



Cisco Expo 2009

Дизайн сетевой инфраструктуры для систем IP видеонаблюдения



Анастасия Марченко

Системный инженер

amarchen@cisco.com

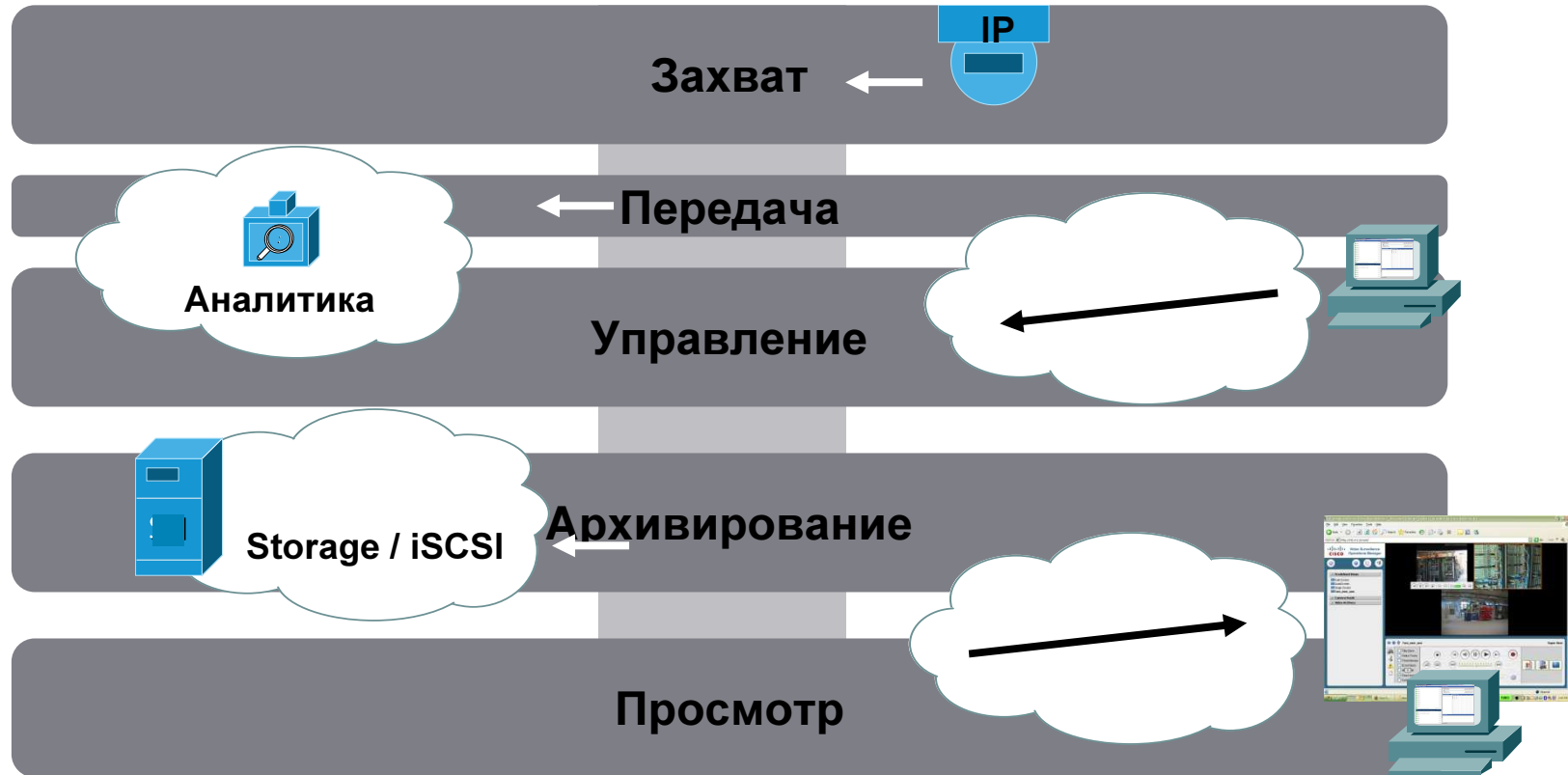
План презентации

1. Планирование инфраструктуры для IP видеонаблюдения
2. Сервисы сети для IP видеонаблюдения
3. QoS для IP видеонаблюдения
4. Применение PfR
5. Виртуализация и криптование
6. Заключение

Планирование инфраструктуры для IP видеонаблюдения



Компоненты IP Видеонаблюдения



**Мониторинг в реальном
режиме времени**

**Расследование после
инцидента**

Планирование IP видеонаблюдения

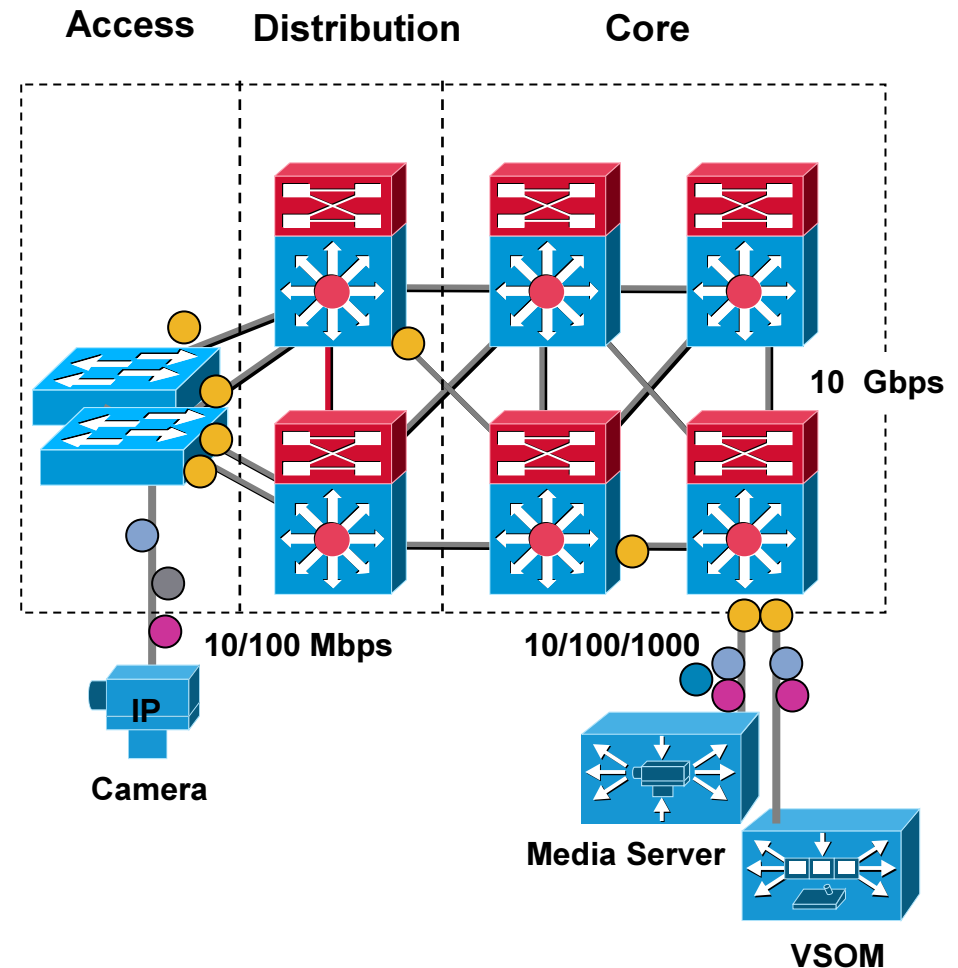
1. Определить количество камер на каждом объекте наблюдения
2. Питание через PoE/внешний блок питания
3. Оценить кодек, разрешение, bitrate/framerate для каждого объекта наблюдения
4. Определить требования к длительности хранения
5. Проверить поддержку необходимых функций на коммутаторах
6. Провести аудит сети и определить требуется ли обновление/редизайн
7. Определить параметры серверов для системы управления и вычислить необходимые ресурсы для хранения

