Сравнительный анализ шифрования удаленных подключений (VPNs) основанных на разных технологиях

О себе

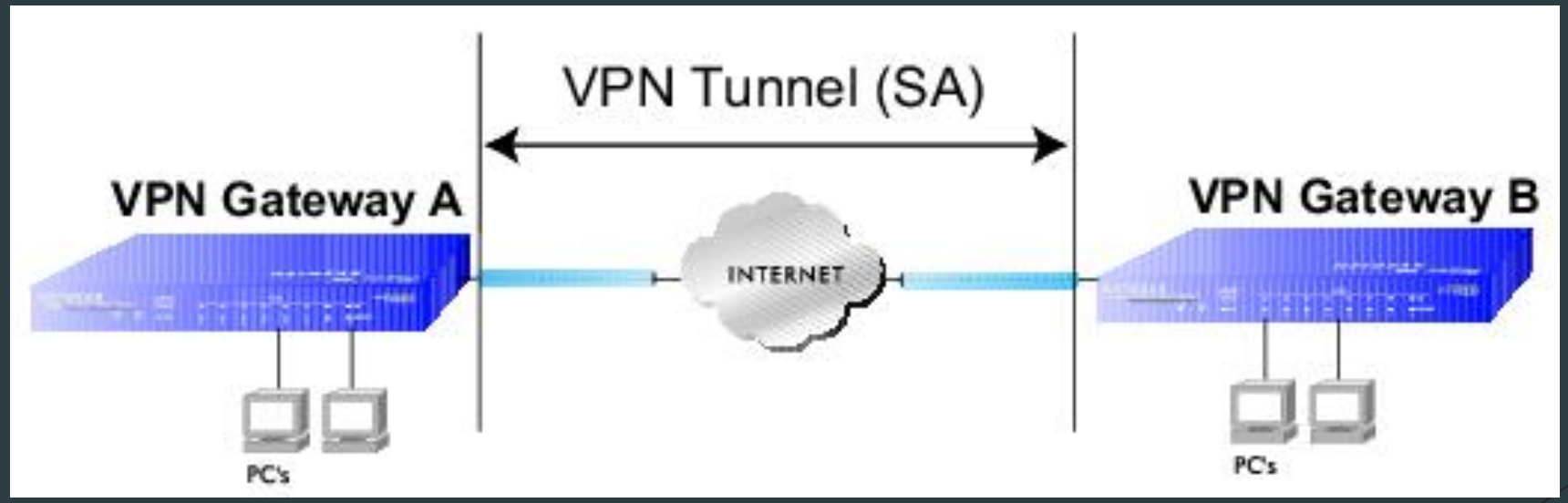
- Пафнутьева Арина Евгеньевна
- 3-ий курс в Морском Государственном Университете, специальность: информационная безопасность телекоммуникационных систем
- Около года техник компьютерного центра МГУ им. адм. Г.И. Невельского
- С ноября 2015 года тренер академии MikroTik, образованной на базе МГУ им. адм. Г.И. Невельского

Цель презентации

- Обзор поддерживаемых технологий для построения VPNs(туннелей) на базе оборудования MikroTik
- Углубленное рассмотрение стандартов, протоколов и алгоритмов для обеспечения безопасной передачи данных по туннелям
- Сравнительный анализ скоростей и уровня безопасной передачи данных для шифрованных каналов.

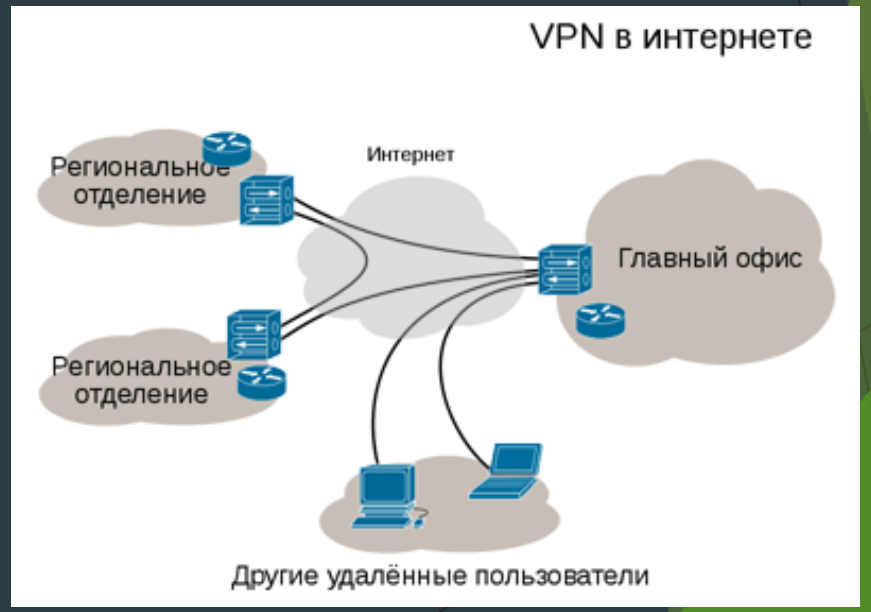
Что такое VPN?

