La virtualizzazione dell’infrastruttura di rete

La rete: la visione tradizionale

- La rete è un componente passivo del processo che trasporta i dati “meglio che può”
- L’attenzione è sulla disponibilità di banda e sull’affidabilità degli apparati
- La sicurezza di rete riguarda principalmente l’accesso da Internet
- La periferia è “terra di nessuno” almeno come apparati e gestione

Il primo colpo: la “minaccia” dei Wi-Fi

- Il Wi-Fi porta potenzialità e rischi, e costringe ad occuparsi della periferia, apparati compresi
- A questo si aggiunge il problema dei consulenti, presente da tempo ma senza vere soluzioni
  - Accedono alla rete con i propri sistemi e le proprie esigenze, e potenzialmente con virus

La convergenza e i nuovi servizi

- Le promesse di risparmio immediato sulle bollette sono uno dei motori principali per la diffusione della telefonia su IP
  - Ma le potenzialità di audio e video su IP sono ancora tutte da scoprire; il vero esempio è Skype
- Questi servizi chiedono alla rete non solo banda ma anche qualità del servizio
- Le aziende cominciano a desiderare un unico “canale” verso il carrier

MPLS e la virtualizzazione della connettività

- È una tecnologia che porta il concetto di switching in un contesto tradizionalmente regno del routing IP
- Permette di creare *circuiti virtuali* trasparenti al livello IP
- Finora utilizzata principalmente dai carrier e dalle grandi aziende

Multi Protocol Label Switching

- Al pacchetto IP viene aggiunto in testa un header MPLS contenente una label
- Il pacchetto viene poi instradato in base alla label, senza esaminare l'header IP (o SNA, o …)

Circuiti virtuali e MPLS

- Sull'infrastruttura di rete possono essere disegnati dei circuiti virtuali (label-switched path, LSP) in base ai quali sono definite delle tabelle di switching per i frame MPLS
  - Manualmente o mediante protocolli (LDP, RSVP)
  - Si ottiene quindi l'efficienza delle tecnologie di switching in fase di forwarding dei pacchetti (anziché applicare l'applicare l'algoritmo IP)
- Si applica il routing solo in ingresso (esteso con la possibilità di avere un lsp come destinazione) e in uscita dal backbone
  - È una tecnologia da carrier o da backbone

Altre possibilità dei circuiti MPLS

- Ridondanza con uno o più circuiti di backup
  - Convergenza veloce grazie a protocolli di segnalazione
  - Possibilità di load balancing con diverse politiche
    - Nota: i protocolli sono standard, ma come utilizzarli dipende dagli apparati
- Vantaggio rispetto ad ATM: le risorse sono prenotate ma non occupate
  - ma MPLS sfrutta comunque tecnologie best-effort
- Vantaggio rispetto a IP: le risorse prenotate sono disponibili quando necessario
  - Se il network engineering è fatto bene

MPLS e qualità del servizio

- È possibile “convertire” 3 bit del campo DSCP (ToS) di un pacchetto IP, o del campo 802.1p (QoS) di una frame Ethernet in bit del campo Exp della label MPLS, e viceversa
- Questo, insieme ad una buona gestione delle code hardware sulle interfacce di uscita da parte degli apparati, permette di gestire la qualità del servizio sul backbone
- È possibile anche differenziare i circuiti virtuali in base alla qualità di servizio desiderata soprattutto in termini di protezione

Integrazione con la gestione della periferia

- La tendenza è verso una periferia sempre più basata sullo switching anziché sul routing (Metroethernet per i carrier)
  - Protezione della connettività mediante protocolli “tipo spanning tree” per lo più proprietari con tempi di convergenza *carrier class* (<50 ms)
  - Utilizzo delle VLAN per la segregazione
- È possibile “convertire” i TAG VLAN in label MPLS
  - dato che comunque ci si muove verso un livello 2 Ethernet in tutti i contesti, in ambiente Metroethernet viene proposto il VLAN stacking (802.1ad) in alternativa a MPLS

Scenari di utilizzo

Protezione del traffico

- Grazie ai circuiti di backup ed a meccanismi per la gestione di path alternativi MPLS offre una resilienza molto alta “a costo zero”
  - i tradizionali meccanismi IP “scoprono” sul momento se ci sono cammini alternativi
  - La protezione riguarda l’intero circuito, comprese le cadute di nodo o di link
  - scalabilità elevata, anche se il traffic engineering deve essere curato (spesso i circuiti sono disegnati “a tavolino”)

