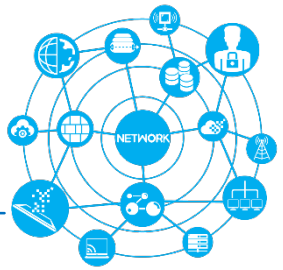
Programmazione & Sicurezza delle Reti
nella Grande Azienda

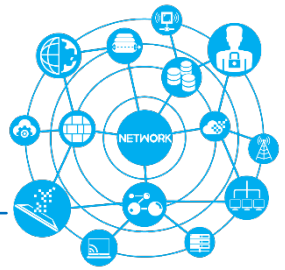
Marco Zardini
Local IT Service Manager - Italy & South Europe
GlaxoSmithKline S.p.A.

www.gsk.it - www.gsk.com

AGENDA



- Progettazione, implementazione e management della rete LAN/WAN con i requirements di Business Continuity e Disaster Recovery
  - Standard Framework
  - Concetti di Business Continuity e Disaster Recovery
  - Analisi dei bisogni (business requirements)
  - Principi di progettazione e implementazione
  - Service model: maintenance e incident management
- Applicazioni Client Server e distribuite
  - Definizioni e Terminologie
  - L’esperienza dei webinar
- Info-Protect
  - Gestione e Protezione delle Informazioni
  - Catalogazione delle Informazioni

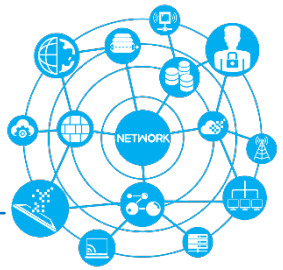


Progettazione, implementazione e management della rete LAN/WAN

…con i requirements di Business Continuity e Disaster Recovery

Standard Framework

Project & Service Management



Project Management

Requirements → Proposal (STP) → Project Approval

Design & Planning → Implementation & Test → GoLive & Tuning

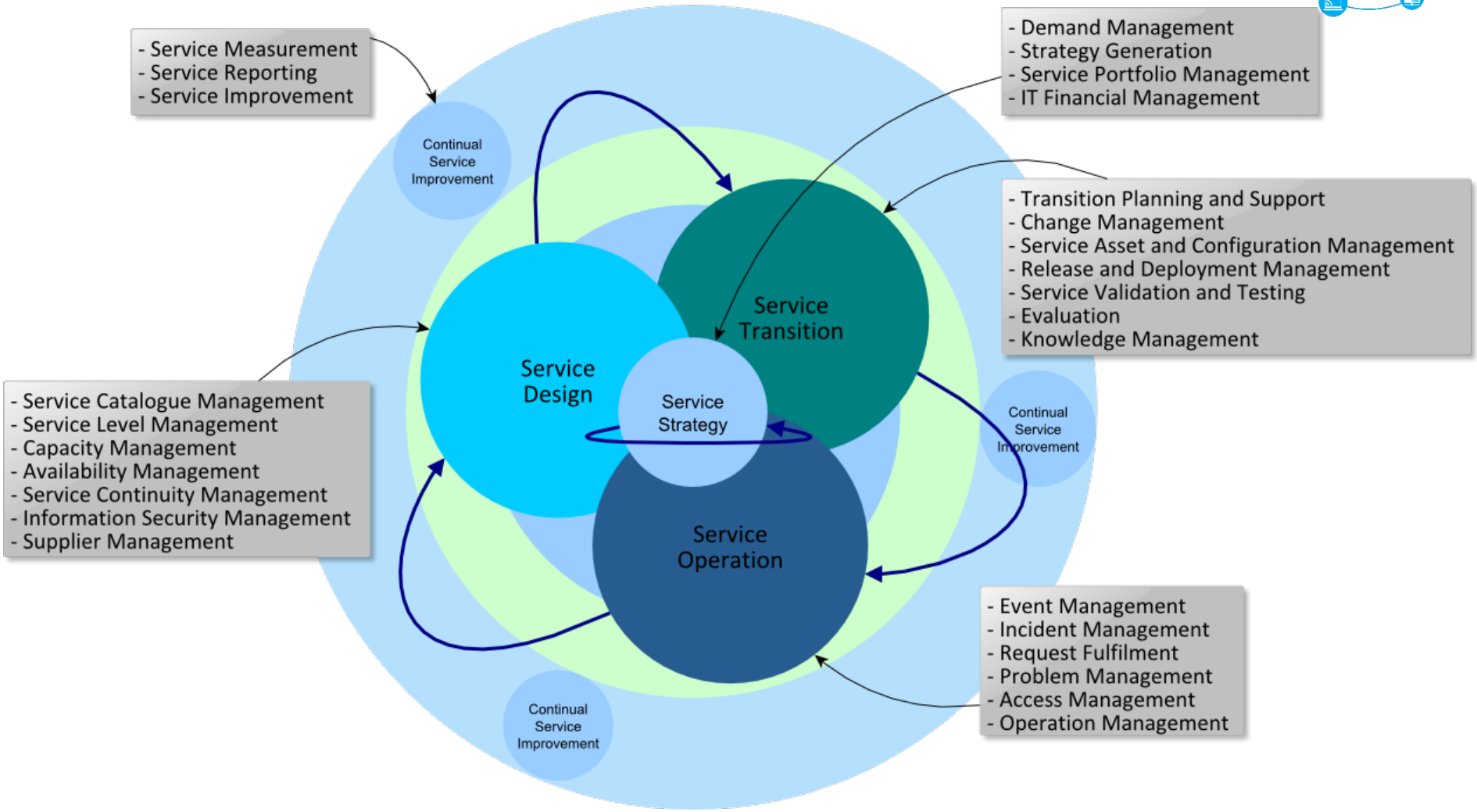
Service Management

- Maintenance
- Incident Management
- KPI (Key Performance Indicator)
- VoC (Voice of the Customers)
- Service Improvment

ITIL → **I**nformation **T**echnology **I**nfrastructure **L**ibrary

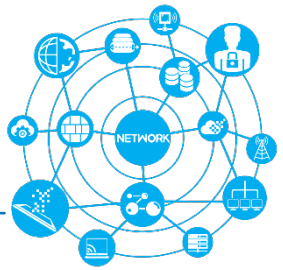
Standard Framework - ITIL

Best practice for IT Service Management



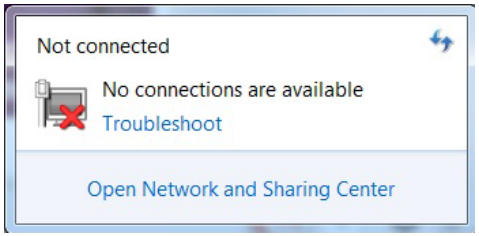
Business Continuity (1)

Definizione



DOMANDA: Quale ‘danno’ al Business Aziendale può derivare dalla **indisponibilità *prolungata*** di un suo processo o di un servizio specifico?

OVVERO: Qual è il ‘danno’ che può derivare dalla indisponibilità prolungata di una **applicazione** e/o della perdita dei **dati**?



Business Continuity Management

- Utilizza modelli orientati alla **identificazione dei rischi** e all’analisi dei **potenziali impatti** (su un’organizzazione, un ente o un sistema).
- Lo scopo è di assicurarne la **resilienza**, ovvero la capacità di rispondere efficacemente a guasti importanti o eventi disastrosi.

Standard di riferimento:
ISO 22301 (2012) Business Continuity Management
(replace BS 25999-2)

Business Continuity (2)

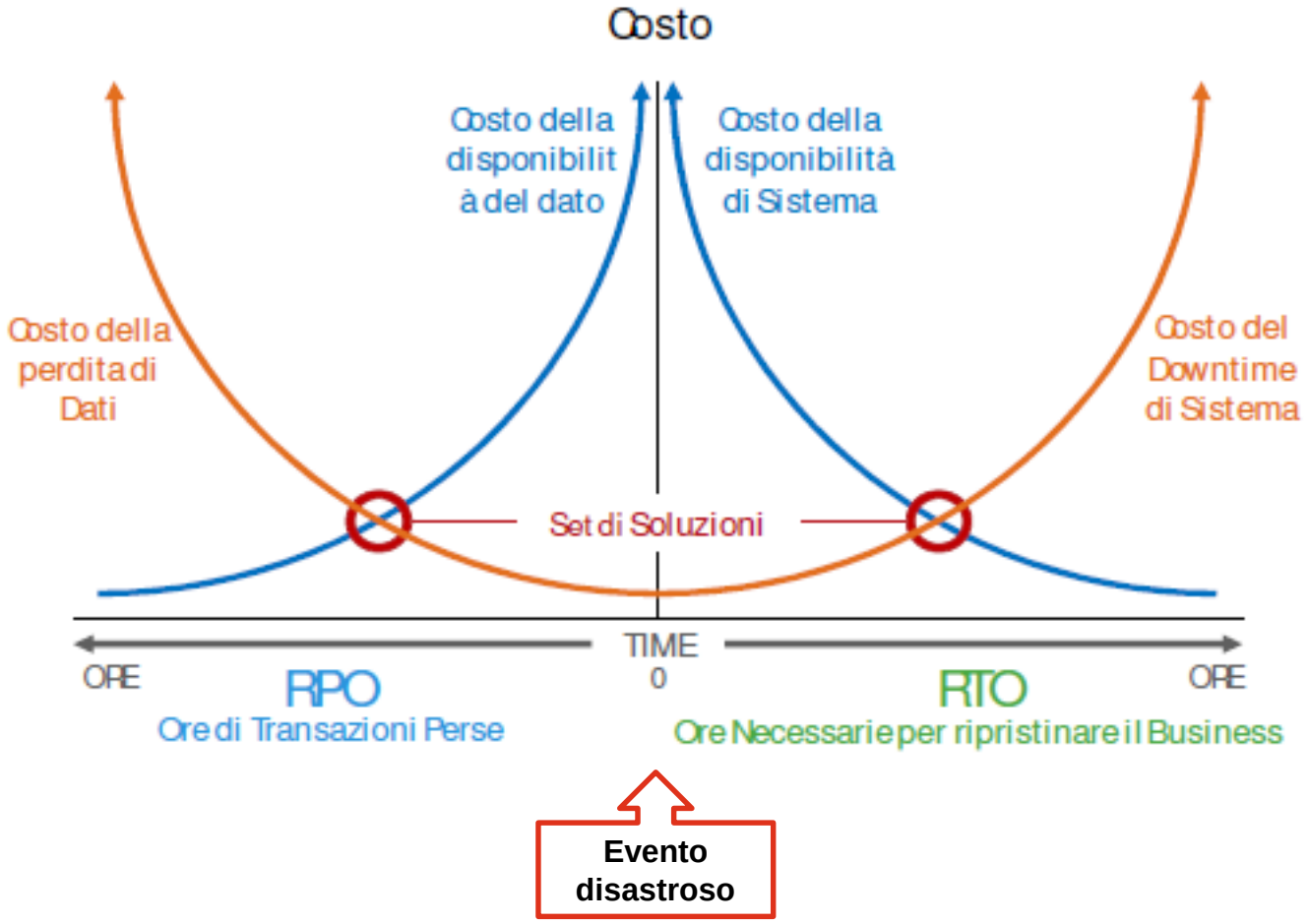
Definizione

OUTPUT:

- Gli **impatti** (economico/finanziari, legali, reputazione, safety, etc), che si possono subire nel caso di mancata erogazione del processo, della perdita di un sistema, etc.
- L'**RTO** (Recovery Time Objective = acceptable amount of time to restore the function), ovvero misura il periodo masimo di fermo accettabile di un processo o servizio.
- L'**RPO** (Recovery Point Objective = acceptable latency of data that will be recovered) indica il punto al quale viene recuperata la determinata attività / processo critico in termini di informazioni disponibili/file storici recuperati
- Le **risorse** necessarie per il funzionamento del processo o sistema (assets critici, funzioni di suppporto, terse parti, etc.).
- Eventuali **correlazioni** con altri processi o sistemi.

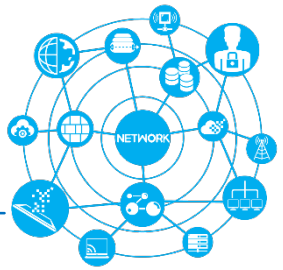
Business Continuity

RPO/RTO & Costs



Requirements

Analisi dei bisogni



Chi / Cosa / Dove / Come / Quando / Criticità & Disponibilità

OUTPUT

- Numero di utenti & contemporaneità (entità)
- Location (una sede, multi-sede → connessioni geografiche e/o accesso remoto)
- Hardware che andrà in rete (Tipologia di PC, Server, Periferiche, building automation, controllo accessi, videosorveglianza, facilities services, etc)
- Accesso a sistemi/servizi locali, centrali, cloud o terze parti (firewalling, B2B, VPN)
- Sistemi Operativi coinvolti (Microsoft, Unix, Apple, …NAS, DB)
- Definizione degli utenti, la tipologia di accesso, autenticazione e autorizzazione

- Mileston del Project Plan
- Budget

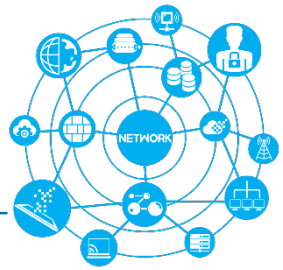
- Availability (disponibilità)
- Reliability (affidabilità)
- RTO & RPO

BACKGROUND

- Standard o Procedure comuni
  (Policy, Standard Operating Procedure – SOP, Guideline)

Principi di progettazione

Da dove si parte?



…si parte dai **REQUIREMENTS** !!!

Elemento ‘focalizzante’?

- **DATI**
- ma anche le **Applicazioni** !!!

E quali sono i loro ‘elementi caratterizzanti’ che ci interessano ???

- Grado di importanza (strategica, riservatezza, unicità, etc.)
- Dove risiedono
- Availability (disponibilità / performance)
- Piani di ‘Disaster Recovery’ (di processo, applicativi, etc.)