- VPN(Virtual Private Network) – защищенное соединение-туннель, проходящее через интернет от хоста A к хосту B.



Зачем нужно использовать VPN?

- Удаленная работа с сетью.
- Высокий уровень защиты данных, который могут остаться в интернете, если не шифровать траффик.



Какие технологии используются для создания туннелей в оборудовании MikroTik?

Stateless (без состояния)	Client-server
GRE	L2TP
IP-IP	PPTP
EoIP	OpenVPN
	PPPoE
	SSTP

Нешифрованные туннели в роутерах MikroTik

- Stateless: GRE (P2P), IP-IP (P2P), EoIP
- Client-server: PPPoE

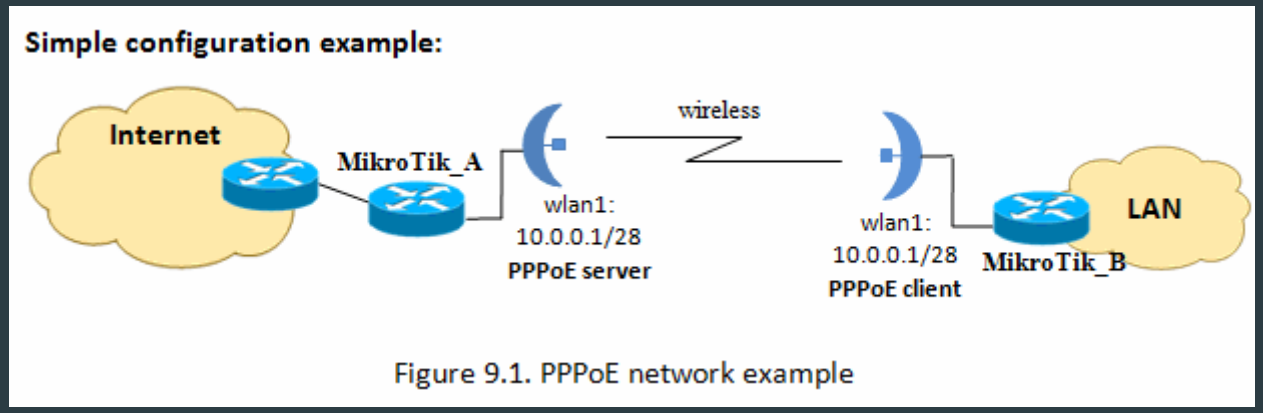
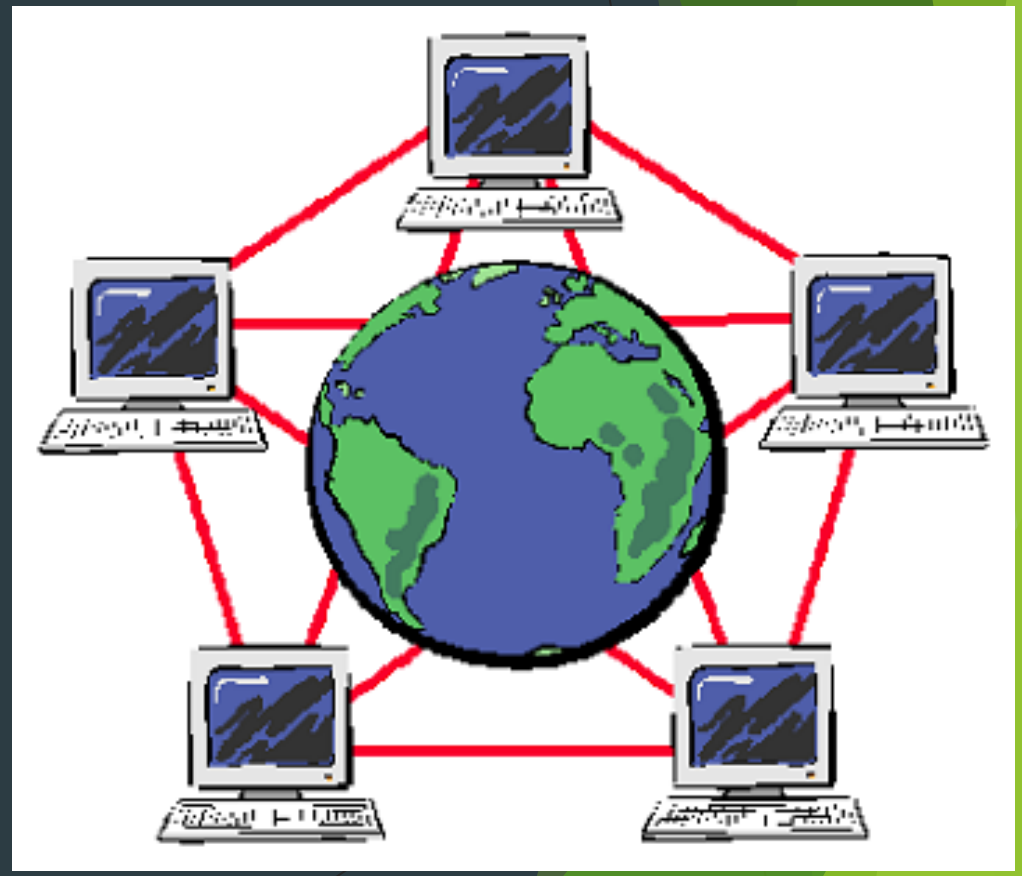