Планирование IP видеонаблюдения

8. Выделить IP-адресное пространство и VLAN-ы
9. Определить запущены ли в сети сервисы NTP, Syslog, SNMP, системы управления сетью
10. Проанализировать существующие политики QoS, оценить требуемые изменения для IP видеонаблюдения
11. Определить необходимость в криптовании и права доступа к видео, которые удовлетворяют потребностям пользователей и соответствуют корпоративным стандартам по безопасности
12. Определить видеопотоки, которые должны мониториться в реальном режиме времени
13. Определить необходимость в обучающих курсах

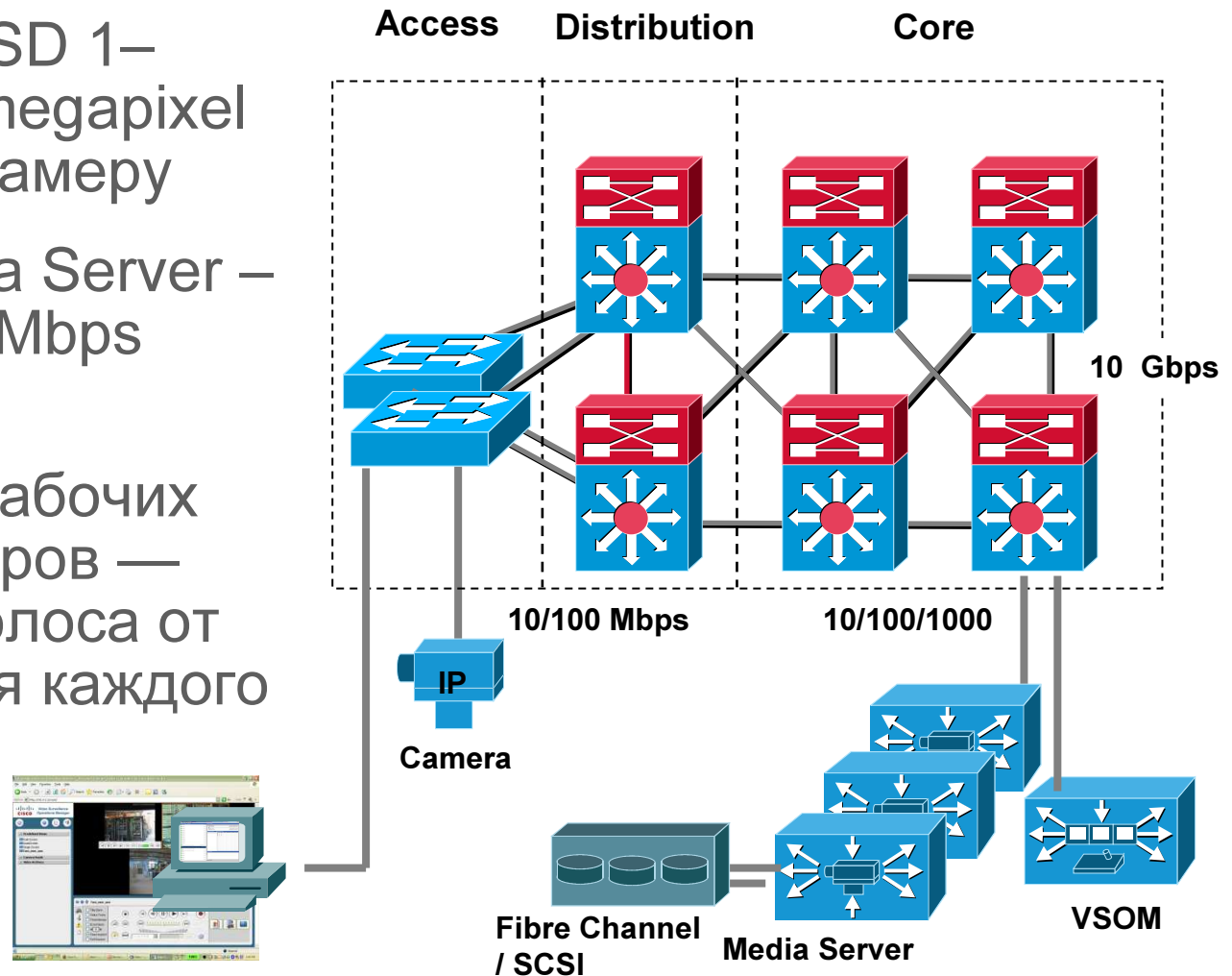
Дизайн кампусной сети для IP видеонаблюдения

1. ● Видеопотоки однонаправленные — настройка очередей на аплинках и портах, куда подключены серверы
2. ● Устройства системы IP видеонаблюдения находятся в отдельном VRF/VLAN
3. ● QoS маркировка — камерами (trust DSCP) или на порту коммутатора
4. ● Настройка Port security
5. ● Планирование для точек агрегации трафика



Дизайн кампусной сети для IP видеонаблюдения

1. Полоса для SD 1–2mbps—HD/мегапиксел 3–5mbps на камеру
2. Каждый Media Server — не более 200Mbps Input/Output
3. Количество рабочих мест операторов — требуемая полоса от 2–20mbps для каждого



Планирование IP видеонаблюдения через WAN/MAN

1. Организация канала связи с требуемой полосой пропускания (доступность, стоимость)
2. Должны ли потоки перенаправляться для видеоаналитики?
3. Локальное хранилище
4. Резервный Media Server
5. Proxy Media Server
6. Резервирование MAN/WAN каналов связи—performance routing
7. Кодек(MJPEG/MPEG-4/H.264)



**Сервисы сети для IP
видеонаблюдения**
Инсталляция, эксплуатация,
детекция неисправностей



Сервисы сети для IP видеонаблюдения

Преимущества по сравнению с аналоговыми системами

1. IP сеть — доступ к видео в любое время из любого места
2. Транспорт видео через надежную и резервируемую IP инфраструктуру
3. Применение сетевых протоколов и сервисов для управления

Настройка оборудования через web

Dynamic Host Configuration Protocol (DHCP)

Cisco Discovery Protocol (CDP)

Power over Ethernet (PoE)

Simple Network Management Protocol (SNMP)

Syslog

Network Time Protocol (NTP)

Начальная конфигурация

1. Большинство IP камер поддерживают DHCP
2. Персонал на удаленной площадке просто подключает камеру к IP сети
3. Инженер настраивает камеру удаленно через IP сеть

The screenshot displays the configuration interface for an Axis 207 Network Camera. The browser window shows the 'Basic Setup' page with the following fields:

- Device ID: CIVS-IPC-2500
- Camera Name: CAM001DESEA7903
- Description: CIVS-IPC-2500 (IP) Roaming
- Enable LED Operations:
- Current Date/Time: 10/01/08 17:25:05
- Time Zone: (GMT-05:00) Eastern Time (US & Canada)
- Adjust for Daylight Saving Time:
- Check here if you want to update the time automatically through the NTP server from the internet:
- NTP Server Address: 192.0.2.33
- NTP Port: 123
- Configuration Type: Fixed IP Address
- IP Address: 192.0.2.50
- Subnet Mask: 255.255.255.240
- Gateway: 192.0.2.49
- Primary DNS: 192.0.2.49
- Secondary DNS:

The 'Advanced TCP/IP Settings' page is also visible, showing the following configurations:

- DNS Configuration: Use the following DNS server address: Domain name: ese.cisco.com, Primary DNS server: , Secondary DNS server: .
- NTP Configuration: Use the following NTP server address: Network address: 192.0.2.17
- Host Name Configuration: Use the host name: axis-00408c8e03b0
- Link-Local Address: Auto-Configure Link-Local Address
- HTTP: HTTP port: 80
- NAT traversal (port mapping): NAT traversal is disabled.