NB: una rete LAN/WAN è una ‘**infrastruttura di supporto**’

Esempi:

BackUp dei dati:

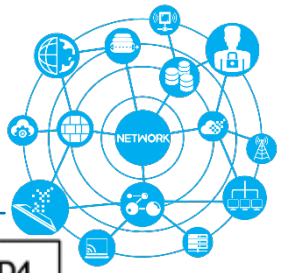
1) Tape off-site (RTO di giorni)
2) SAN - Copy Asincrono (RTO di poche ore)
3) SAN - Copy Sincrono (RTO di pochi minuti)
4) Cluster (RTO tendente a zero)

Server Applicativi:

1) Virtualizzazati (ie VMWARE)
2) Replica fisica dei Server (‘clonazione’)

Implementazione: modello di riferimento

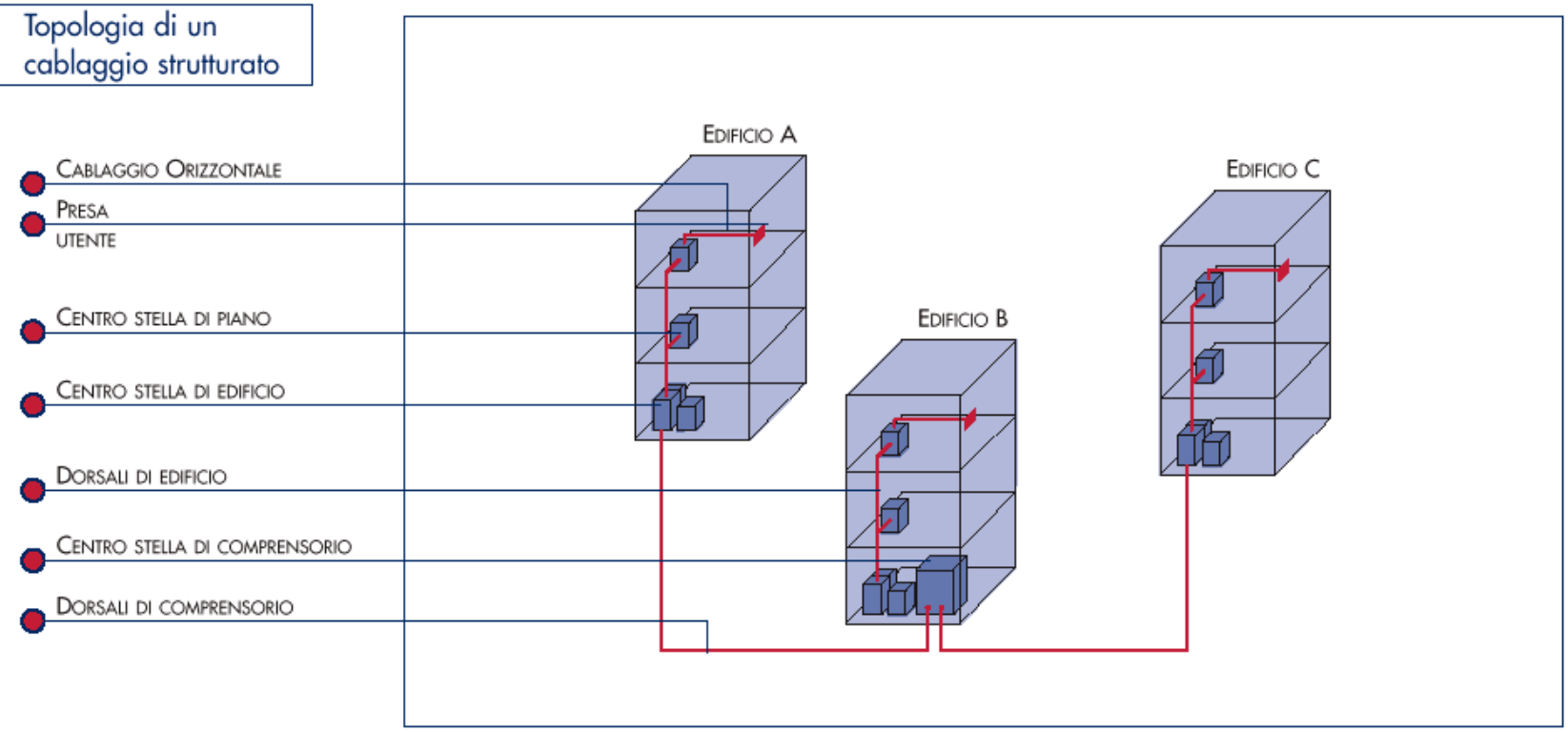
Infrastruttura passiva



Layer	Application/Example		Central Device/ Protocols		DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP	GATEWAY	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT		
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names		
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP		Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP	Can be used on all layers	Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch Bridge WAP** PPP/SLIP	Land Based Layers	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**		

Infrastruttura passiva

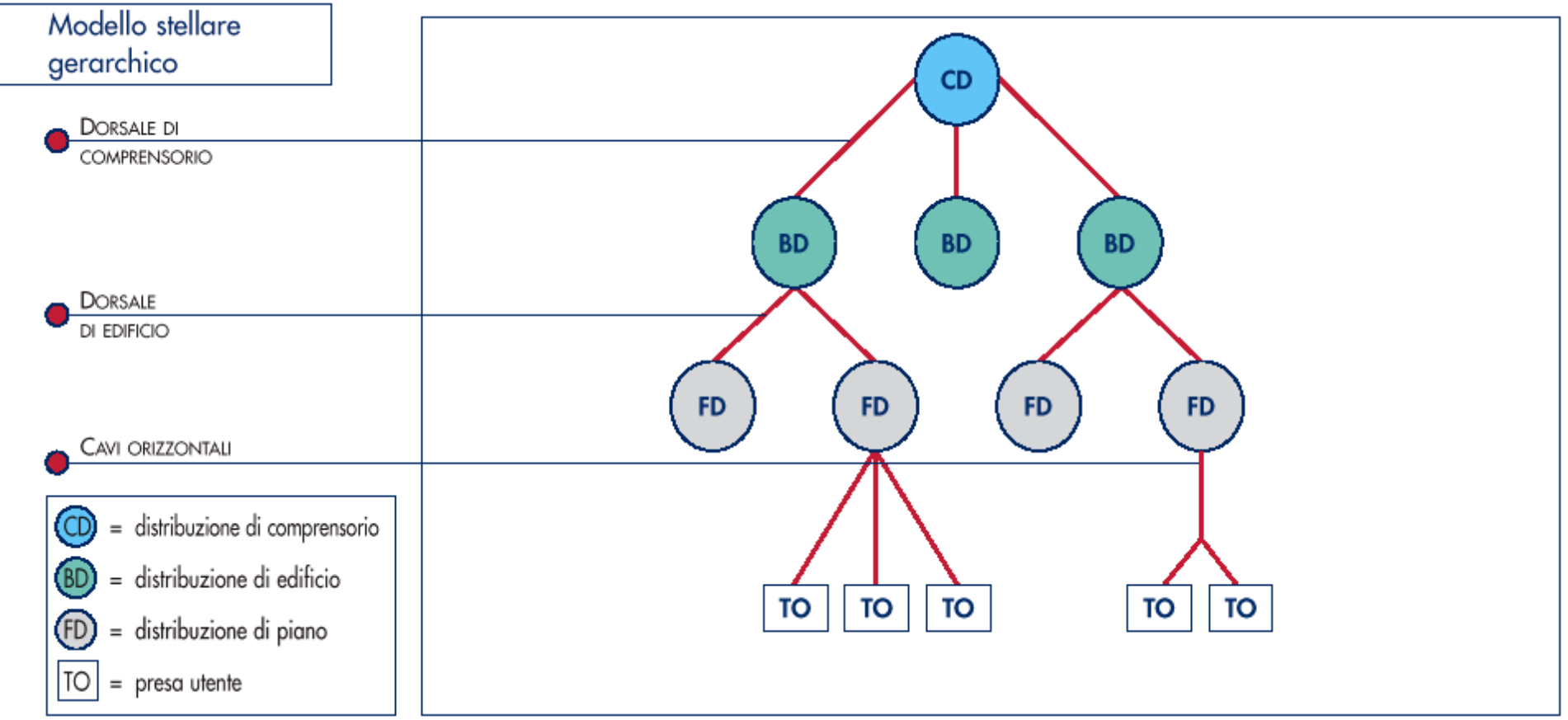
Campus distribution



- Integra diversi sistemi/servizi: rete dati, telefonia (IPT), videosorgeglianza, controllo accessi, facility automation, automazione industriale (SCADA), etc.
- Standard → EN 50173 o ISO/IEC 11801: differiscono per la nomenclatura ma anche per per alcuni vincoli qulitativi sulle prestazioni dei collegamenti [impedenze, attenuazione, return loss, diafonía, NEXT (near end cross talk) ACR (Attenuation to Cross talk Ratio), etc.]…

Infrastruttura passiva

Campus distribution



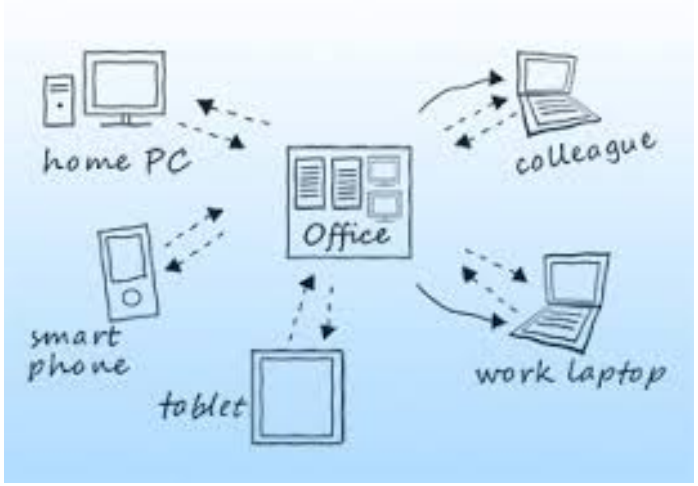
Implementazione Infrastruttura Passiva (1)

Secondo i principi di DR

Scenario di riferimento	RTO	Strategia
Work Area / building 'secondari' non accessibili → incendio, allagamento, contaminazione, indisponibilità delle facilities.	1-5 giorni	Spostare le persone in altre aree

Architettura

1) Spazi 'free' disponibili → sale riunioni, aree uffici non utilizzate, etc.
2) Network device 'spare' (hub/switch)
3) Utilizzo della rete Wireless
4) Telelavoro (remote working) → Laptop & infrastruttura di accesso remoto

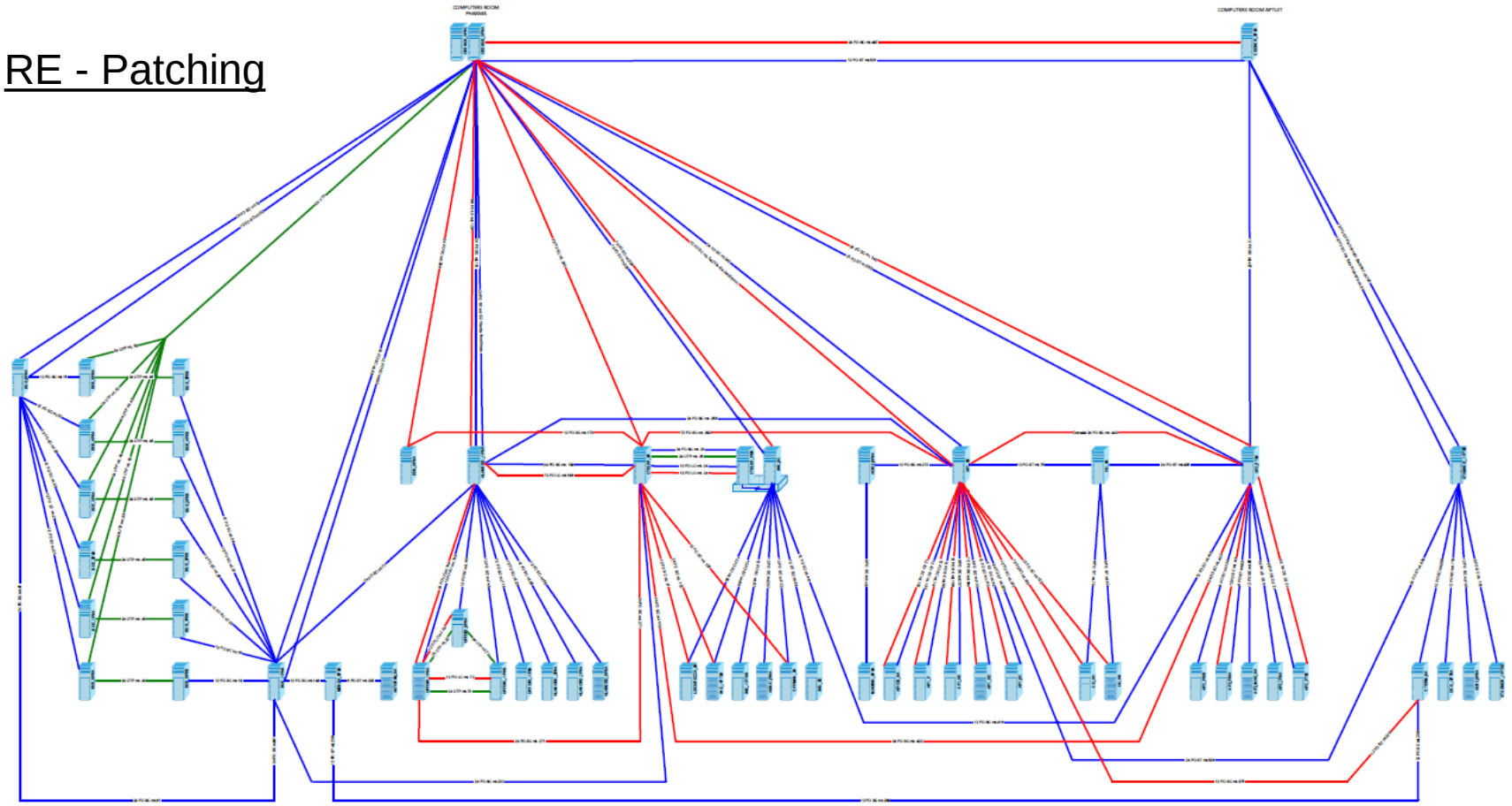


Implementazione Infrastruttura Passiva (2)