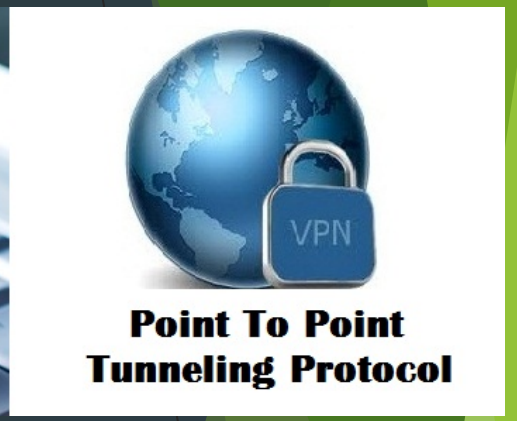
Figure 9.1. PPPoE network example



Шифрованные туннели в роутерах MikroTik

- Client-server: L2TP, PPTP, oVPN, SSTP

VPN	Способ шифрования
L2TP	MPPE 128
PPTP	MPPE RC4/ MPPE 128
OpenVPN	TLS (AES, BF)
SSTP	TLS (AES, RC4)



Технологии и алгоритмы шифрования

- MPPE
- TLS
- AES
- BF
- RC4

MPPE - Microsoft Point-to-Point Encryption

- MPPE – протокол шифрования данных, используемый на базе соединений PPP. Использует алгоритм PSA RC4, поддерживает 40-, 56-, 128-битные ключи. В роутерах MikroTik, собственно и поддерживается усиленный 128-битный ключ.

- MPPE требует использование ключей шифрования, генерируемых в процессе проверки подлинности по протоколу MS-CHAP, MS-CHAP2 или EAP-TLS

TLS – Transport Layer Security

- TLS – криптографический протокол, обеспечивающий защищенную передачу данных между узлами в сети Интернет. TLS использует ассиметричную криптографию для аутентификации, симметричное шифрование для обеспечения конфиденциальности, коды аутентичности для сохранения целостности сообщений.
- Поподробнее об:
  1. Ассиметричная криптография (RSA, Diffie-Hellman, DSA, ECDSA)
  2. Симметричное шифрование (RC4, IDEA, Triple DES, SEED, Camelia, AES)
  3. Коды аутентичности/хен-функции (MD5, SHA)

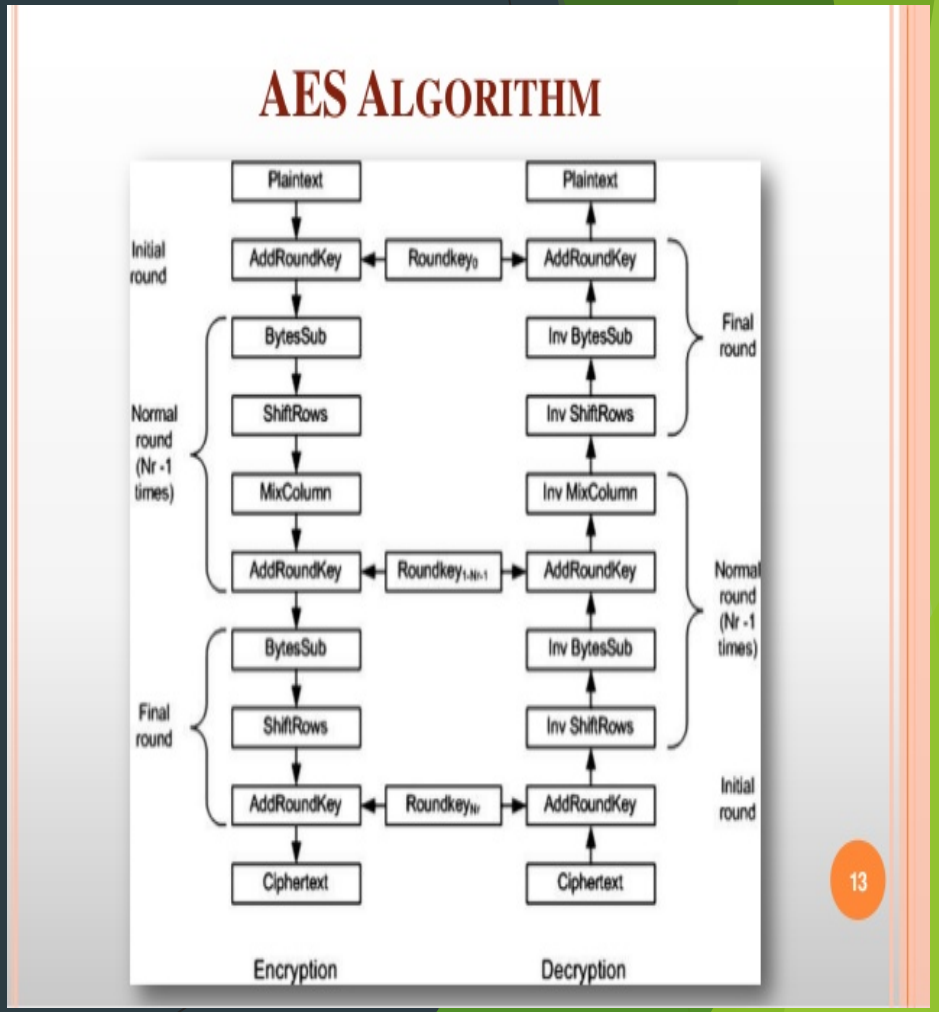
AES – Advanced Encryption Standart

- AES – симметричный алгоритм блочного шифрования

Длина блока входных данных и промежуточного состояния данных одинакова и равна **128 бит**.