Создание DHCP пула на маршрутизаторе

Первоначально адрес устанавливается динамически

```
!  
ip dhcp pool cameras  
  network 192.0.2.48 255.255.255.240  
  default-router 192.0.2.49  
  domain-name ese.cisco.com  
  dns-server 10.102.6.247 10.68.226.120  
!  
!  
interface GigabitEthernet0/0.208  
  description inside interface for ip cameras  
  encapsulation dot1Q 208  
  ip address 192.0.2.49 255.255.255.240  
!  
ip dhcp excluded-address 192.0.2.52  
! assigned address may be excluded from pool
```

**Cisco IP camera requests
IP Address via DHCP.
MAC address printed on camera housing**

No response in 90 seconds - 192.168.0.100

router

show ip dhcp binding

switch

*show mac address-table dynamic interface
show cdp neighbors detail*

IPVS Address Allocation

192.0.2.32 /30	ISR NM NME-VMSS-HP16
192.0.2.36 /30	EVM-IPVS-16A (optional Analog Gateway Network Module)
192.0.2.48 /28	Reserved for IP Cameras (0.0.0.15)
192.168.211.0/24	iSCSI Management Subnet

Дополнительно для IP камер Cisco

Cisco Discovery Protocol (CDP) включен по умолчанию

The screenshot shows the Cisco Internet Camera web interface in Microsoft Internet Explorer. The browser address bar shows 'http://192.0.2.'. The page title is 'Facilitates Implementation and Troubleshooting'. On the left, there is a navigation menu with 'Home', 'Setup', 'Advanced Setup', and 'IP Filter'. Below the menu is an image of a Cisco camera. The main content area is titled 'Advanced Setup' and has several sections: CDP (with 'Enable CDP (Cisco Discovery Protocol)' checked), HTTP/HTTPS, RTP/RTSP, and QoS. A terminal window overlay is positioned over the right side of the page, displaying the command 'vs-rm150a#show cdp neighbors g0/1 det' and its output. Red dashed circles highlight the following fields in the terminal output: 'Device ID: 001DE5EA798F', 'Entry address(es): IP address: 192.0.2.19', 'Platform: CIVS-IPC-2500, Capabilities: Host', 'Interface: GigabitEthernet0/1, Port ID (outgoing port): eth0', 'Holdtime: 147 sec', 'Version: 1.1.1', 'advertisement version: 2', 'Duplex: full', 'Power drawn: 9.000 Watts', 'Power request id: 45260, Power management id: 3', 'Power request levels are: 9000 0 0 0 0', and 'Management address(es): IP address: 192.0.2.19'. A 'Logout' button is visible at the bottom of the web interface.

Cisco Camera
CIVS-IPC-2500

MAC / IP Address

Device Type / Firmware Version

Duplex / Power Requirements

Power over Ethernet

LAN коммутатор должен поддерживать 802.3af

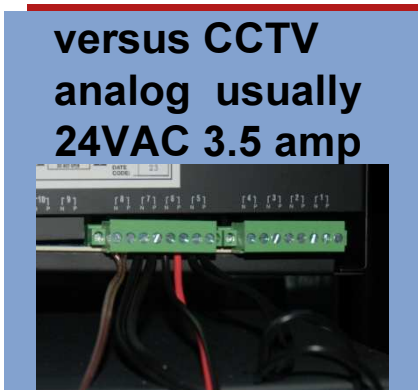
```
3750-access#show cdp neighbors gigabitEthernet 1/0/2
-----
Device ID: 001DE5EA79D3
Entry address(es):
  IP address: 192.0.2.50
Platform: CIVS-IPC-2500, Capabilities: Host
Interface: GigabitEthernet1/0/2, Port ID (outgoing p
Holdtime : 153 sec

Version :
1.1.1

advertisement version: 2
Duplex: full
Power drawn: 9.000 Watts
Power request id: 57831, Power management id: 3
Power request levels are:9000 0 0 0 0
Management address(es):
  IP address: 192.0.2.50
```



Max. Power Levels at Input of Powered Device
Class 3 is 6.49 to 12.95 Watts – up to 100 meters



```
3750-access#show power inline gigabitEthernet 1/0/2
```

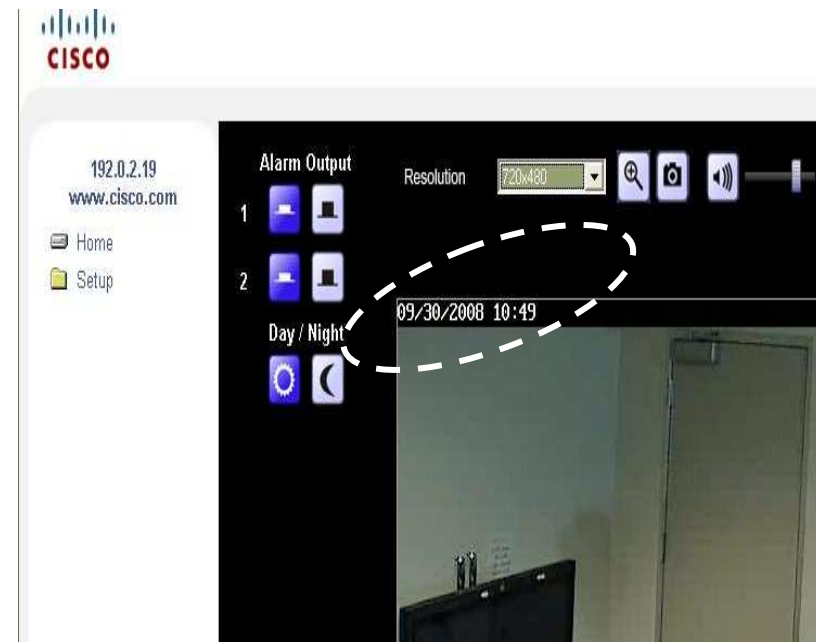
Interface	Admin	Oper	Power (Watts)	Device	Class	Max
Gi1/0/2	auto	on	9.0	CIVS-IPC-2500	3	15.4

Interface	AdminPowerMax (Watts)	AdminConsumption (Watts)
Gi1/0/2	15.4	15.4

Network Time Protocol (NTP)

Критично при расследовании инцидентов

1. Синхронизация часов на камере с единым источником времени
2. Локальное время отображается камерой
3. Возможность сравнения времени на камерах



Syslog

1. Маршрутизаторы Cisco отправляют syslog сообщения на сервера логирования (категория 'local7')
2. Cisco IP камеры используют категорию 'user'
3. Включение логирования уровня 'debug'

```
/etc/syslog.conf
```

```
#
```

```
local7.debug
```

```
user.debug
```

```
/var/adm/logs/cisco.log
```

```
/var/adm/logs/cisco.log
```

4. Перегрузка syslog процесса

```
# kill -HUP `cat /etc/syslog.pid`
```

```
Sep 30 15:13:50 [192.168.16.30.4.2] 192.168.16.30 09/30/2008 15:23:17 Stream: RTSP stream started. [ip: video, UDP: 192.168.16.30:5002 -> 192.0.2.2:6500, vsom]
```

```
Sep 30 15:14:20 [192.168.16.30.4.2] 192.168.16.30 09/30/2008 15:23:48 NTP: Synchronization OK.
```

Шаги по инсталляции IP Камеры

1. Создать (проверить) DHCP пул and interface on router
2. Document (update) switch, router and DNS with hostname and IP address assigned to camera

3. Настроить IP камеру (**https://camera_ip_address**)

Factory Default Initialization Screen (настроить пароли)

Administration - > Users (Создать пользователя для VSOM)

Setup - > Basic Setup (NTP, фиксированный IP адрес)

Setup - > Advanced Setup -> QoS

Security -> Complexity

Audio/Video -> Video -> Options (включить timestamp и текст для отображения)

Status -> Syslog & Log (включить syslog логирование и указать IP адрес сервера)

Setup -> IP Filter (настройка листов контроля доступа к камере)

4. Выполнить настройки на VSOM

Настройка камеры в VSOM

Добавление новой IP камеры

Важно:
QoS, NTP, Syslog, и пр.
Должны быть настроены через
Web-интерфейс камеры

Hostname / IP Address →

Media Type
Format
Resolution →

Bitrate [Constant Bit Rate] →

Имя пользователя и пароль
для VSOM
Должен быть идентичен настроенному
на камере →

Add a new IP/Network Camera

Camera Type | Camera Groups | Adv. Config | Map Info. | Rights

Camera Information

*Camera Name: TEST
Description:
*Camera Type: Cisco 2500 IP Camera
*Host IP/Name: 192.0.2.55
*Status: Enabled