Secondo i principi di DR

Scenario di riferimento	RTO	Strategia
Distruzione del ‘backbone building distribution’ → incendio	< 1 giorno	Backbone building distribution ridondata su percorsi alternativi

Architettura



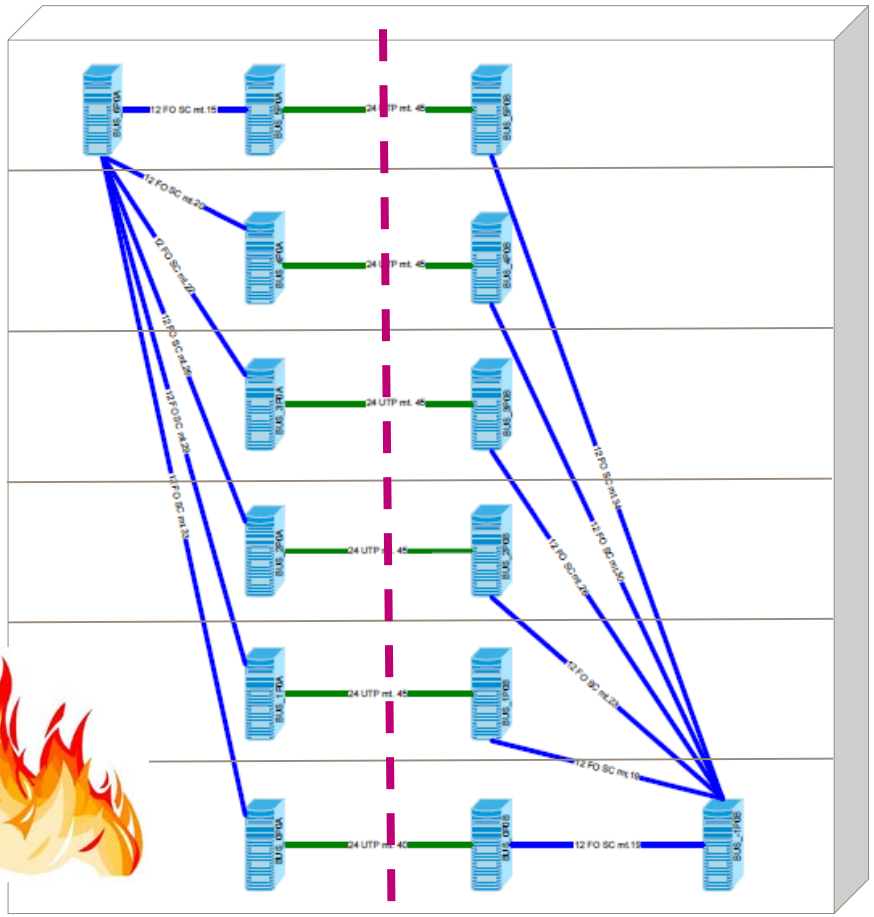
Implementazione Infrastruttura Passiva (2)

Secondo i principi di DR

Scenario di riferimento	RTO	Strategia
Distruzione del ‘backbone building distribution’ → incendio di una sezione (area limitata) del bulding	< 1 giorno	Backbone building distribution ridondata su percorsi alternativi

Architettura

Sezione A



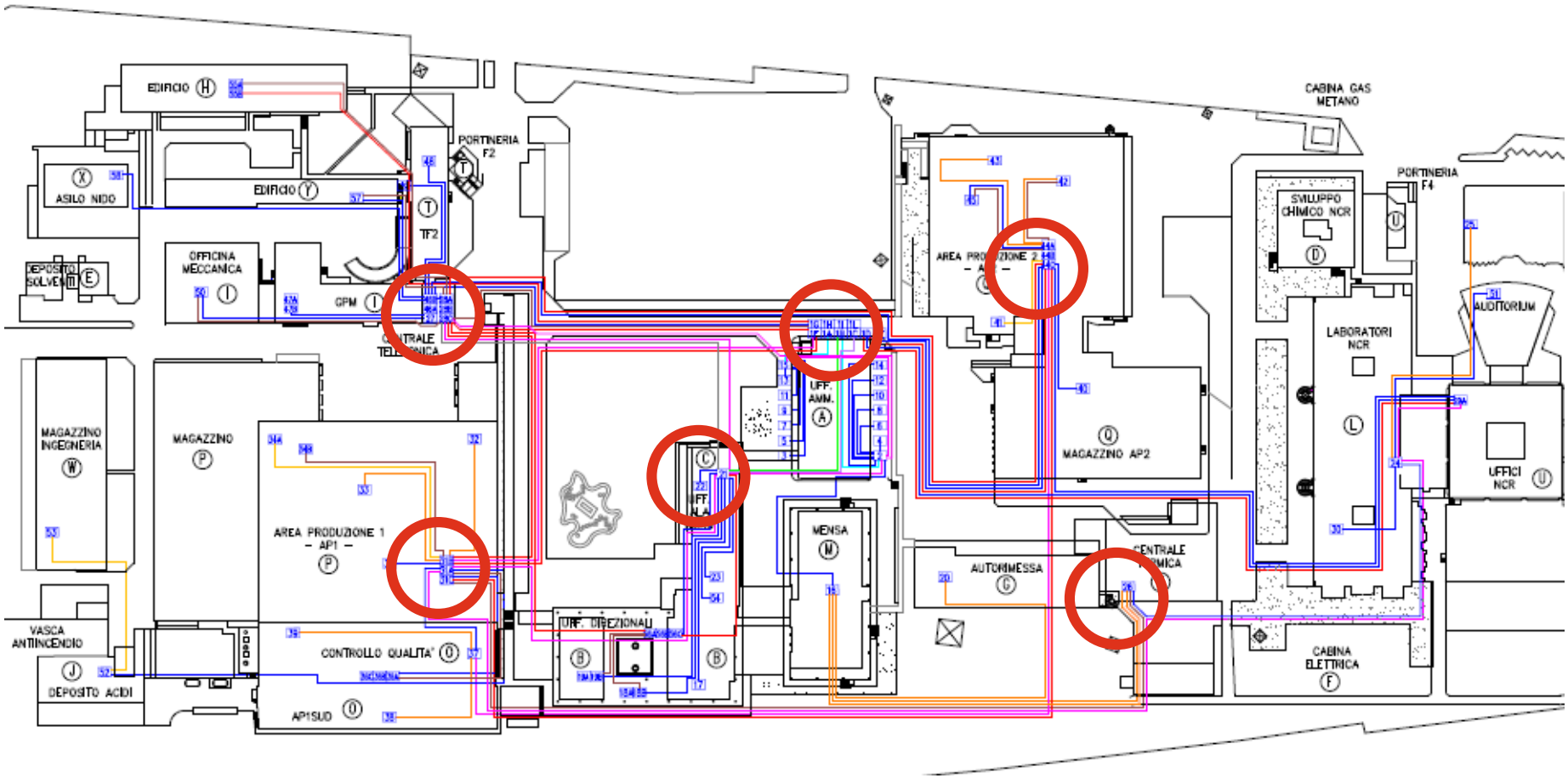
Sezione B

Implementazione Infrastruttura Passiva (3)

Secondo i principi di DR

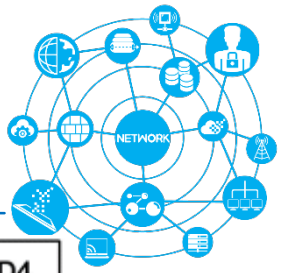
Scenario di riferimento	RTO	Strategia
Distruzione del 'backbone campus distribution' → incendio, guasto fisico sulle vie-cavo interrate, etc.	< 1 giorno	Backbone campus distribution ridondata su percorsi alternativi

Architettura



Implementazione

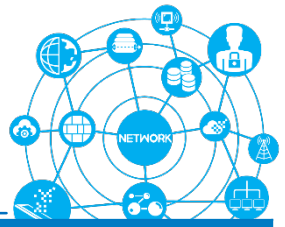
Infrastruttura attiva



Layer	Application/Example		Central Device/ Protocols		DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP	GATEWAY	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT		
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names		
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP		Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP	Can be used on all layers	Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch Bridge WAP** PPP/SLIP	Land Based Layers	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**		

Implementazione Infrastruttura Attiva (1)

Data Link / Layer 2



Scenario di riferimento	RTO	Strategia
Distruzione del 'backbone distribution' → incendio, guasto fisico sulle vie-cavo interrate, etc	< 5 min	Utilizzo di Switch & STP (Spanning Tree Protocol)

Architettura

STP è un protocollo di Layer 2 attivo su bridge e switch su una rete Ethernet (IEEE 802.1D).
Il suo scopo è di non creare loop (loop-free topology) quando sono disponibili link ridondanti sul network. Assicura anche la corretta gestione dei pacchetti di broadcast.
Utilizza un algoritmo 'distribuito' con lo scopo che il grafo dei collegamenti disponibili sia coperto da un 'albero'
Secondo una 'gerarchia' fra gli switch, viene individuato (election) un 'root switch' dell'albero che copre e una parte dei collegamenti disponibili viene messa in stato di «blocking».
Nel caso un nodo diventi irraggiungibile lo switch cercherà di ricostruire un percorso alternativo per raggiungerlo.

CONS: tempi di convergenza, traffico di 'servizio' sulla rete → Rapid-STP, OSPF

Spanning Tree Steps

1. Root Bridge election
2. Root Port election
3. Designated Port election
4. Alternative (Blocking) Port election

Root Bridge Election

The bridge with the lowest bridge ID is elected as the root bridge. The bridge ID comprises of the following:

1. Priority number
2. MAC address of bridge/switch

Port status (sequential order):

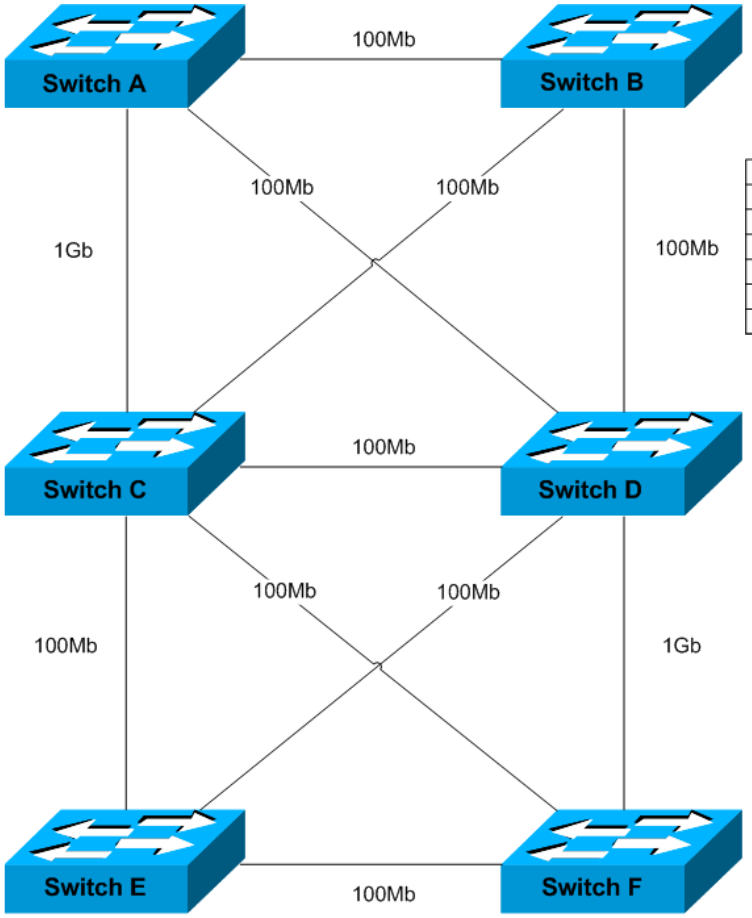
1. Blocking – As the name suggests the port blocks all traffic and does not participate in frame forwarding / receiving. Due to this no MAC address are learnt. Though BPDU`s from neighbouring switches are excepted.
2. Listening – The port still cannot forward or receive frames but can receive and send BPDU`s.
3. Learning – Once the port is in the learning state the port starts learning MAC address.
4. Forwarding – When in the forwarding state the port sends/receives frames and BPDU`s in addition to populating its MAC address table.
5. Disabled – The port is administratively shutdown

Implementazione Infrastruttura Attiva (1)

Data Link / Layer 2

Scenario di riferimento	RTO	Strategia
Distruzione del 'backbone distribution' → incendio, guasto fisico sulle vie-cavo interrate, etc	< 5 min	Utilizzo di Switch & STP (Spanning Tree Protocol)

Architettura



Switch	Bridge ID
Switch A -	32768.aa.aa.aa.aa.aa.aa
Switch B -	32768.bb.bb.bb.bb.bb.bb
Switch C -	32768.cc.cc.cc.cc.cc.cc
Switch D -	32768.dd.dd.dd.dd.dd.dd
Switch E -	32768.ee.ee.ee.ee.ee.ee
Switch F -	32768.ff.ff.ff.ff.ff.ff

Switch-A> (enable)set spantree root 1
VLAN 1 bridge priority set to 8192.
VLAN 1 bridge max aging time set to 20.
VLAN 1 bridge hello time set to 2.
VLAN 1 bridge forward delay set to 15.
Switch is now the root switch for active VLAN 1.
Switch-A> (enable)

Oppure:

Switch-A> (enable)set spantree priority 8192 1
Spantree 1 bridge priority set to 8192.
Switch-A> (enable)

Esempio pratico:

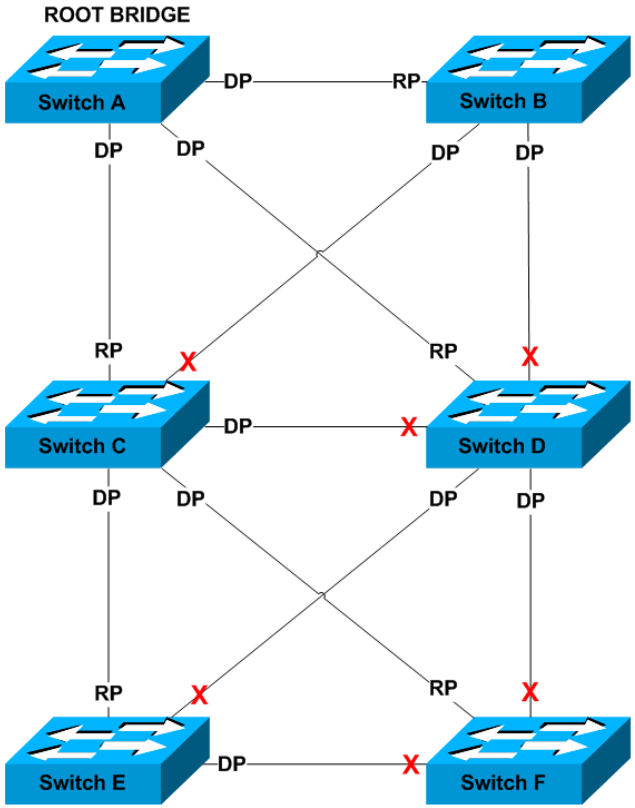
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 118 priority 20480
…
interface GigabitEthernet1/0/3
switchport access vlan 118
switchport mode access

Implementazione Infrastruttura Attiva (1)

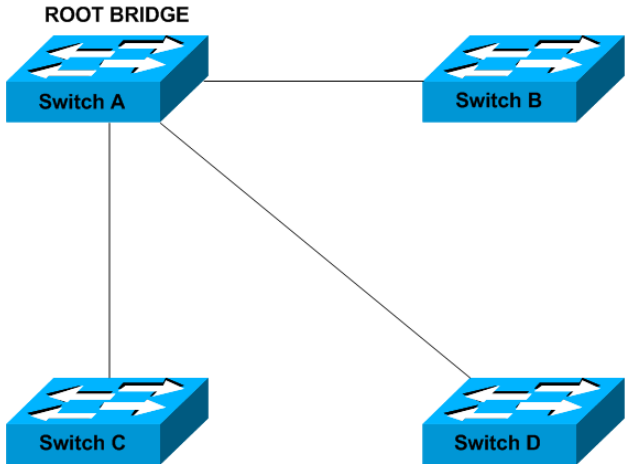
Data Link / Layer 2

Scenario di riferimento	RTO	Strategia
Distruzione del 'backbone distribution' → incendio, guasto fisico sulle vie-cavo interrate, etc	< 5 min	Utilizzo di Switch & STP (Spanning Tree Protocol)

Architettura



Spanning Tree defines 3 port roles: Root Port, Designated Port, Blocking (Alternative Port)



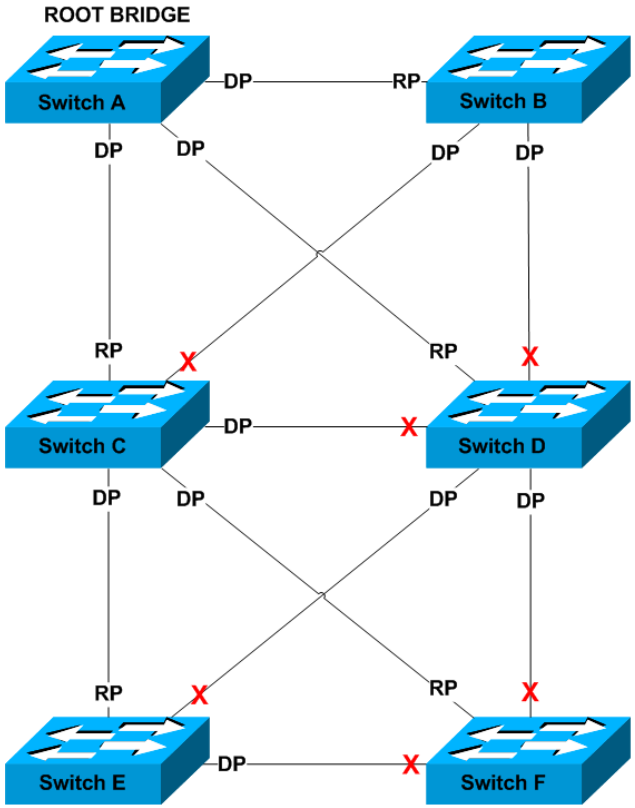
Topologia finale

Implementazione Infrastruttura Attiva (1)

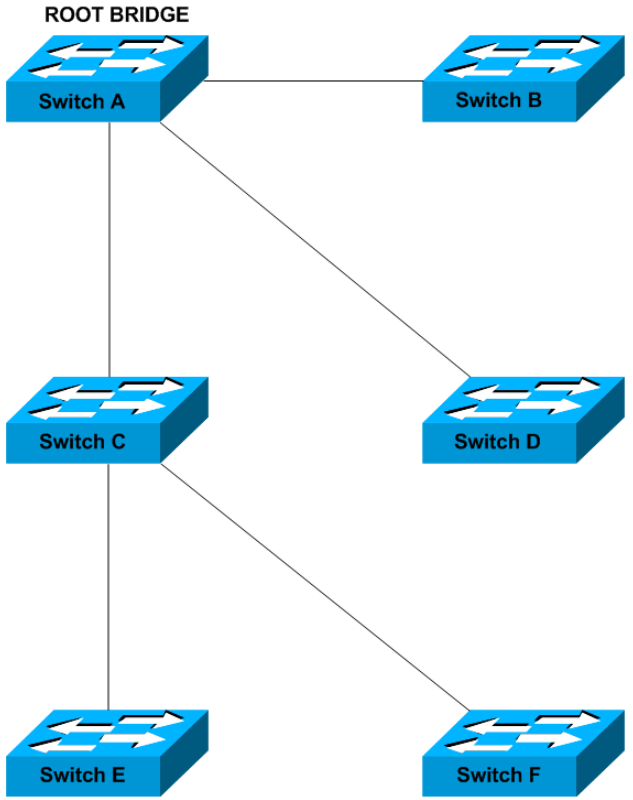
Data Link / Layer 2

Scenario di riferimento	RTO	Strategia
Distruzione del 'backbone distribution' → incendio, guasto fisico sulle vie-cavo interrate, etc	< 5 min	Utilizzo di Switch & STP (Spanning Tree Protocol)

Architettura



Spanning Tree defines 3 port roles: Root Port, Designated Port, Blocking (Alternative Port)



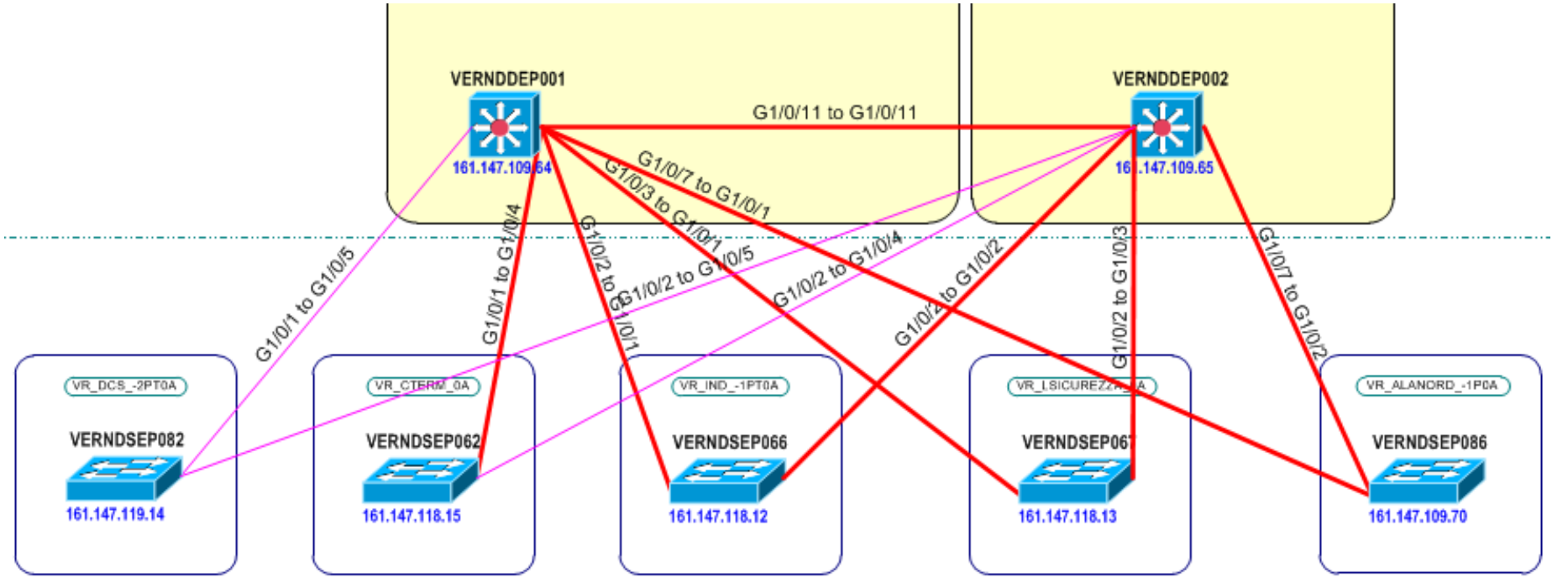
Topologia finale

Implementazione Infrastruttura Attiva (1)

Data Link / Layer 2

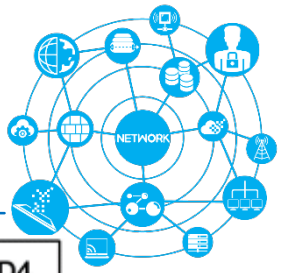
Scenario di riferimento	RTO	Strategia
Distruzione del 'backbone distribution' → incendio, guasto fisico sulle vie-cavo interrate, etc	< 5 min	Utilizzo di Switch & STP (Spanning Tree Protocol)

Architettura



Implementazione

Infrastruttura attiva



Layer	Application/Example		Central Device/ Protocols		DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP	GATEWAY	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT		
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names		
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP		Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP	Can be used on all layers	Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch Bridge WAP** PPP/SLIP	Land Based Layers	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**		

Implementazione Infrastruttura Attiva (2)

Network / Layer 3

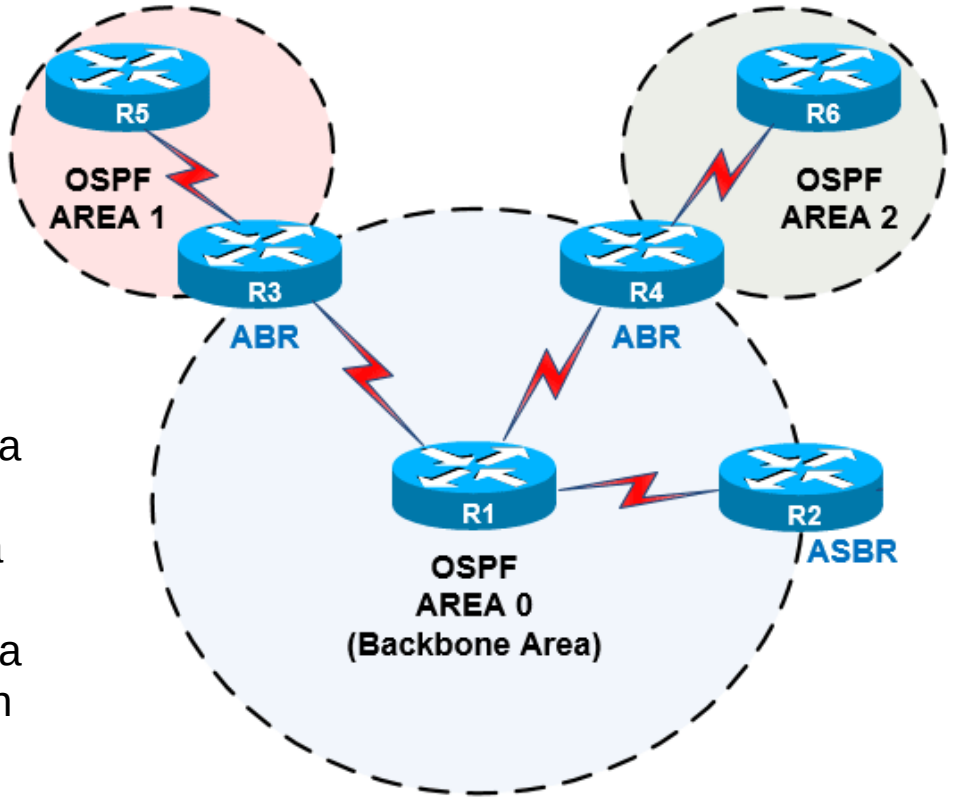
Scenario di riferimento	RTO	Strategia
Main Core Network down → guasto fisico	< 1 min	Infrastruttura di core network e link ai device di periferie ridondati + OSFP protocol

Architettura

Open Shortest Path First (OSFP):

- protocollo di routing di tipo ‘link state’
- rispetto al STP è più performante e utilizza gli IP e non MAC
- Gestisce il bilanciamento di carico (i pacchetti viaggiano su percorsi diretti verso la stessa destinazione pur avendo ‘costi’ differenti).

- Una rete OSP è divisa in aree, composte da gruppi non sovrapposti di router (le loro ‘informazioni’ sono raggruppate per singola area).
- Le stub area necessitano di relegare ad una route di default lo scambio per il traffico con quelle esterne al dominio di appartenenza.