Начало шифрования: копирование данных в массив state – State[r, c] = input[r + 4c] для 0 ≤ r < 4 и 0 ≤ c < Nb

Далее после применения процедур трансформации state копируется в массив выходных данных по правилу output[r + 4c] = State[r, c] с теми же условиями для r и c



RC4 – Rivest cipher 4

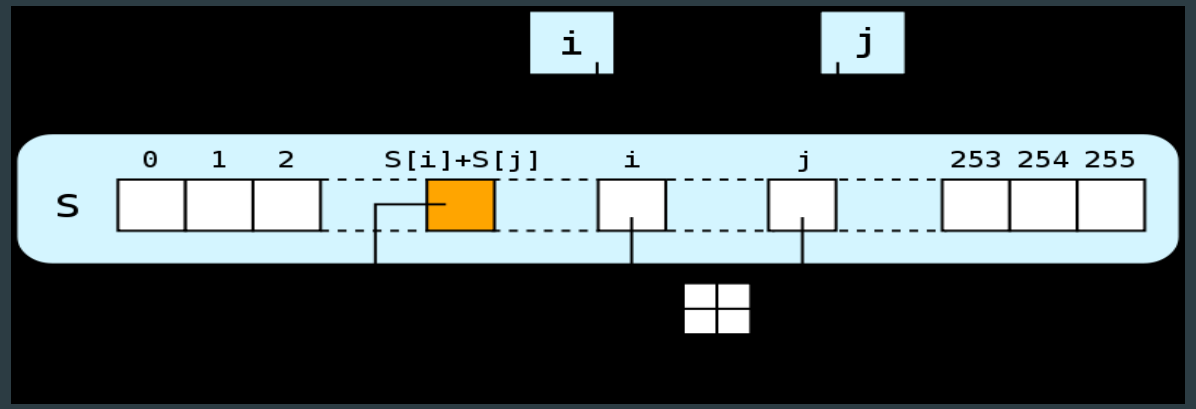
- RC4 – потоковый шифр, применяющийся в различных системах защиты информации в компьютерных сетях.
- Строится на основе генератора

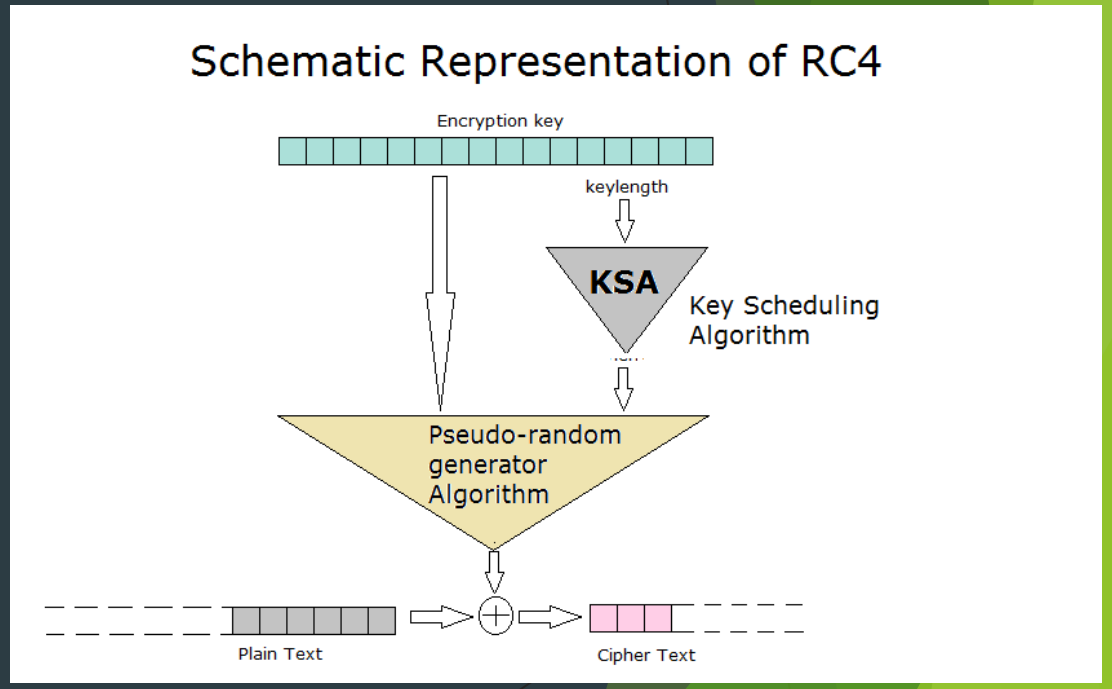
псевдослучайных битов.

