105D* | 4 | 1416,00 | 5664,00 |
| Аппараты (аналоговые) | | 0 | 0,00 | 0,00 |
| Дополнительные расходы | Блок питания для *SMT-i3105D* | 4 | 283,20 | 1132,80 |
| Работы по настройке | | 1 | 6000,00 | 6000,00 |
| | | | | 24297,60 |

*VLAN* имеет те же свойства, что и физическая локальная сеть, но позволяет конечным станциям группироваться вместе, даже если они не находятся в одной физической сети. Такая реорганизация может быть выполнена на основе программного обеспечения вместо физического перемещения устройств [6]. *L2* коммутаторы гарантируют скорость переправления фреймов, обеспечиваемую средой передачи данных, и не дают задержки, которая возникает при использовании традиционных программно-ориентирован-ных методов коммутации с помощью маршрутизаторов.

В традиционных сетях с коммутаторами, не

поддерживающими *VLAN*, весь широковещательный трафик попадает во все порты. *VLAN* увеличивает производительность сети, помещая широковещательный трафик внутри маленьких и легко управляемых логических доменов. *VLAN* позволяет администратору создавать, группировать и перегруппировывать сетевые сегменты логически и немедленно, без изменения физической инфраструктуры и отсоединения пользователей и серверов. Как видно из рис. 2, все рабочие станции и прочая сетевая техника центрального офиса и каждого филиала (выделены пунктирными линиями) вынесены в отдельные *VLAN* (центральный офис – *VLAN#2*, филиал 1 – *VLAN#4*, филиал 2 – *VLAN#3*), а *IP* АТС и *SIP* софт свитч объединены в одну *VLAN* (*VLAN#1).*