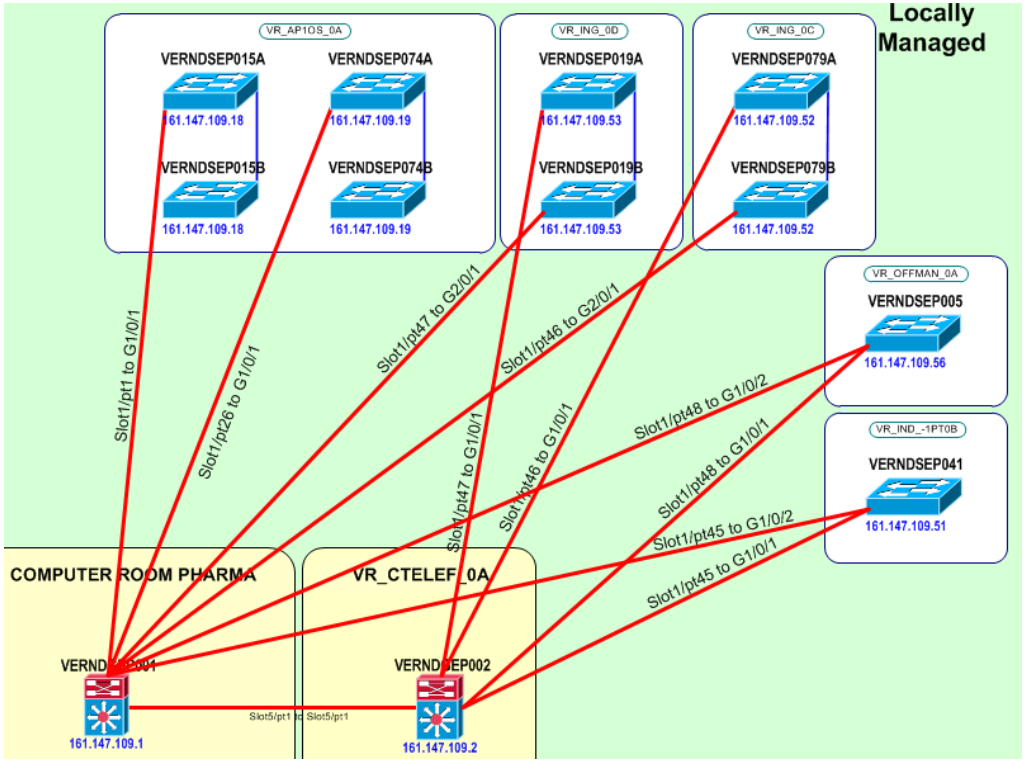


Implementazione Infrastruttura Attiva (2)

Network / Layer 3

Scenario di riferimento	RTO	Strategia
Main Core Network down → guasto fisico	< 1 min	Infrastruttura di core network e link ai device di periferie ridondati + OSFP protocol

Architettura



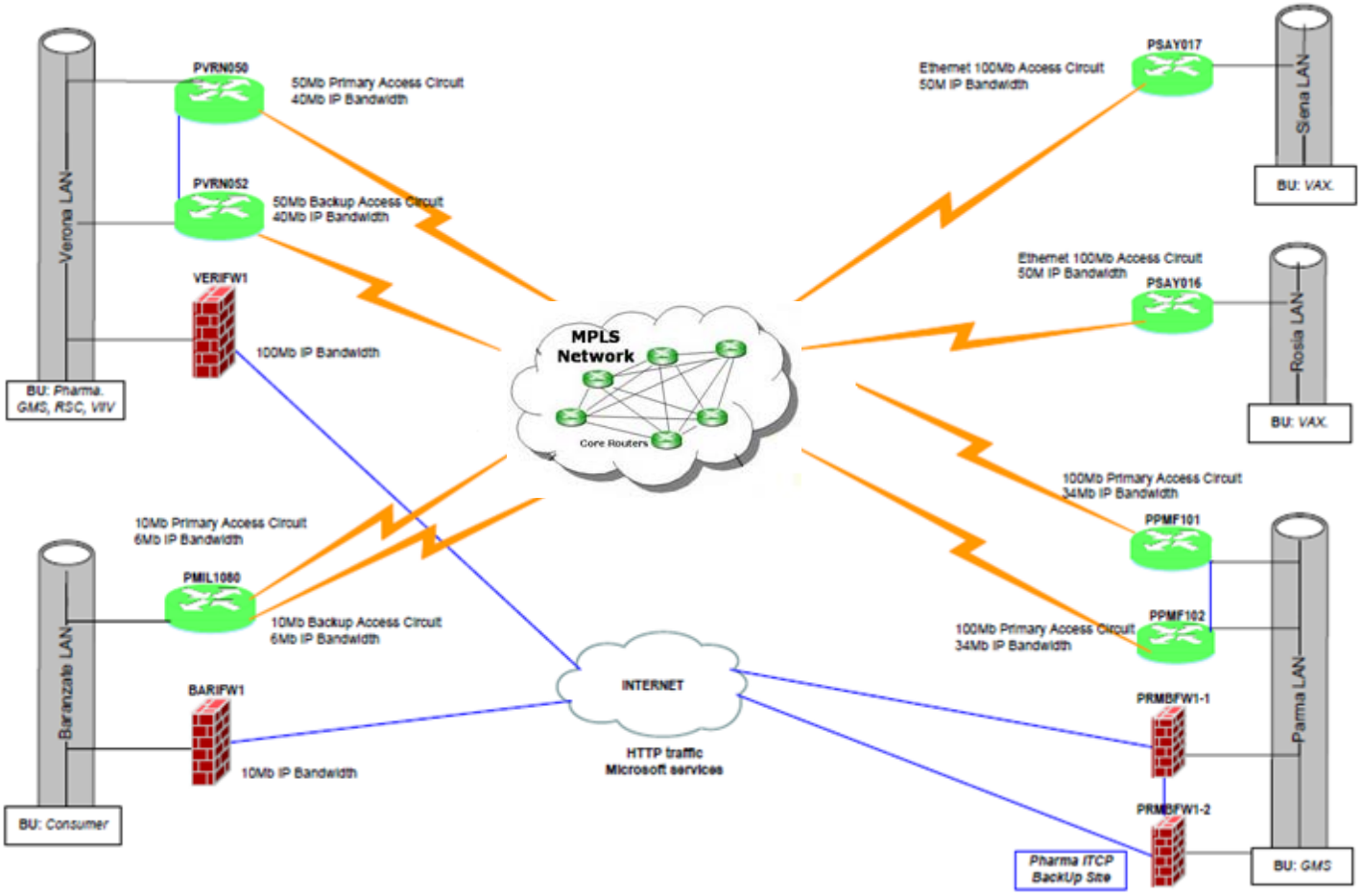

```
router ospf 1
 log-adjacency-changes
 area 14 authentication message-digest
 area 14 nssa
 summary-address 161.147.118.0 255.255.255.0
 redistribute connected metric 1 subnets
 network 161.147.109.64 0.0.0.0 area 14
 network 161.147.110.7 0.0.0.0 area 14
 network 161.147.113.3 0.0.0.0 area 14

interface GigabitEthernet1/0/1
 description to VERNDGEP001
 no switchport
 ip address 161.147.110.7 255.255.255.254
 ip ospf message-digest-key 1 md5 7 153A5B1857263E2A793065
 ip ospf network point-to-point

interface GigabitEthernet1/0/12
 description to VERNDGEP004
 no switchport
 ip address 161.147.113.3 255.255.255.254
 ip ospf message-digest-key 1 md5 7 123155034107190A7B2874
 ip ospf network point-to-point
```

Implementazione Infrastruttura Attiva (3)

Data Link / Layer 2

Scenario di riferimento	RTO	Strategia
Distruzione del 'WAN backbone' → incendio al provider, guasto fisico sulle vie-cavo interrate, fermi elettrici etc	< 5 min	Utilizzo percorsi «esterni» alternativi & BGP (Border Gateway Protocol)

Architettura



BGP (Border Gateway Protocol):

- è un protocollo di routing utilizzato per connettere tra loro più router che appartengono a sistemi/reti 'autonome';
- funziona attraverso la gestione di una tabella di reti IP (o *prefissi)*, che forniscono informazioni sulla raggiungibilità delle diverse reti

Service Model

Maintenance (1)

MANUTENZIONE:

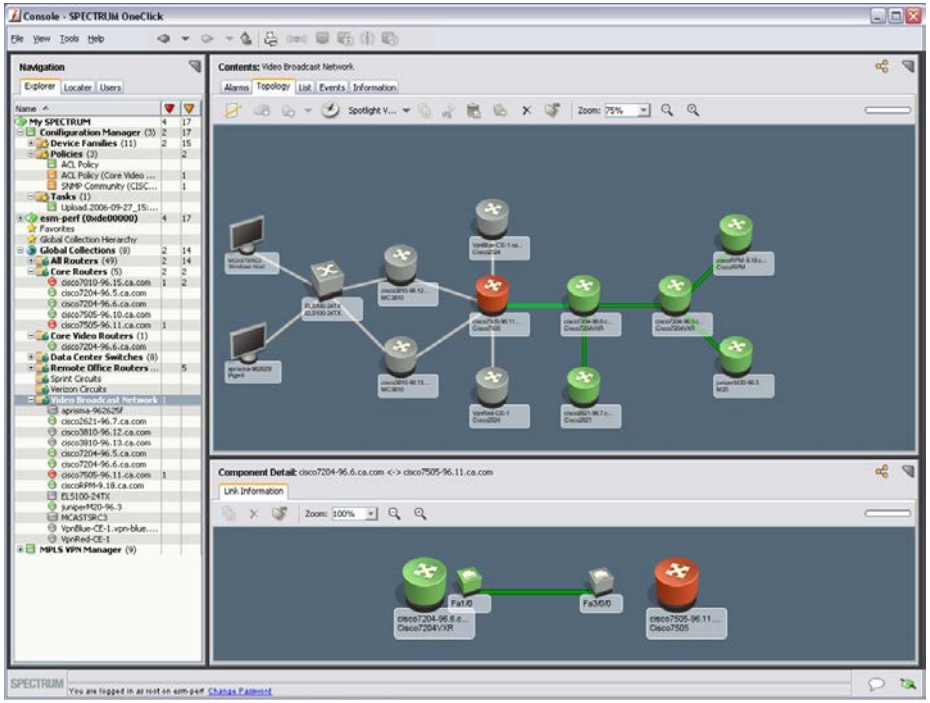
- *Preventiva* → eseguo un intervento di "sostituzione" o "riparazione" prima che si manifesti un guasto/disservizio.
- *Proattiva-Migliorativa* → Tech. Refresh
- *Incidentale* → eseguo un intervento (programmato o urgente) a seguito di un guasto

Service Model

Maintenance (2)

NETWORK MONITORING:

- Network topography → diagramma di rete (grafo). Ha lo scopo di monitorare lo stato dei link (up/down) e le variazioni nel tempo (data collection).
- Parametri qualitativi → response time, availability, uptime,…
- Event & triggering → Alerts & notification
- Backup → salvataggio automatico e periodico delle configurazioni
- Access management → accesso ‘centralizzato’ ai sistemi di rete
- Change management → apportare dei cambi di configurazione seguendo un opportuno processo di verifiche e autorizzazioni formali.



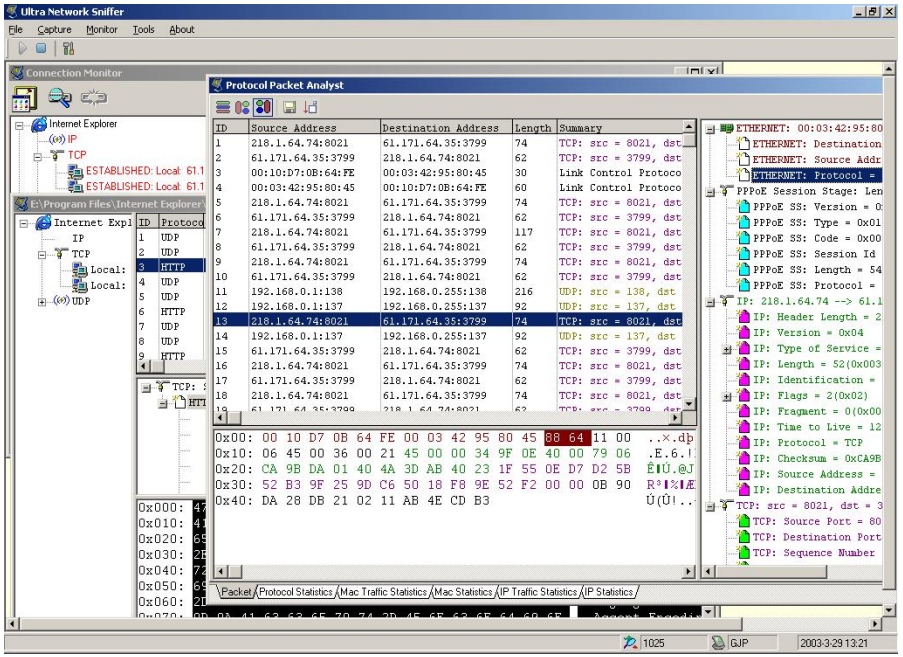
Spectrum

Service Model

Maintenance (3)

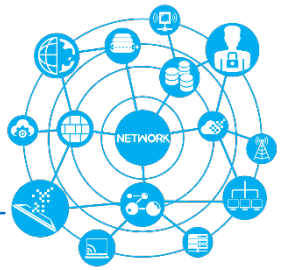
SNIFFER DI RETE (analizzatori di rete):

- Hanno lo scopo di analisi e individuazione di diversi problemi di rete (routing, performance, problemi di ritrasmissione, perdita di pacchetti, etc) ma anche di security (tentativi di intrusione).
- Sono elementi ‘passivi’ sulla rete → ascoltano e memorizzano i pacchetti.
- Se collegati a uno switch, devono essere sulla porta di ‘span’ o "port mirroring" in grado di riceve il traffico circolante su tutte le porte dello switch.
- Sono in grado di analizzare i vari livelli (data link, network, …application), ovvero possono scomporre e comprendere la struttura die diversi protocolli di rete.



Service Model

Incident Management



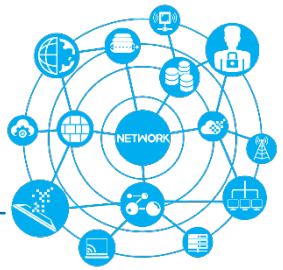
SISTEMA DI RACCOLTA E GESTIONE DEGLI INCIDENTI (TICKETING SW):

- Permette di raccogliere in modo strutturato gli incidenti (frame)
- Da feedback all'utente (per step, sino alla risoluzione)
- Gestione delle priorità
- Gestione degli impatti (ticket padre & figli)
- Strumento di Analisi su:
    - Guasti ripetitivi
    - Verifica dei Service Level Agreement (SLA) – tempi di analisi, intervento e risoluzione.