- Уязвим если используются не

случайные ключи или один ключевой поток

используется дважды



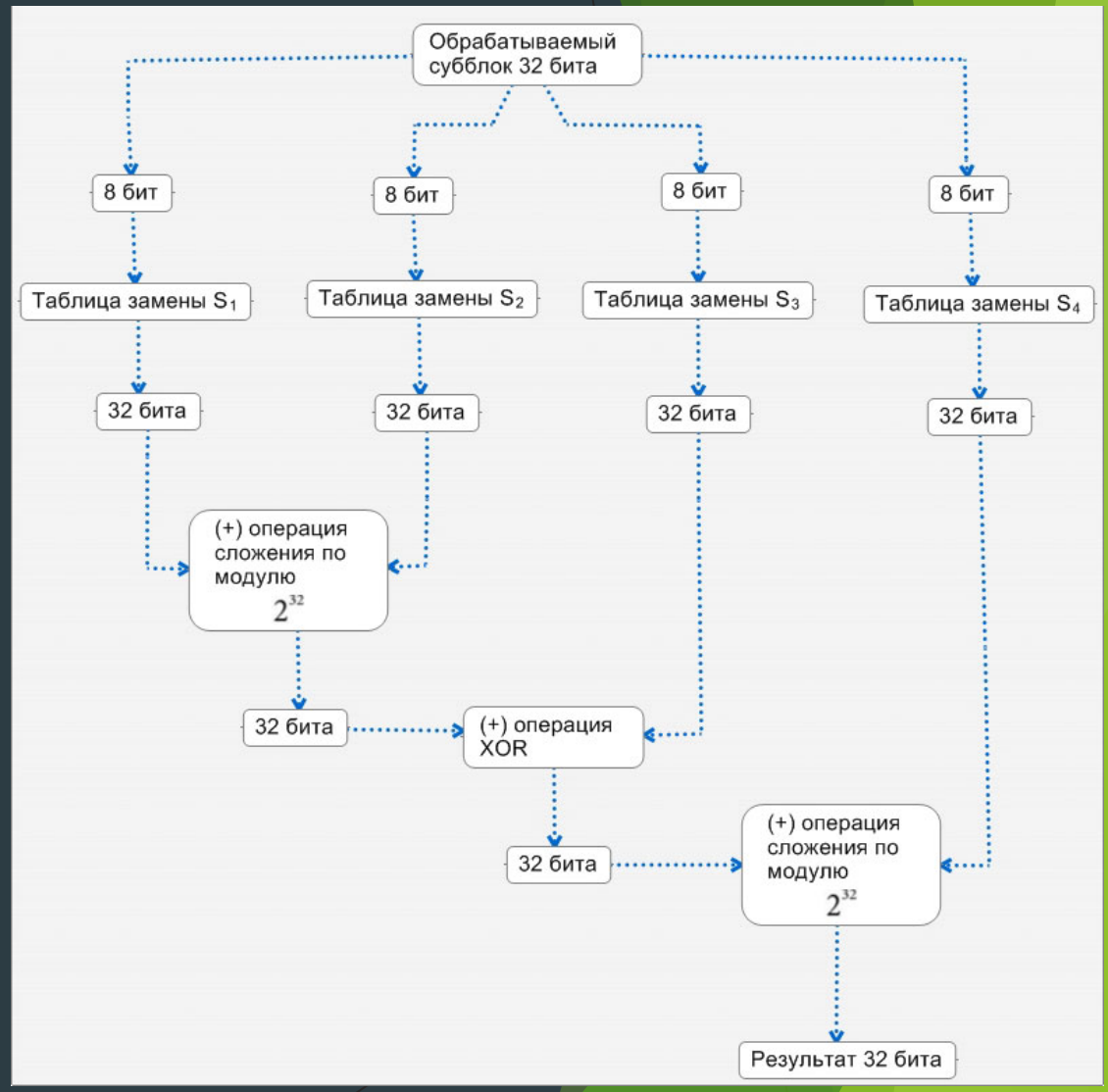


BF - Blowfish

- BF – криптографический алгоритм, реализующий блочное симметричное шифрование с переменной длиной ключа.

Алгоритм состоит из расширения и шифрования данных. На этапе расширения исходный ключ (до 448 бит) преобразуется и общий объем ключей получается 33344 бита.

Далее происходит шифрование текста полученными ключами и функцией F(x).



Отдельно про IPSec (IP Security)

- IPSec – набор протоколов для обеспечения защиты данных передаваемых по протоколу межсетевого уровня IP. Обеспечивает высокую надежность передаваемой информации в результате сложного алгоритма работы протоколов.
- На оборудовании MikroTik при конфигурации туннеля на базе L2TP, использование IPSec обеспечивает высокую надежность канала.