Camera Feed

*Server: VSMS_Site150
*Media Type: MPEG-4
*Format: NTSC
*Resolution: 4CIF (704 x 480)
*Transport: TCP UDP
Multicast Address: (Leave blank for unicast)
*Bitrate: 1024
*Quality: [Slider]

Camera requires authentication

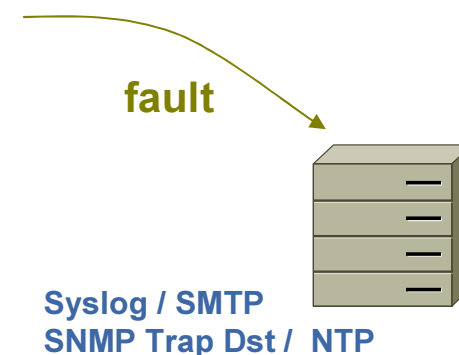
*Username: vsom
*Password:

Безопасность на порту коммутатора

```
macro name CIVS-IPC-2500
description Cisco Video Surveillance 2500 Series IP Camera
switchport mode access
switchport access vlan $VLAN
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
mls qos trust dscp
spanning-tree portfast
spanning-tree bpdupfilter enable
load-interval 60
no shutdown
@
```

Разрешается использовать только MAC адрес первого подключенного устройства

Если камера будет физически отключена от порта для подключения другого устройства, порт перейдет в состояние `error-disabled` и выключится



SNMP traps и syslog сообщения – возможность мониторинга и отправки сообщений ответственным лицам

QoS для IP видеонаблюдения



Cisco medianet Application Classes

DiffServ QoS Recommendations (RFC 4594-Based)

Application Class	Per-Hop Behavior	Admission Control	Queuing & Dropping	Application Examples
VoIP Telephony	EF	Required	Priority Queue (PQ)	Cisco IP Phones (G.711, G.729)
Broadcast Video	CS5	Required	(Optional) PQ	Cisco IP Video Surveillance / Cisco Enterprise TV
Realtime Interactive	CS4	Required	(Optional) PQ	Cisco TelePresence
Multimedia Conferencing	AF4	Required	BW Queue + DSCP WRED	Cisco Unified Personal Communicator
Multimedia Streaming	AF3	Recommended	BW Queue + DSCP WRED	Cisco Digital Media System (VoDs)
Network Control	CS6		BW Queue	EIGRP, OSPF, BGP, HSRP, IKE
Call-Signaling	CS3		BW Queue	SCCP, SIP, H.323
Ops / Admin / Mgmt (OAM)	CS2		BW Queue	SNMP, SSH, Syslog
Transactional Data	AF2		BW Queue + DSCP WRED	Cisco WebEx / MeetingPlace / ERP Apps
Bulk Data	AF1		BW Queue + DSCP WRED	E-mail, FTP, Backup Apps, Content Distribution
Best Effort	DF		Default Queue + RED	Default Class
Scavenger	CS1		Min BW Queue (Deferential)	YouTube, iTunes, BitTorrent, Xbox Live

QoS на IP Камере

192.0.2.52
www.cisco.com

Home

- Setup
 - Basic Setup
 - Advanced Setup
 - IP Filter
- Administration
- Audio/Video
- Security
- Applications
- Status

Advanced Setup

CDP Enable CDP (Cisco Discovery Protocol)

HTTP/HTTPS Enable HTTP Alternative Port (1024-65535)
 Enable HTTPS Alternative Port (1024-65535)

RTP/RTSP RTSP Port: (554,1024-65535)
RTP Data Port:
Max RTP Data Packet: bytes (400-1400)
 Enable Multicast

QoS Enable QoS Mode Audio Video Both
DSCP: (0-63)

Cancel Save

Cisco Camera CIVS-IPC-2500

IP Camera Deployment

SmartPort Macros

```
macro name CIVS-IPC-2500
description Cisco Video Surveillance 2500 Series IP Camera
switchport mode access
switchport access vlan $VLAN
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
mls qos trust dscp
spanning-tree portfast
spanning-tree bpdudfilter enable
load-interval 60
no shutdown
@
```



macro apply CIVS-IPC-2500 \$VLAN 208

Remember to write memory !

```
3750-access(config)#interface gigabitEthernet 1/0/2
```

```
3750-access(config-if)#macro apply CIVS-IPC-2500 $VLAN 208
```

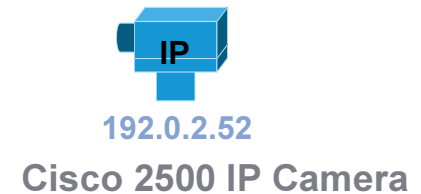
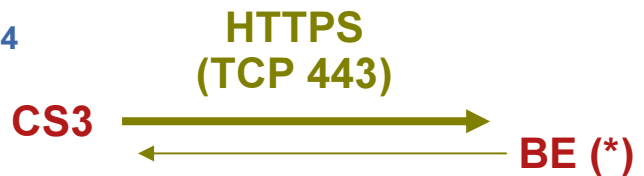
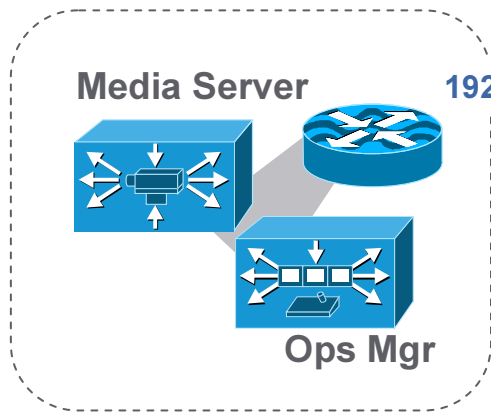
%Warning: portfast should only be enabled on ports connected to a single host. Connecting hubs, concentrators, switches, bridges, etc... to this interface when portfast is enabled, can cause temporary bridging loops. Use with CAUTION

%Portfast has been configured on GigabitEthernet1/0/2 but will only have effect when the interface is in a non-trunking mode.

```
3750-access(config-if)#
```

QoS (DSCP) Settings

Камера/Media Server/Станция оператора



```

class-map match-any VSOM
!
description Video Surveillance Operations Manager
match access-group name HTTP
!
ip access-list extended HTTP
!
    Matches Client requests to Web Server
permit tcp host 192.0.2.34 eq www any
!
policy-map INGRESS_Integrated_Services_Engine
class VSOM
    set ip dscp cs3
class class-default
    set ip dscp cs3
!
interface Integrated-Service-Engine1/0
service-policy input INGRESS_Integrated_Services_Engine
    
```

NME-VMSS-HP16

(*) DSCP not set by camera on control plane

IP Camera Deployment—Egress Queuing

L2 Priority Queue (1P3Q3T)

Рекомендуется использование приоритетных очередей на транковых портах между коммутаторами

```
!  
interface GigabitEthernet1/0/1  
description Uplink port  
switchport trunk encapsulation dot1q  
switchport mode trunk  
load-interval 60  
priority-queue out  
mls qos trust dscp  
!
```

By default,
DSCP values 0-15 are mapped to queue 2 and threshold 1.
DSCP values 16-31 are mapped to queue 3 and threshold 1.
DSCP values 32-39 and 48-63 are mapped to queue 4 and threshold 1.
DSCP values 40-47 are mapped to queue 1 and threshold 1.