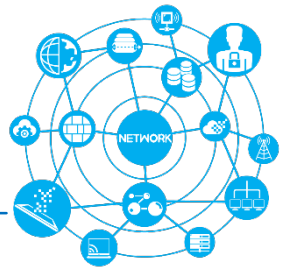
… l'espeienza dice:

- Spesso non è un problema di rete!
- Per il primo e veloce check utilizzate comandi semplici quale 'ping' e il 'tracert'

AGENDA



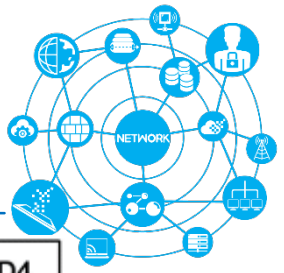
- Progettazione, implementazione e management della rete LAN/WAN con i requirements di Business Continuity e Disaster Recovery
  - Standard Framework
  - Concetti di Business Continuity e Disaster Recovery
  - Analisi dei bisogni (business requirements)
  - Principi di progettazione e implementazione
  - Service model: maintenance e incident management
- Applicazioni Client Server e distribuite
  - Definizioni e Terminologie
  - L’esperienza dei webinar
- Info-Protect
  - Gestione e Protezione delle Informazioni
  - Catalogazione delle Informazioni



Applicazioni Client Server e distribuite

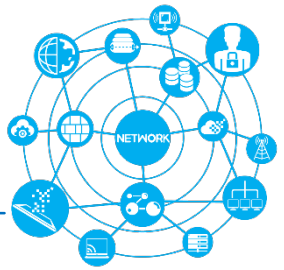
Applicazioni

Client/Server o distribuite



Layer	Application/Example		Central Device/ Protocols		DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP	GATEWAY	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT		
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names		
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP		Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP	Can be used on all layers	Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch Bridge WAP** PPP/SLIP	Land Based Layers	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**		

Definizioni e Terminologie (1)



Architettura CLIENT – SERVER:

- Accesso e utilizzo di un servizio ‘centralizzato’ (risiede su un ‘server’) mediante un software client ‘locale’.
- Sono spesso definiti dei SLA (Service Level Agreement) e un Service Model.

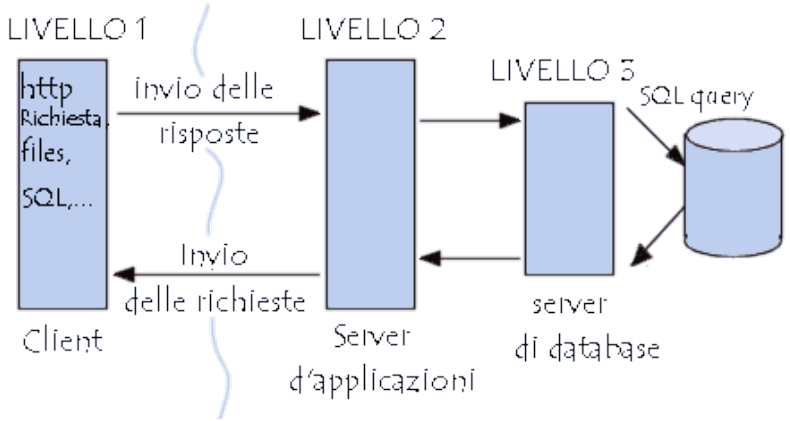
Server:

- Sempre disponibile
- Implementazione in ‘environment’ sicuro e protetto (Data Center)
- IP fisso

Client:

- On-Demand
- Interfaccia solo verso il Server (non comunica con gli altri client)
- IP dinamico

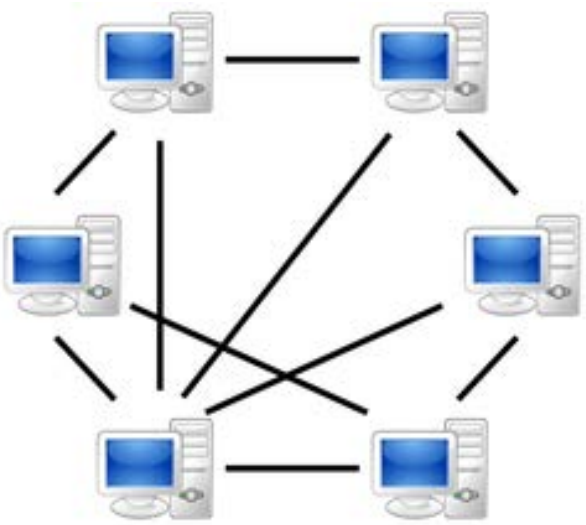
Software as a Service (SaaS)

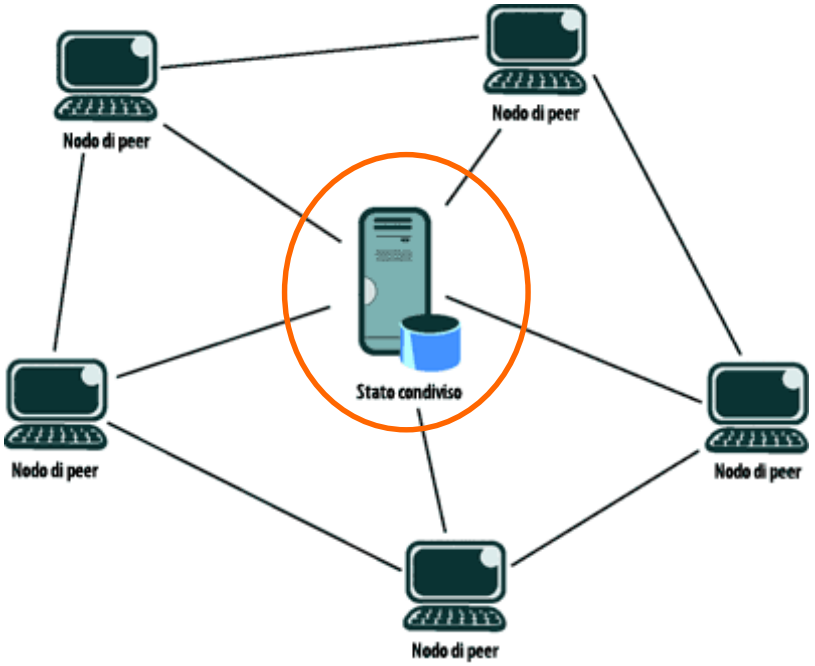


Definizioni e Terminologie (2)

Architettura PEER 2 PEER (P2P) :

- Coppie di client che – tramite un software comune/omogeneo – comunicano tra loro.
- Non sempre è presente un server (servizio centralizzato) se non nella fase di ricerca e instaurazione della comunicazione tra le due coppie di client.





Webinair

WEB + SEMINAR

collaborative conferencing through audio, video, and rich content sharing capabilities.

Webinar

- **Evento Live** (con o senza audience presente)
- **Disponibile solo nel momento dell'erogazione**
- **Partecipanti attivi on line (singoli o in gruppo)**
- **Interazione con i relatori**

Evento promozionale virtuale di GSK con interazione tra l'audience e il relatore, finalizzato a fornire informazione medica-scientifica ed education agli Operatori Sanitati.

Webcast

- **Evento registrato** (con o senza audience presente)
- **Partecipanti passivi (singoli o in gruppo)**
- **Nessuna Interazione**

Conferenza registrata disponibile on demand.

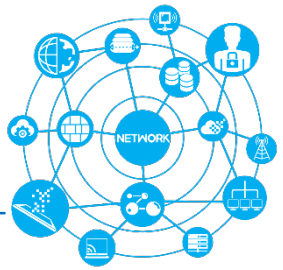
Webmeeting

- **Evento focalizzato sullo scambio e la discussione tra più persone**
- **Disponibile solo nel momento dell'erogazione**
- **Partecipanti attivi**
- **Interazione con i relatori**

Incontro di informazione medico-scientifica virtuale e strutturato, finalizzato a presentare agli Operatori Sanitari (Medici e Farmacisti) le caratteristiche bilanciate dei medicinali/vaccini di GSK.

Webinair

Framework



Target → Media Definition → Set-Up → Live Test → Live event

TARGET - “chi” invitare (attendees) , “come e dove” gestire il meeting, “quando” organizzarlo (planning), lo “scopo” e gli “argomenti” (agenda) del meeting.

MEDIA DEFINITION - E’ individuata la miglior in termini di hardware (PC/iPad), software (Live Meeting, WebEx, etc), audio (casse audio, amplificazione, microfono, etc) , video (uso il PC, proiettore, etc) e connettività (ADSL, 3/4G, etc).

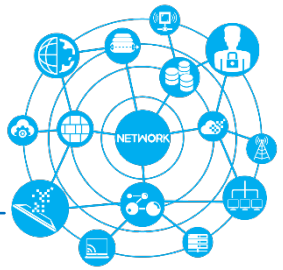
SET-UP - Sono resi disponibili (provide /installation) tutti gli elementi definiti precedentemente. Si deve tener presente che l’erogazione di alcuni servizi, come software e connettività, possono richiedere del tempo e costi aggiuntivi.

LIVE TEST - E’ una fase importante perché permette di individuare eventuali problemi o criticità e si ha la possibilità di identificarne una soluzione. Il Live test deve avvenire qualche giorno prima dell’evento e presso la location finale prevista nell’evento.

LIVE EVENT – Ricordarsi di collegarsi qualche minuto prima dell’inizio dell’evento dell’evento in modo tale da accertarsi che la parte audio/video funzioni perfettamente (eventualmente rifare il setup audio/video).
Al “presenter” (o meeting organizer) è richiesto di collegarsi e attivare la sessione almeno 20 minuti prima dell’orario previsto e fare l’upload sulla piattaforma di eventuali contenuti (prediligere la presentazione di slide rispetto allo screen sharing). Ricordarsi di mettere tutti in “mute” e di definire all’inizio del meeting le “regole del gioco” (come intervenire, come segnalare problemi, sessione Q&A, etc)

Webinair

Dotazioni



CONNETTIVITA'	• Rete GSK (uffici GSK) • ADSL • Connessione 3G o 4G (es: Vodafone MIFI) • Public wireless • Rete dati messa a disposizione dall'ente ospitante (ospedale, sede congressuale)
HARDWARE	• Laptop GSK • iPad GSK • PC messo a disposizione dell'ente ospitante
AUDIO (microfono e speaker)	• Integrato nell'Hardware • Kit vivavoce (es. clearone) • Casse esterne solo per audio • Diffusione audio messo a disposizione dell'ente ospitante (auditorium, sala congressi)
WEBCAM (acquisizione video)	• Webcam Integrata • Webcam esterna • Acquisizione video messa a disposizione dell'ente ospitante (auditorium, sala congressi)
PROIEZIONE	• Monitor PC/iPad • Proiettore esterno • Diffusione video messo a disposizione dell'ente ospitante (auditorium, sala congressi)
SOFTWARE	• Live Meeting (GSK) • WebEx (GSK) • Piattaforma Corporate (SABA) • Pacchetto chiavi in mano

Webinair

Esempio pratico – Medical Meeting

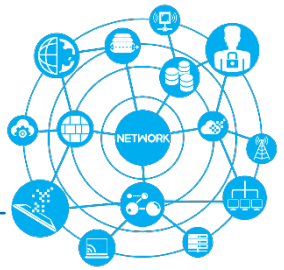
Urology Forum, Riardo - Congresso della Società Europea di Urologia, Madrid – marzo 2015

Webinair

Esempio pratico – GSK Auditorium

Webinair

Principali caratteristiche



- Peer-level (one2one, one2many, etc)
- Application:
  - Web Services (web browser app. based on Adobe Flash, Java, etc.)
  - Client download and installation (local app.)
- Real Time Services: Voice-over-IP (VoIP), Video-over-IP, Text-over-IP (ToIP)

Layer	Application/Example	
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management	
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**	
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.	
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting	

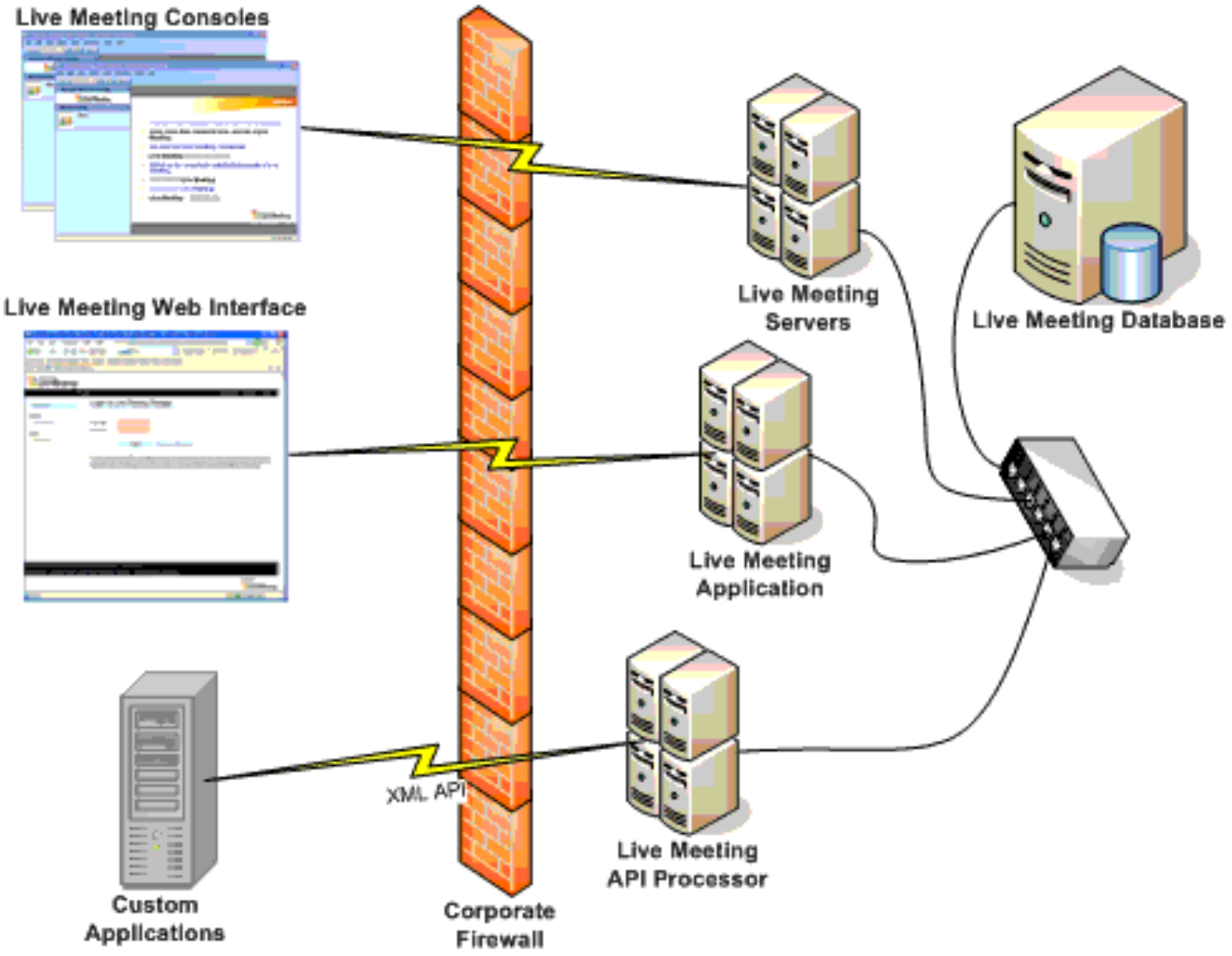
← **RTP** (Real-Time Transport Protocol)