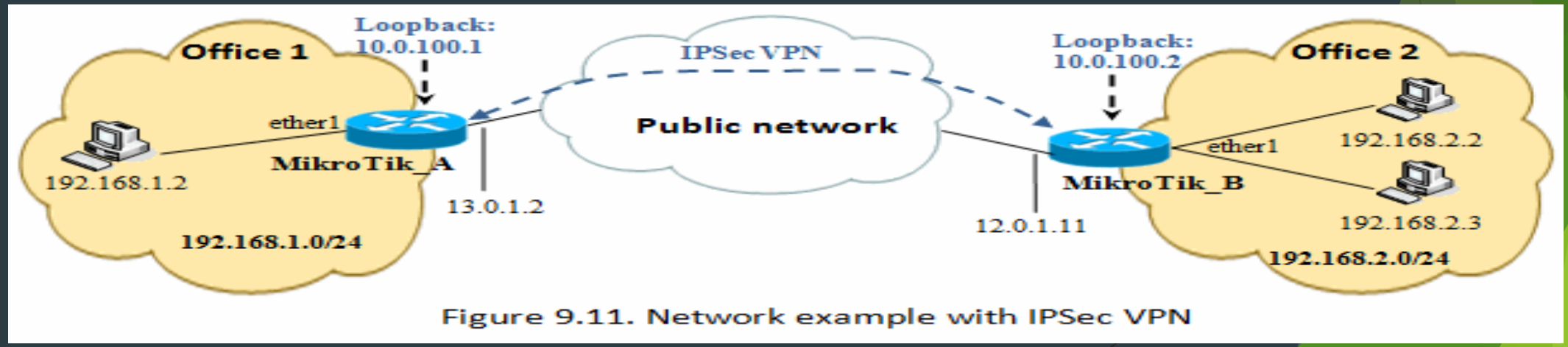
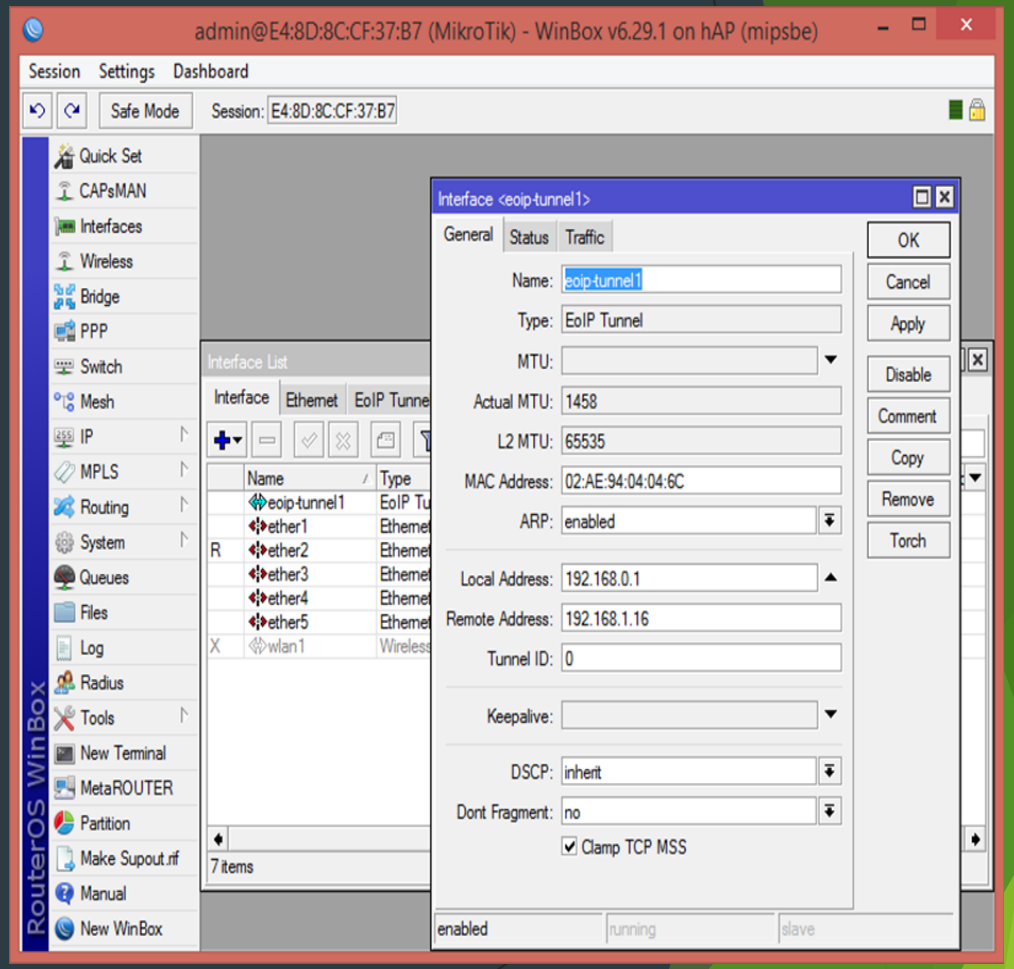


Figure 9.11. Network example with IPSec VPN

Туннели без состояния

- Туннель EoIP забирает около 10-15% полосы пропускания, что может быть существенно для каналов с низкой пропускной способностью.
- GRE. Из-за отсутствия шифрования (в GRE-туннелях происходит только инкапсуляция, без фрагментации), данная технология показывает достаточно высокую пропускную способность.