DSCP '40' is CS5

Применение PfR



Характеристики видеопотока в MPEG-4

1. Объект-ориентированное кодирование — передает изменения
2. Периодическая синхронизация — отправляется полный фрейм (I-frame)
3. P- и B- фреймы содержат изменения в видеоданных
4. Обычно инкапсулируется в UDP/RTP
5. При тестировании 30 IP пакетов было необходимо для передачи одного I-frame
6. Передача P- или B- фрейма требует одного или нескольких пакетов. Средний размер пакета при тестировании 1054 байта ~ 115 pps от камеры
7. RTP заголовок содержит номер пакета в потоке, таким образом потерянные пакеты известны
8. Потеря пакетов ухудшает качество изображения
9. Допустимы потери в пределах 1%

Приемлемая задержка—Низкие потери



RTT Min/Avg/Max: 64/71/78 ms

Source to Destination Latency one way Min/Avg/Max: 31/35/40 ms

Destination to Source Latency one way Min/Avg/Max: 32/36/42 ms

Source to Destination Jitter Min/Avg/Max: 0/3/8 ms

Destination to Source Jitter Min/Avg/Max: 0/3/9 ms

MOS score: 4.06

Потери 1/10th 1%

IP SLA UDP Jitter

Высокая задержка—Отсутствие потерь



RTT Min/Avg/Max: 252/274/294 ms

Source to Destination Latency one way Min/Avg/Max: 120/135/148 ms

Destination to Source Latency one way Min/Avg/Max: 124/139/153 ms

Source to Destination Jitter Min/Avg/Max: 1/10/25 ms

Destination to Source Jitter Min/Avg/Max: 0/9/25 ms

MOS score: 3.88

IP SLA UDP Jitter

Низкая задержка—Высокие потери



Потери 1%

RTT Min/Avg/Max: 2/2/3 ms

Source to Destination Latency one way Min/Avg/Max: 0/0/0 ms

Destination to Source Latency one way Min/Avg/Max: 0/0/0 ms

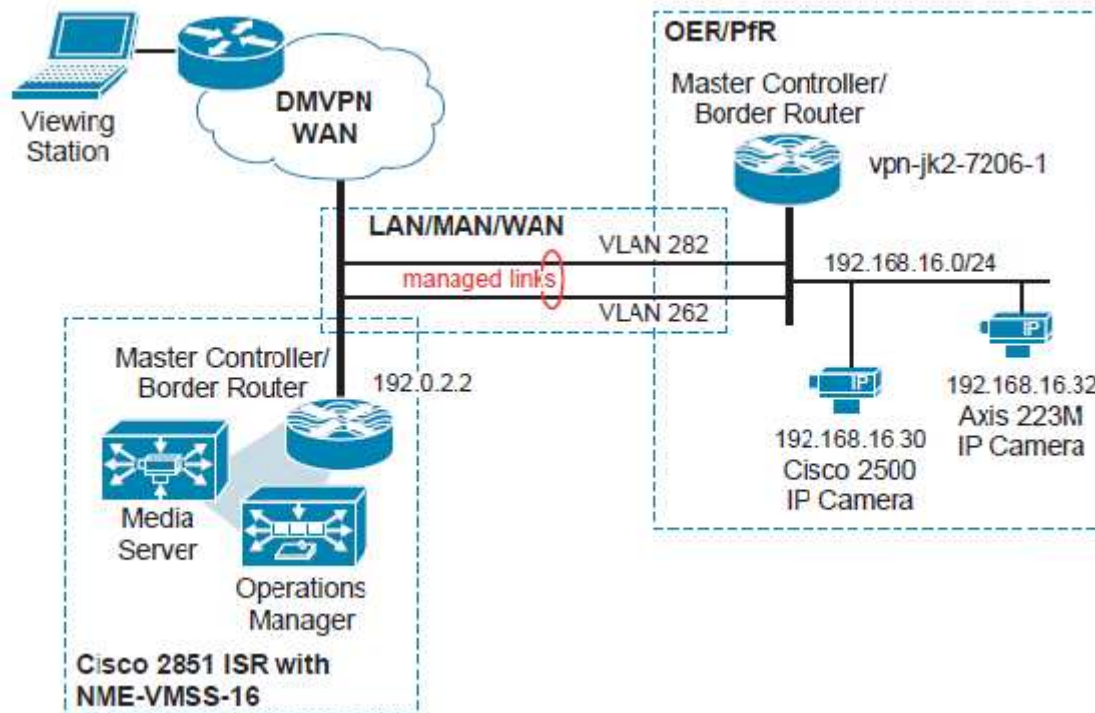
Source to Destination Jitter Min/Avg/Max: 0/1/1 ms

Destination to Source Jitter Min/Avg/Max: 0/1/1 ms

MOS score: 3.76

IP SLA UDP Jitter

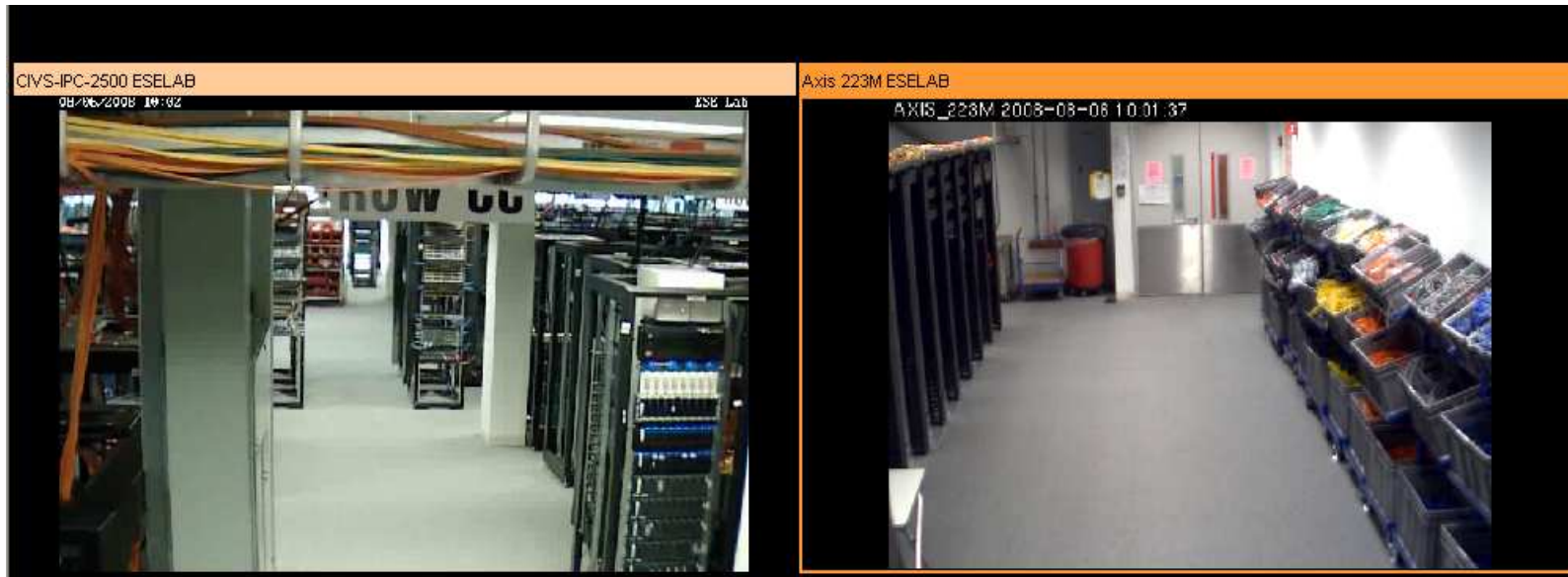
Выбор маршрута без PfR



```
vpn-jk2-7206-1#show oer master border
Border      Status  UP/DOWN      AuthFail  Version
192.168.16.1  INACTIVE SHUTDOWN      0 2.1
```

```
vpn-jk2-7206-1#show ip cef exact-route 192.168.16.30 192.0.2.2
192.168.16.30 -> 192.0.2.2 : FastEthernet0/1.262 (next hop 192.168.12.2)
vpn-jk2-7206-1#show ip cef exact-route 192.168.16.32 192.0.2.2
192.168.16.32 -> 192.0.2.2 : FastEthernet0/1.262 (next hop 192.168.12.2)
```