← **UDP** (User Datagram Protocol) o TCP (Transmission Control Protocol)

← **IP**

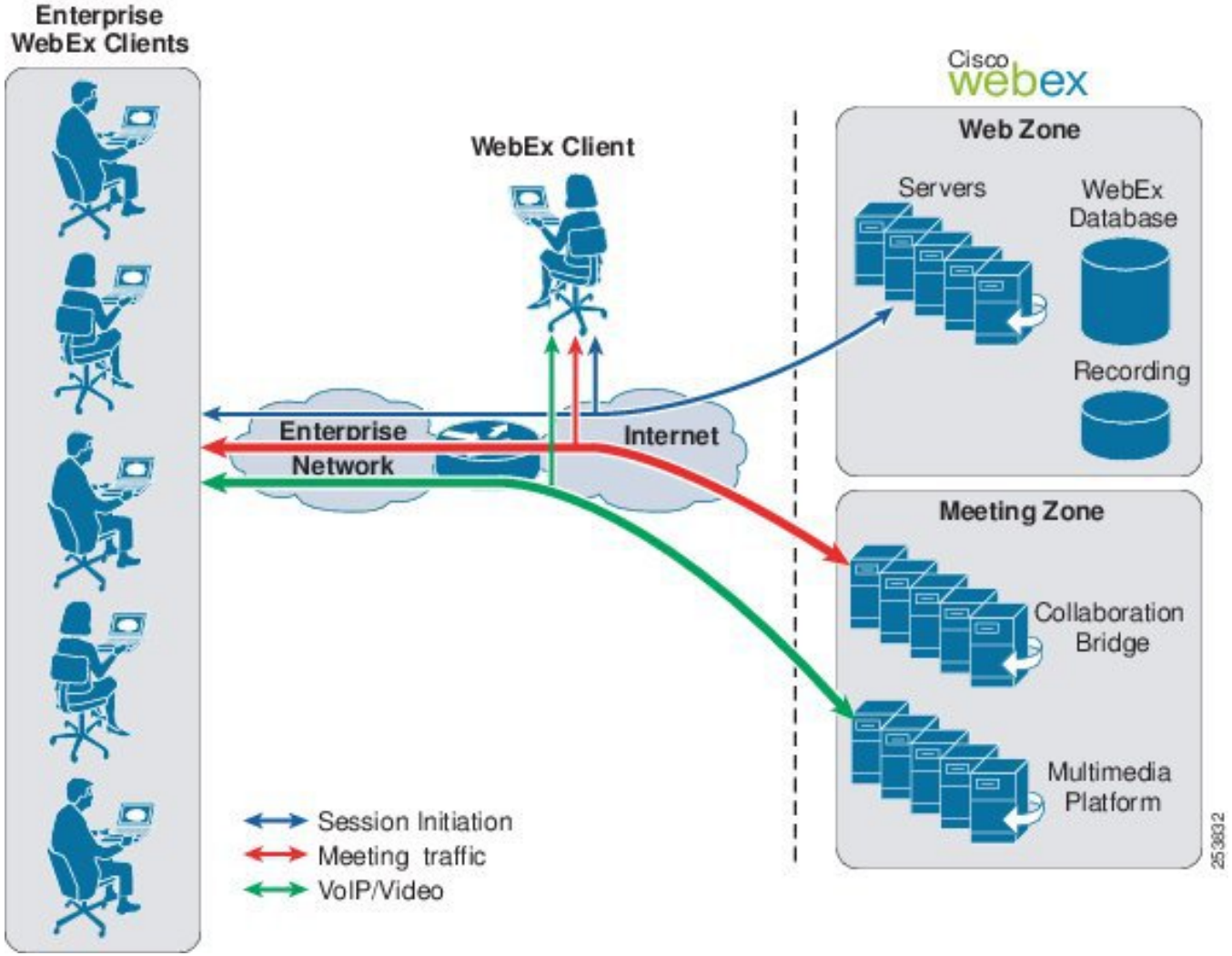
Webinair

MS Live meeting architecture



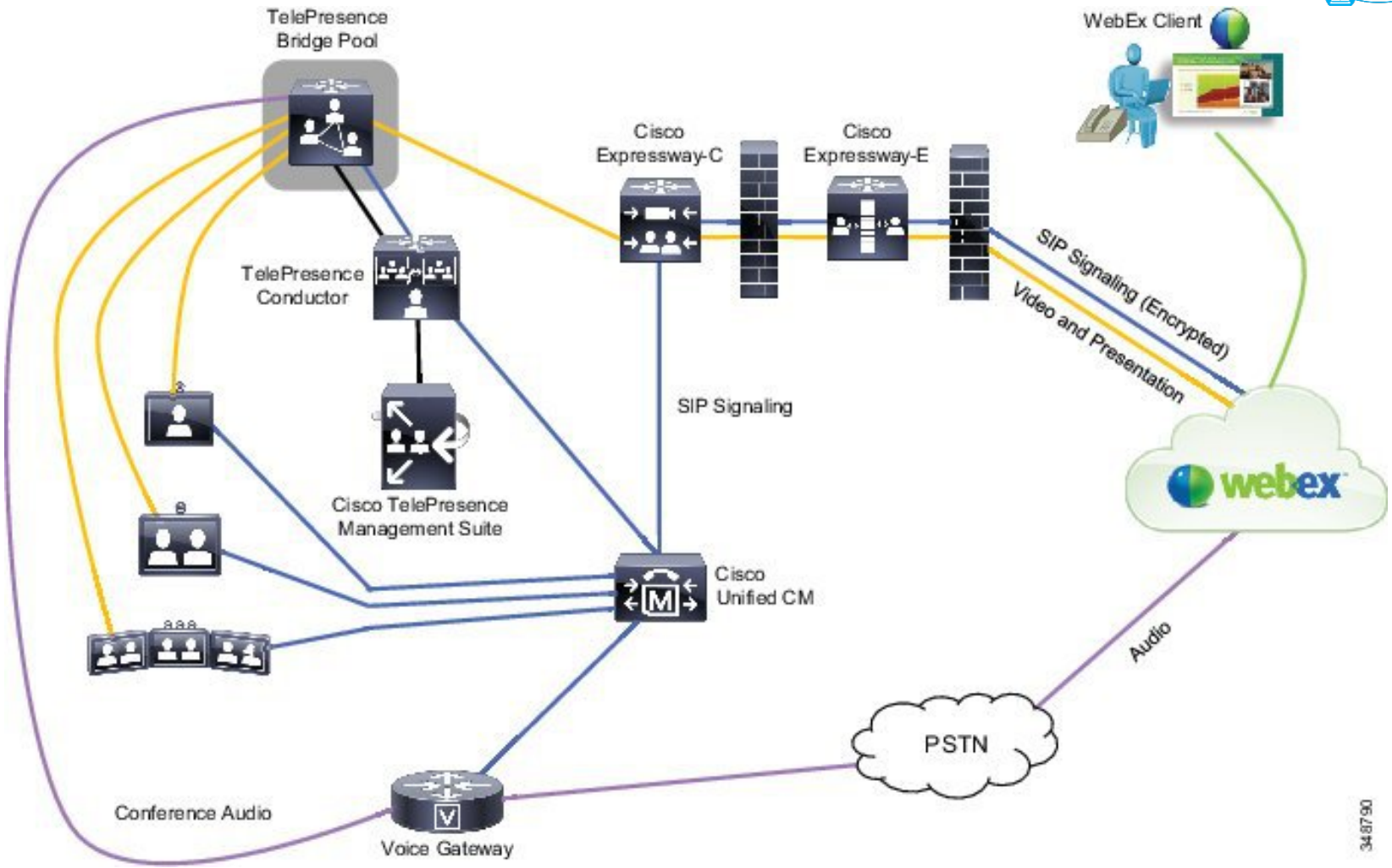
Webinair

CISCO WebEx architecture (1)

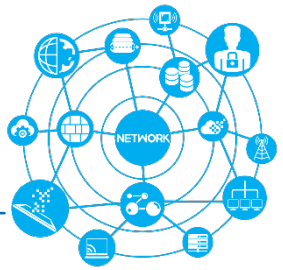


Webinair

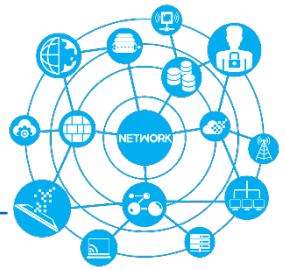
CISCO WebEx architecture (2)



AGENDA



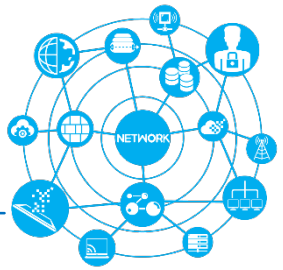
- Progettazione, implementazione e management della rete LAN/WAN con i requirements di Business Continuity e Disaster Recovery
  - Standard Framework
  - Concetti di Business Continuity e Disaster Recovery
  - Analisi dei bisogni (business requirements)
  - Principi di progettazione e implementazione
  - Service model: maintenance e incident management
- Applicazioni Client Server e distribuite
  - Definizioni e Terminologie
  - L’esperienza dei webinar
- Info-Protect
  - Gestione e Protezione delle Informazioni
  - Catalogazione delle Informazioni



Info-Protect

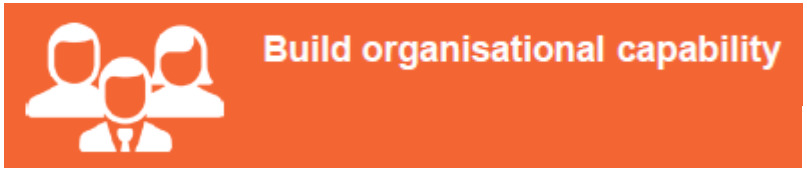
Gestione delle Informazioni (1)

Le informazioni, patrimonio dell'Azienda !!!



TRENDs:

- Increased collaboration with third parties
- Continued growth in the use of mobile devices
- Use of social media (Twitter, Instagram, Facebook, etc.)
- Consolidation of information into online storage (Cloud)



Failure to protect information has very serious consequences, including:

- Reputational damage
- Loss of intellectual property or missed commercial targets
- Legal complications in the form of potential litigation and fines or compensation for data breaches

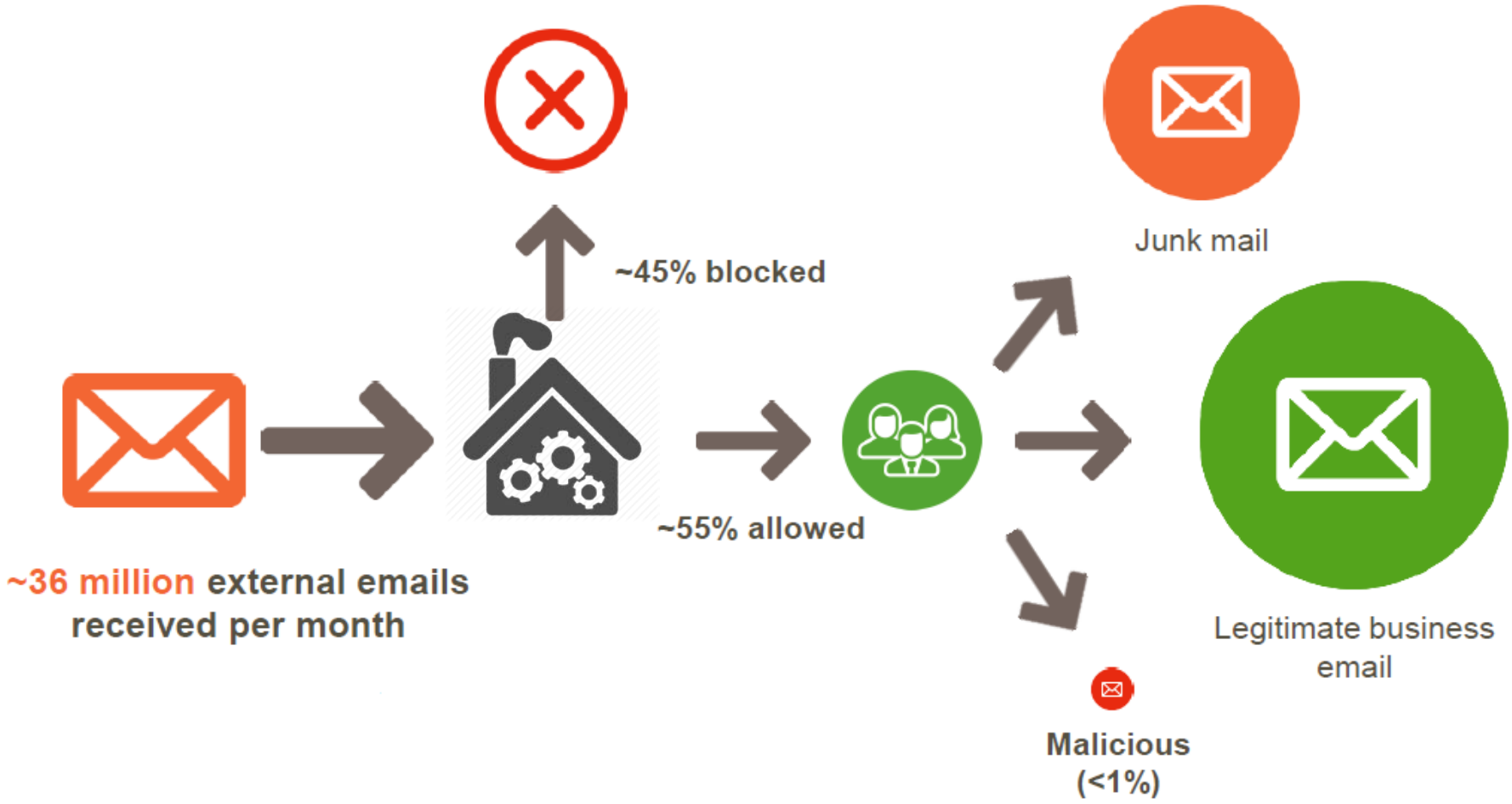
Gestione delle Informazioni (2)