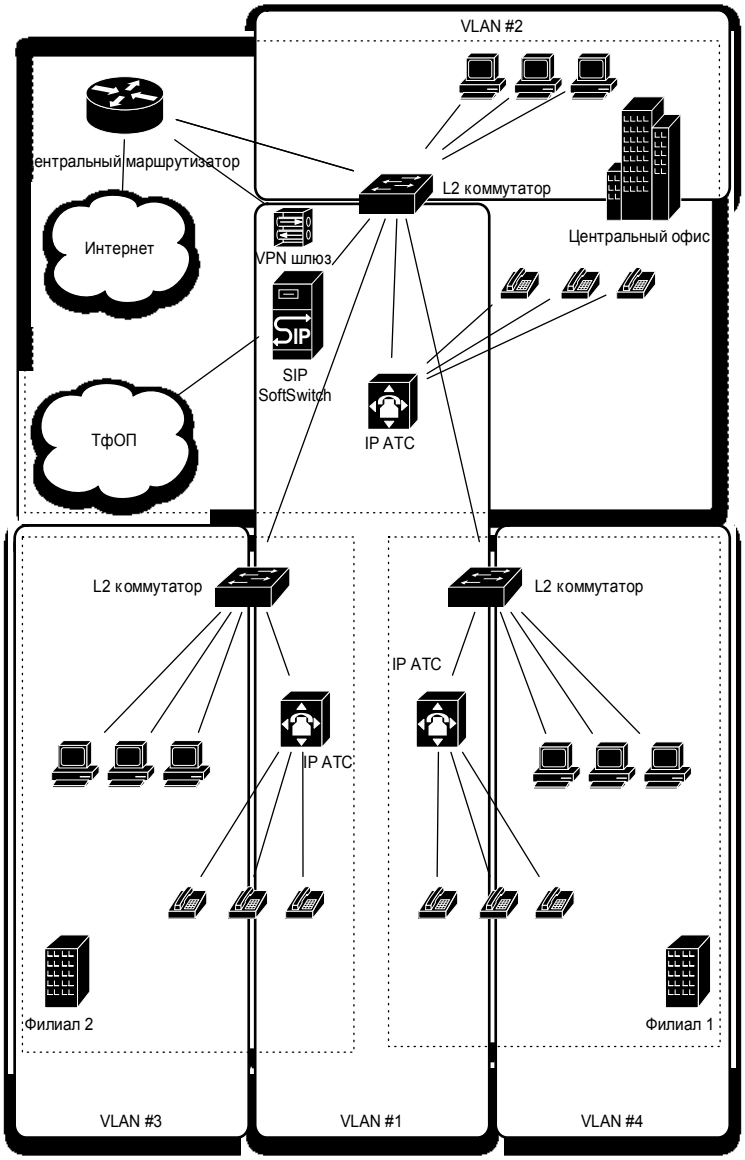


Рис. 2. Карта корпоративной *IP* сети

Данная виртуальная локальная сеть (*VLAN#1*) не имеет выхода в Интернет и связи с локальными сетями центрального офиса и филиалов. Перемещение всей инфраструктуры *VoIP* в отдельную закрытую *VLAN* позволило максимально обезопасить оборудование *VoIP* и отказаться от шифрования данных *VoIP* там, где это невозможно средствами имеющегося оборудования.

Поскольку для обеспечения защиты все *IP* АТС и *SIP* софт свитч внесены в отдельную *VLAN*, для доступа к ней и удобного администрирования *VoIP* оборудования из любой точки сети установлен сервер *VPN* (*VPN* шлюз) с шифрованием 128 бит. Данная мера позволила полностью обезопасить телефонную сеть от рядовых пользователей корпоративной сети и от атак из сети Интернет. Связь между виртуальными локальными сетями реализуется центральным маршрутизатором.

Для корректной работы *VoIP* необходима стабильная полоса пропускания канала связи. В данной корпоративной сети это требование реализовано следующим образом: скорость доступа для *VLAN#2,3,4* ограничена до значения, равного скорости транспортного канала пере-

дачи данных до центрального коммутатора минус 64 кбит/с*количество абонентов телефонной сети офиса или филиала. Например, скорость канала связи центральный офис-филиал равна 100 Мбит/с, количество абонентов телефонной связи в филиале – 40 человек. Имеем скорость канала передачи данных между внутренней ЛВС филиала и центральным офисом/Интернет – 97 Мбит/с. Уменьшение скорости канала на 3 Мбит/с не скажется на качестве работы сетевых сервисов для пользователей, но позволит решить проблему потери пакетов и увеличения времени задержек, что критично для *VoIP* телефонии.

### Выводы

Выделение виртуальной сети для *VoIP* оборудования из общей ЛВС на логическом уровне позволило с минимальными финансовыми затратами избавиться от проблем, связанных с сетевой инфраструктурой. Данное решение является простым во внедрении и обслуживании и, даже с учетом стоимости *L2* коммутаторов с поддержкой *VLAN*, значительно менее дорогим, чем обновление *VoIP* оборудования или увеличение скорости транспортных каналов.

### Список литературы

1. Гольдштейн Б.С. Протокол SIP. Справочник. – СПб.: BHV-Санкт-Петербург, 2005. – 456 с.

2. Gail Robinson. Speeding net traffic with tiny mirrors // EE Times. – 22.08.2011.

3. Джим Андерсон. LSI // Мир ЦОД. – 04.10.2012 / Интернет-ресурс: http://www.osp.ru/dcworld/2012/10/ 13017740.html.

4. ITU-T Recommendation G.114 (05/2003) / Интернет-ресурс: http://www.itu.int/rec/T-REC-G.114-200305-I/en.

5. Whitfield Diffie, Martin E. Hellman. New Directions in Cryptography // IEEE Transactions on information theory. – November 1976. – Vol. IT-22. – No. 5 / Интернет-ресурс: http://www-ee.stanford.edu/~hellman/publications/24.pdf.

6. D. McPherson, B. Dykes. VLAN Aggregation for Efficient IP Address Allocation // IETF. – February 2001 / Интернет-ресурс: http://www.ietf.org/rfc/rfc3069.txt