PfR выбирает канал с наилучшими характеристиками



30
sec.

```
vpn-jk2-7206-1(config-oer-mc)#no shut
vpn-jk2-7206-1(config-oer-mc)#
Aug 12 11:04:48.110 edt: %OER_MC-5-NOTICE: System enabled
Aug 12 11:04:51.870 edt: %OER_MC-5-NOTICE: BR 192.168.16.1 UP
...
Aug 12 11:04:52.062 edt: %OER_MC-5-NOTICE: Uncontrol Prefix 192.0.2.0/27, Traffic Class in Fast Mode
Aug 12 11:05:18.306 edt: %OER_MC-5-NOTICE: Route changed Prefix 192.0.2.0/27, BR 192.168.16.1, i/f Fa0/1.282, Reason None, OOP Reason Timer Expired
```

route
change

Состояние префиксов

```
vpn-jk2-7206-1#show oer master prefix
```

```
OER Prefix Statistics:
```

```
Pas - Passive, Act - Active, S - Short term, L - Long term, Dly - Delay (ms),
```

```
P - Percentage below threshold, Jit - Jitter (ms),
```

```
MOS - Mean Opinion Score
```

```
Los - Packet Loss (packets-per-million), Un - Unreachable (flows-per-million),
```

```
E - Egress, I - Ingress, Bw - Bandwidth (kbps), N - Not applicable
```

```
U - unknown, * - uncontrolled, + - control more specific, @ - active probe all
```

```
# - Prefix monitor mode is Special, & - Blackholed Prefix
```

```
% - Force Next-Hop, ^ - Prefix is denied
```

Prefix	State	Time	Curr BR	CurrI/F			Protocol
	PasSDly	PasLDly	PasSUn	PasLUn	PasSLos	PasLLos	
	ActSDly	ActLDly	ActSUn	ActLUn	EBw	IBw	
	ActSJit	ActPMOS	ActSLos	ActLLos			

192.0.2.0/27	HOLDDOWN	@106	192.168.16.1	Fa0/1.282			STATIC
	U	U	0	0	0	0	0
	72	72	0	0	723	1	
	3	0	0	0			

Current exit is Fa0/1.282 – it has 72ms latency, 3ms jitter and 0 loss

show oer master prefix 192.0.2.0/27 detail

Виртуализация и криптование



Виртуализация

1. Policy-based виртуализация

Ограничение передачи трафика в определенном направлении

Ограничение на основе правил и административных политик.

Пример: Листы контроля доступа, Межсетевые экраны

2. Control plane-based виртуализация

Ограничивает распространение информации о маршрутах

Виртуализированные таблицы маршрутизации

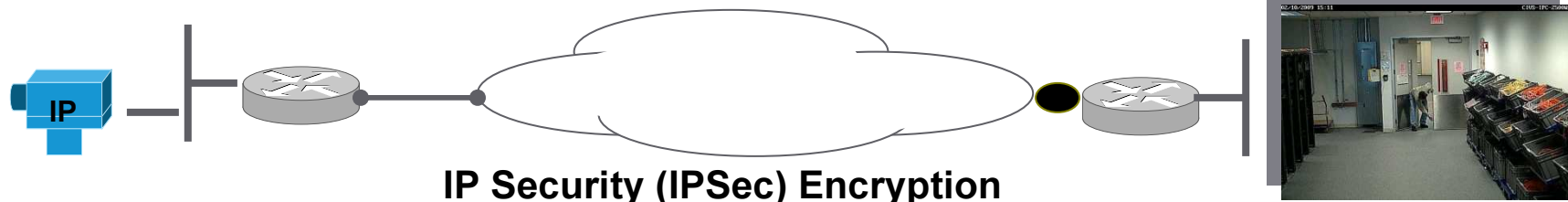
Пример: VPN Routing and Forwarding (*VRF*)

Методы достижения конфиденциальности видеоданных

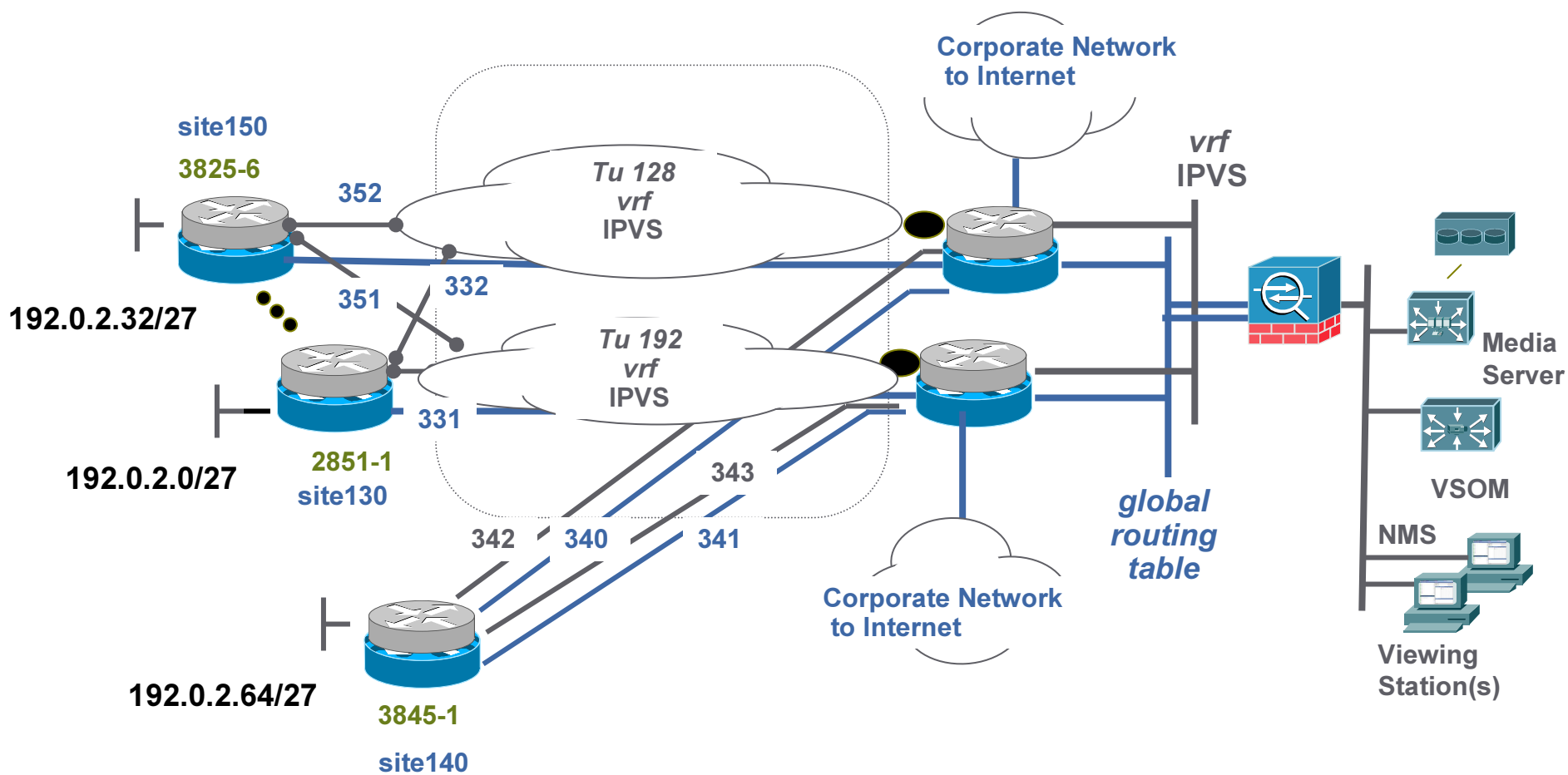
Криптование

1. Криптование обеспечивает конфиденциальность данных (видео)
2. Цифровые сертификаты обеспечивают аутентичность и целостность
3. DMVPN, IPSec/GRE, static VTI are logical tunnels

Изоляция трафика { Множество туннелей может быть создано через один физический канал
Каждый туннель может находиться в отдельном *VRF*