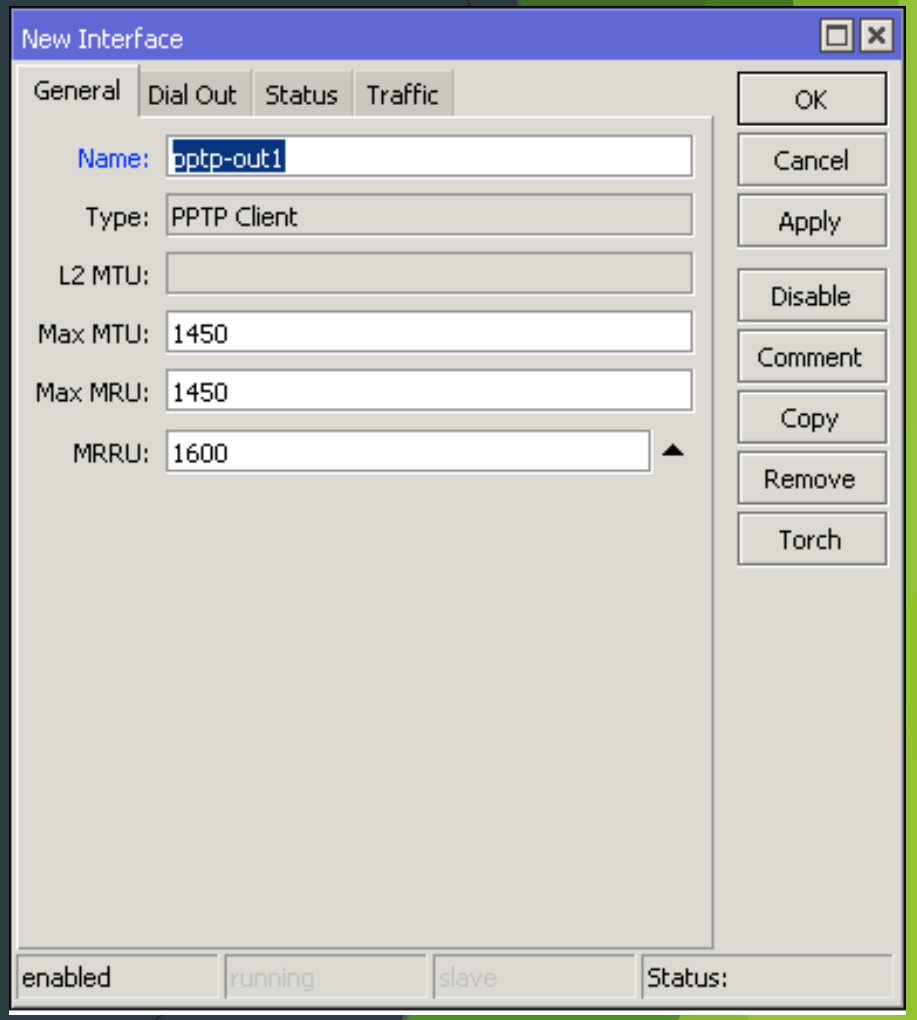


L2TP - tunnel

- Данный туннель является достаточно безопасным, использующийся в комплексе с технологией IPSec, однако вследствие двойной инкапсуляции, работает достаточно медленно. Но тем не менее, на сегодняшний день является самым безопасным из предложенных типов туннелей client-server.

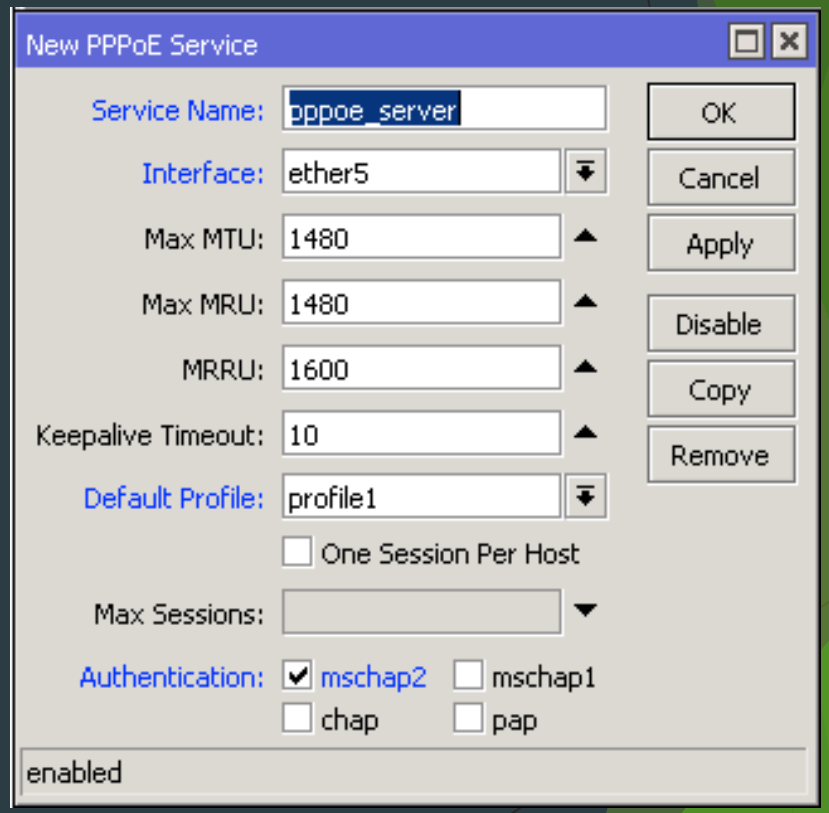
PPTP - tunnel

- Несмотря на то, что этот туннель шифруется, протокол аутентификации (MS-CHAP v.2) имеет ряд уязвимостей, вследствие чего безопасность данного типа туннелей не является его отличительной чертой. Однако он достаточно быстро работает и прост в настройке.