Protect & Increase Security

- Error
- Malware
- Social
- Hacking
- Misuse
- Physical
- Environmental
- Privacy

Gestione delle Informazioni (3)

Esempio: *Email traffic and types of external email*



Catalogazione delle Informazioni

Catalogale per non sbagliare

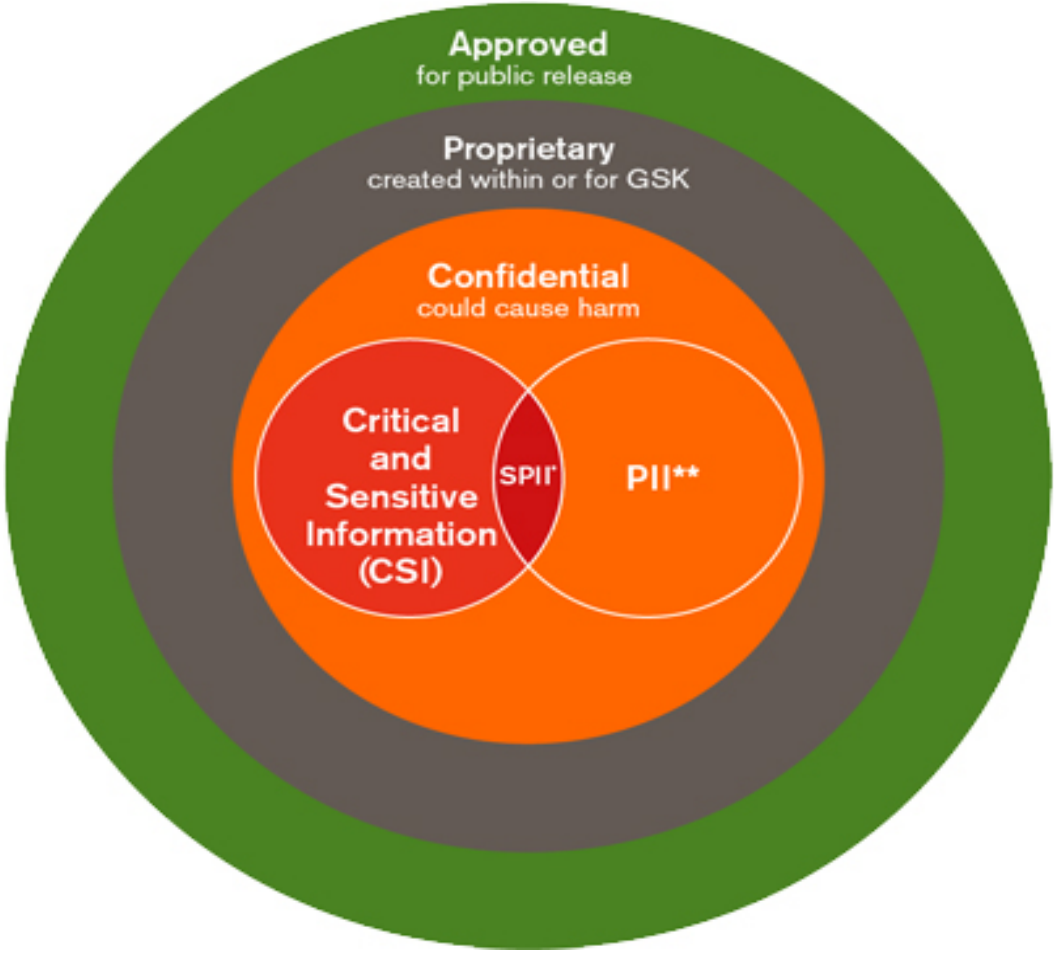
Approved: information that is already in the public domain or approved for release.

Proprietary: information generated within the company.

Confidential: proprietary information, which if disclosed, could damage the interests of the company.

PII: Personally Identifiable Information.

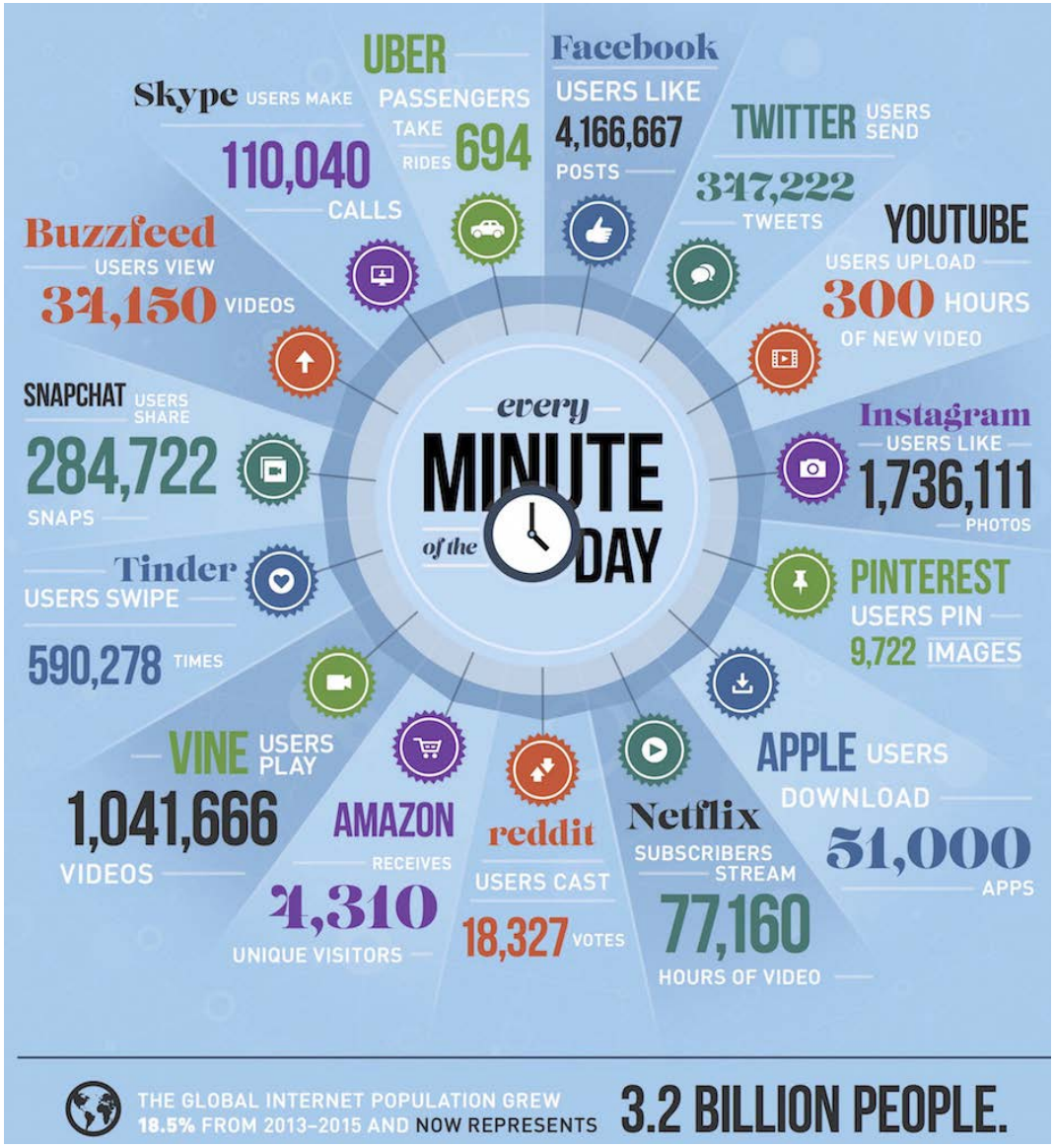
Critical and Sensitive Information (CSI): a subset of Confidential information, whose unauthorised disclosure, unavailability or loss of integrity could result in a significant impact to the company.




THANK
YOU
GRACIAS
ARIGATO
SHUKURIA
DANKSCHEEN
BIYAN
SHUKRIA
TINGKI
YAQHANYELAY
TASHAKKUR ATU
SUKSAMA
EKHMET
MAAKE
GRAZIE
MEHRBANI
PALDIES
KOMAPSUMIDA
GOZAIMASHITA
EFCHARISTO
JUSPAXAR
BOLZÏN
MERCI

BackUp Slide 1

Perché parlare di *Programmazione e Sicurezza delle reti* nella Grande Azienda?



Oggi il <u>focus</u> non - solo dell'utente home - ma di tutte le realtà economiche e industriali sono **Internet & Mobility**

- **Applicazioni di rete**
- **Cloud**
- **Social Media**

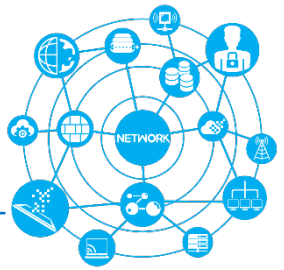
Office 365

SharePoint
Lync
Exchange

Google Apps

aruba.it
SOLUZIONI DATA CENTER

Cosa sta alla base della *Programmazione e Sicurezza delle reti ?*



Layer	Application/Example		Central Device/ Protocols		DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP	**GATEWAY** Can be used on all layers	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT		
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names		
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP		Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP		Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch Bridge WAP** PPP/SLIP	Land Based Layers	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**		

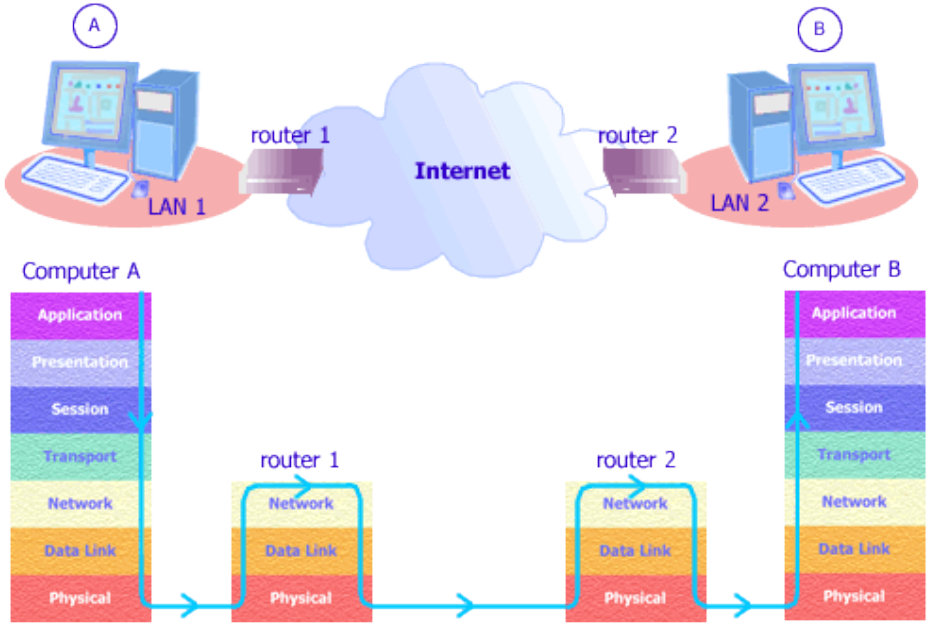
Modello ISO/OSI (Open System Interconnection)

STANDARD che <u>tuttora</u> riassume tutta la teoria sulle reti LAN e WAN

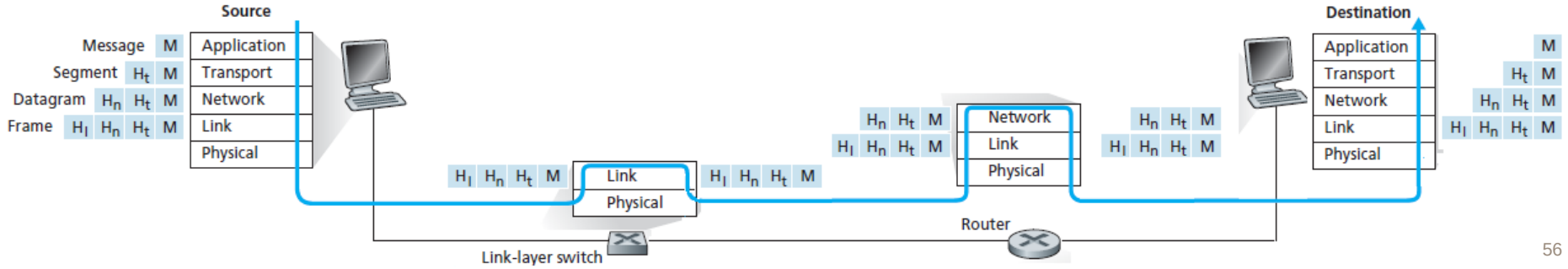
Modello ISO/OSI

Come funziona

Percorso fisico seguito dai dati



Il modello a livelli si basa sul concetto di *incapsulamento*



BackUp Slide 2

Business Continuity

Lifecycle

OUTPUT

E' la definizione di un **Business Continuity Plan** (BCP), "tasks/actions oriented".

Deve includere le seguenti informazioni:

- Campo di applicazione.
- Procedure di notifica e attivazione.
- Organizzazione di ripristino.
- Processi critici supportati.
- Scenari incidentali di riferimento.
- Strategie di ripristino.
- Check-list dei compiti di ripristino.
- Risorse critiche.
- Contatti critici.

Standard di riferimento:

ISO 22301 (2012) Business Continuity Management *(replace BS 25999-2)*