Изоляция трафика Layer-3 virtualization



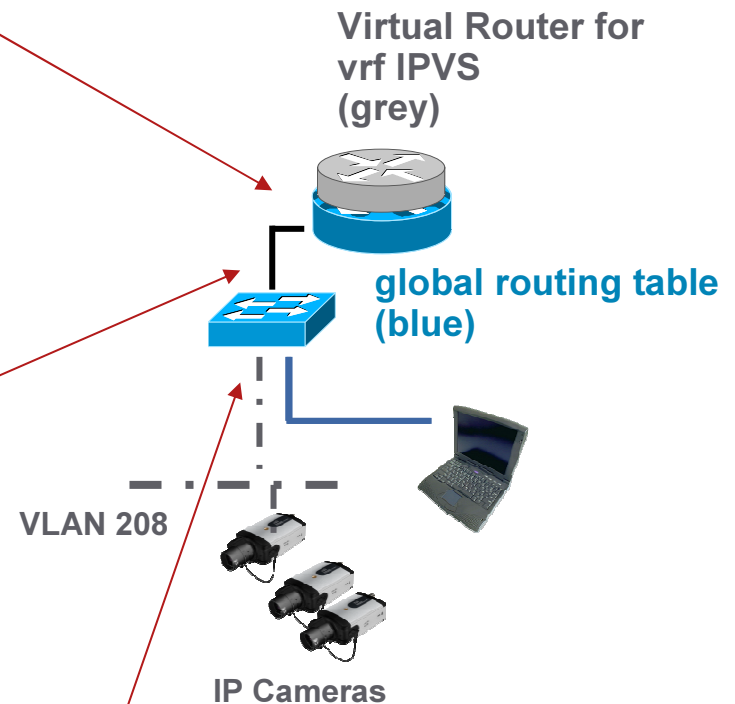
VPN Routing and Forwarding (VRF)

Mapping Layer-2 (VLAN) to Layer-3 (VRF)

```
vpn4-3800-6#sh run int gigabitEthernet 0/0.208
!  
interface GigabitEthernet0/0.208  
description inside interface for ip cameras  
encapsulation dot1Q 208  
ip vrf forwarding IPVS  
ip address 192.0.2.49 255.255.255.240
```

```
!  
interface GigabitEthernet1/0/1  
description trunk to vpn4-3800-6  
switchport trunk encapsulation dot1q  
switchport mode trunk  
load-interval 60  
priority-queue out  
mls qos trust dscp  
end
```

```
!  
interface GigabitEthernet1/0/2  
description CIVS-IPC-2500  
switchport access vlan 208  
switchport mode access  
end
```

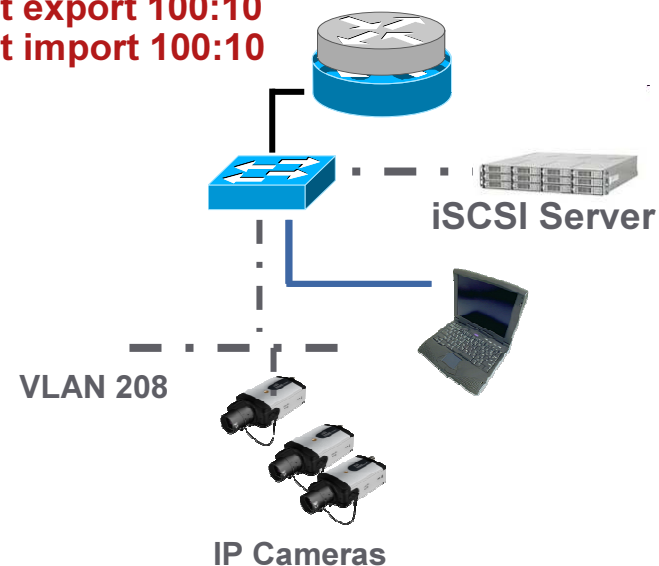


Logical / Management Interface Configuration

All surveillance devices in VRF IPVS

```
!  
interface GigabitEthernet0/0.258  
  description iSCSI Management Subnet  
  encapsulation dot1Q 258  
  ip vrf forwarding IPVS  
  ip address 192.168.211.1 255.255.255.0  
!  
interface Video-Service-Engine1/0      EVM-IPVS-16A  
  ip vrf forwarding IPVS  
  ip address 192.0.2.37 255.255.255.252  
  ip route-cache flow  
  service-module ip address 192.0.2.38 255.255.255.252  
  service-module ip default-gateway 192.0.2.37  
  no keepalive  
!  
interface Integrated-Service-Engine2/0  NME-VMSS-HP16  
  ip vrf forwarding IPVS  
  ip address 192.0.2.33 255.255.255.252  
  ip route-cache flow  
  service-module external ip address 192.168.211.2 255.255.255.0  
  service-module ip address 192.0.2.34 255.255.255.252  
  service-module ip default-gateway 192.0.2.33  
  no keepalive  
!
```

```
hostname vpn4-3800-6  
!  
ip vrf IPVS  
  rd 100:10  
  route-target export 100:10  
  route-target import 100:10  
!
```

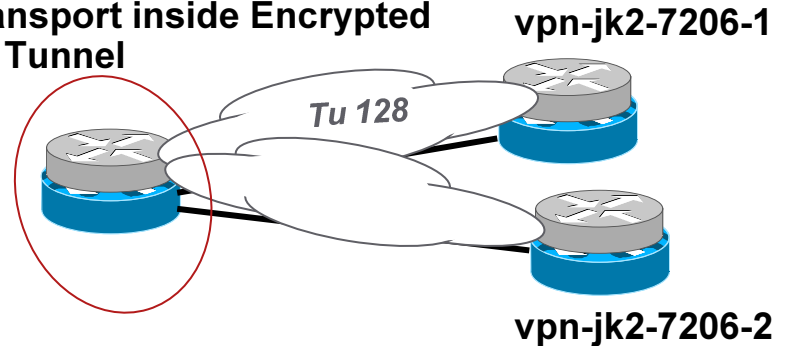


DMVPN Tunnel in VRF IPVS

Tunnel endpoints in Global Routing Table

```
!  
interface GigabitEthernet0/1.332  
  encapsulation dot1Q 332  
  ip address 192.168.15.46 255.255.255.252  
!  
!  
interface Tunnel128  
  ip vrf forwarding IPVS  
  ip address 192.168.15.130 255.255.255.192  
  ip mtu 1400  
  ip nhrp authentication FOO  
  ip nhrp map 192.168.15.129 192.168.15.40  
  ip nhrp map multicast 192.168.15.40  
  ip nhrp network-id 128  
  ip nhrp nhs 192.168.15.129  
  ip summary-address eigrp 65 192.0.2.0 255.255.255.224 5  
  tunnel source GigabitEthernet0/1.332  
  tunnel destination 192.168.15.40  
  tunnel key 128  
  tunnel protection ipsec profile IPVS_Branches_ipsec_profile  
!  
ip route 192.168.15.40 255.255.255.255 192.168.15.45 name vpn-jk2-7206-1_Loopback_0
```