PPPoE - tunnel

- Единственный из туннелей типа client-server, не подвергающийся шифрованию, показывает пропускную способность, соответствующую технологии Ethernet, так как использует данный интерфейс для передачи данных.

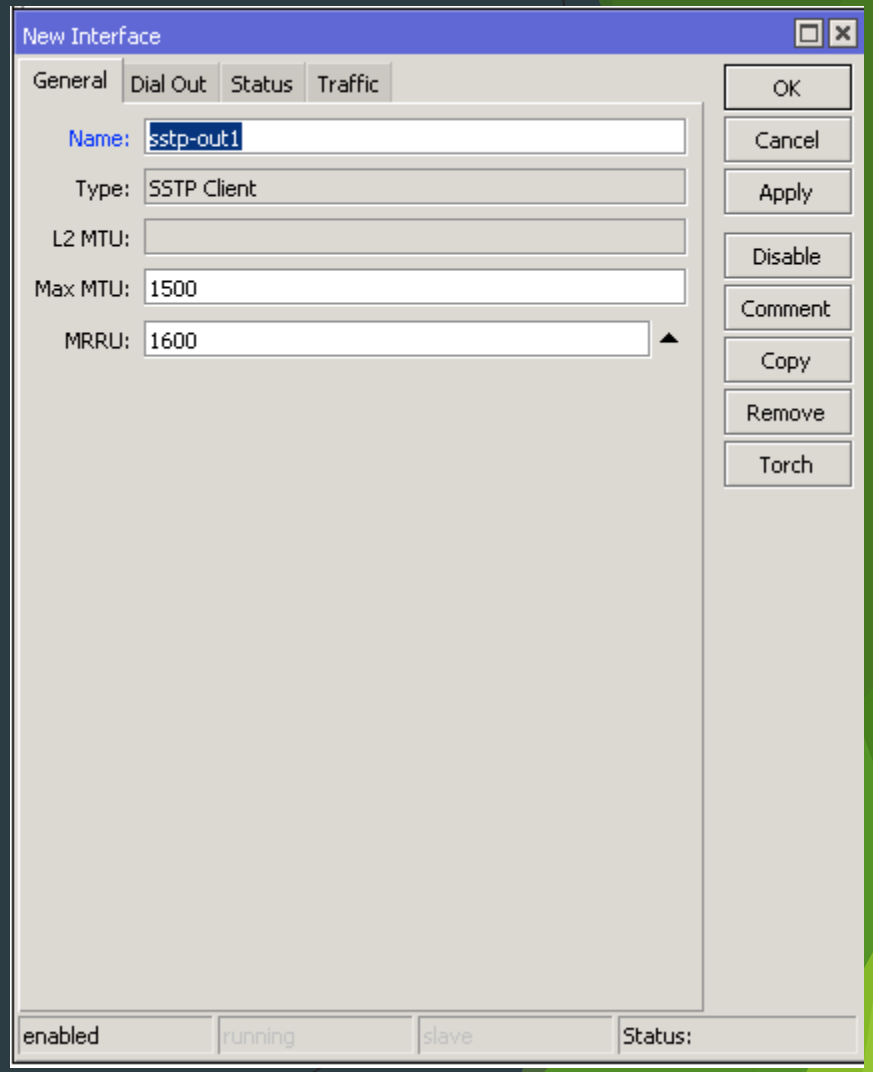


OpenVPN

- Является достаточно новой технологией с открытым кодом. Поддерживает достаточно много криптографических алгоритмов, рассмотренных ранее, наиболее популярные из которых – AES и BF. В зависимости от алгоритма показывает разную скорость работы, однако как правило, работает быстрее чем IPSec.

SSTP - tunnel

- Был представлен компанией Microsoft в Windows Vista, и несмотря на то что доступен теперь и на других ОС, по большей части все равно используется в Windows-системах. Более стабилен чем OpenVPN, а в целом предлагает все те же преимущества.



Сравнение шифрованных туннелей

VPN	Степень безопасности	Скорость
L2TP/IPSec	Наиболее безопасен	Достаточно медленный
OpenVPN	Безопасный	Скорость удовлетворительна
SSTP	Безопасный	Скорость удовлетворительна
PPTP	Уязвимый	Достаточно быстрый
http://mum.mikrotik.com/presentations/EU16/presentation_2955_1458135277.pdf		

Итоги

- Назначение туннелей
- Разбор алгоритмов шифрования
- Разбор каждого типа туннелей
- Сравнительный анализ

ВОПРОСЫ?

Спасибо за внимание!