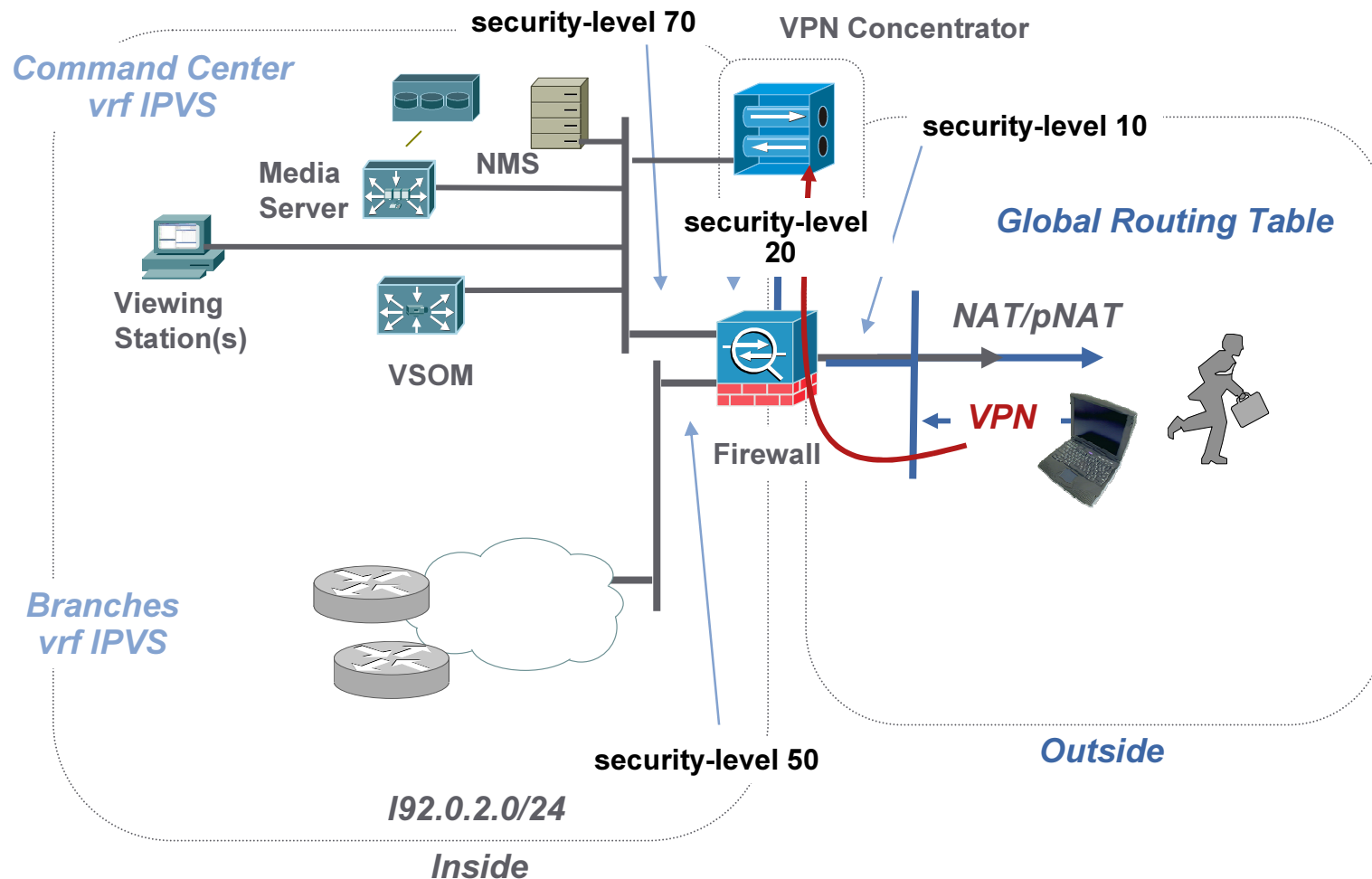
IP Video Surveillance Traffic
WAN transport inside Encrypted
DMVPN Tunnel



Second
tunnel / HE not shown
- similarly configured

Firewall – VRF – VPN Concentrator

Extranet / Internet User access to Video Feeds



Video Surveillance Operations Manager - Windows Internet Explorer

http://192.0.2.65/vsom/

File Edit View Favorites Tools Help

Google

Video Surveillance Operations Manager

CISCO Video Surveillance Operations Manager

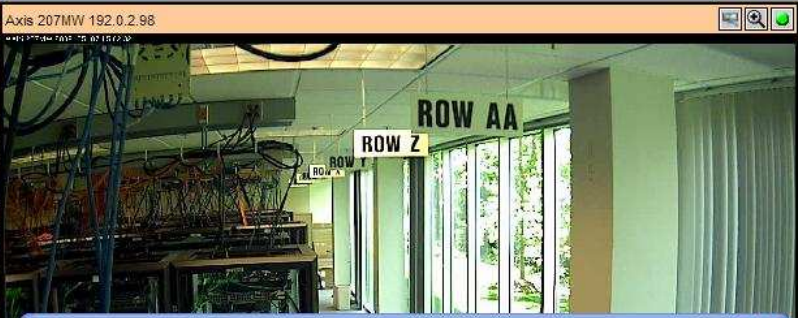
Predefined Views

- #4 2-1
- #3 2Across
- #2 2UP
- #1 single

Camera Feeds

- Expand All
- Axis 207 192.0.2.99
- Axis 207MW 192.0.2.98
- Axis 223M ESELAB
- CIVS-IPC-2500W_1 192.0.2.100
- CIVS-IPC-2500W_2
- CIVS-IPC-2500W_3

Video Archives



status: Connected | VPN Client - Version 5.0.05.0290

Connection Entries Status Certificates Log Options Help

Disconnect New Import Modify Delete

Connection Entry	Host	Transport
DMZ_VPN3080	10.81.7.57	IPSec/UDP

Connected to "DMZ_VPN3080". Connected Time: 0 day(s), 00:06.22

Windows Task Manager

File Options View Help

Applications Processes Performance **Networking**

Local Area Connection

Local Area Connection 3

Adapter Name	Network Utiliz...	Link Sp...	State
Local Area Con...	0 %	100 Mbps	Operational
Local Area Con...	6 %	100 Mbps	Operational

Processes: 61 CPU Usage: 25% Commit Charge: 503M / 3907M



VPN Client | Statistics

Tunnel Details Route Details Firewall

Address Information		Connection Information	
Client:	192.168.15.66	Entry:	DMZ_VPN3080
Server:	10.81.7.57	Time:	0 day(s), 00:06.22
Bytes		Crypto	
Received:	167928556	Encryption:	168-bit 3-DES
Sent:	5524798	Authentication:	HMAC-MD5
Packets		Transport	
Encrypted:	131729	Transparent Tunneling:	Inactive
Decrypted:	131817	Local LAN:	Disabled
Discarded:	102	Compression:	None
Bypassed:	23		

Reset Close

start | Command Prompt | Video Surveillance Op... | status: Connected | ... | Windows Task Manager | 100% | 3:02 PM

Заклучение



Key Points

1. IP Сеть позволяет получить доступ к видео в любое время из любого места через надежную, резервируемую и безопасную инфраструктуру. Сервисы IP сети дают возможность централизованного управления, мониторинга и качественного планирования ресурсов
2. Видеопотоки обладают определенной спецификой, которую необходимо учитывать при планировании QoS
3. Критично минимизировать потери пакетов при передаче видео. PfR является эффективным инструментом для выбора наилучшего канала связи
4. Традиционно системы видеонаблюдения являлись изолированными. Виртуализация дает возможность изолировать видеопотоки в конвергентной сети, а шифрование обеспечивает их конфиденциальность
5. Интеграция видеонаблюдения с другими системами делает его более проактивным и добавляет новые возможности

Дополнительная информация

www.cisco.com/go/designzone

Design Zone - Cisco Systems - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.cisco.com/en/US/netsol/ns742/networking_solutions_program_category_home.html

Worldwide [change] Log In | Account | Register | About Cisco

Search Go

Solutions Products & Services Ordering Support Training & Events Partner Central My Cisco

HOME

SOLUTIONS

ENTERPRISE

PROGRAMS FOR ENTERPRISE

AssureWave Testing

CIO Thought Leadership

Cisco Interoperability Portal

Design Zone

Interaction Network

Managed Services for Enterprise

Media Center

Safe Harbor Testing

Design Zone

Introduction

Technical Resources for the Enterprise

Design Zone is a consolidated resource for design guides, application deployment guides, white papers, videos, and other technical reference materials. Refer to the categories organized under network architectures, technologies, and industry solutions for specific resources.

Network Architectures

[Design Zone for Branch](#)

[Design Zone for Campus](#)

[Design Zone for Data Centers](#)

[Design Zone for WAN/MAN](#)

Technologies

[Design Zone for Interoperability Systems](#)

[Design Zone for Security](#)

[Design Zone for Mobility](#)

[Design Zone for Sustainability](#)

[Design Zone for Unified Communications](#)

[Design Zone for Video](#)

Industry Solutions

[Design Zone for Education](#)

[Design Zone for Financial Services](#)

[Design Zone for Government](#)

Related Links

[Products and Services](#)

[Cisco Services](#)

[Service Oriented Network Architecture](#)

[Places in the Network](#)

[SMB Smart Designs](#)

[All Cisco Validated Designs](#)

Advancing Productivity and Innovation

Explore why The Economist says collaboration is changing how business works.

[Sign Up Now](#)

Accelerate Your Business

Design Zone for Video

Cisco Validated Design Program

Cisco tests and validates architecture- and solution-level designs from technology solutions.

[Learn About the Program](#)

Featured Content

Interactive Design and Solutions Guidance

SONA Podcast Series

Learn more about specific Cisco Validated Design topics.