Qualità del servizio

- È possibile gestire il Class of Service (le reti IP sono comunque best effort) end-to-end
  - essenziale per applicazioni audio/video, ma può essere utilizzato comunque per garantire la qualità e **disponibilità** di banda necessaria a diversi processi

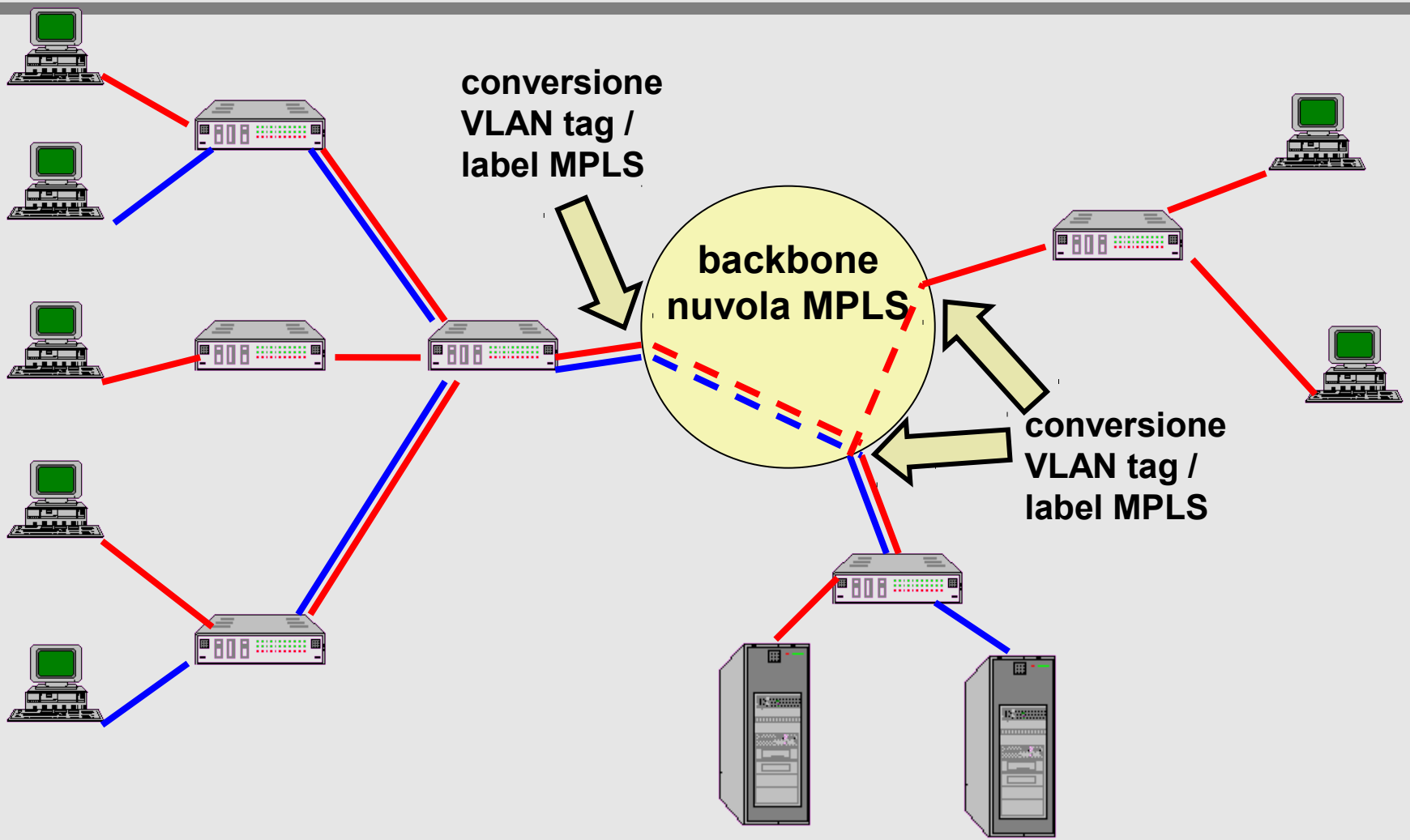
Gestione degli utenti per comunità

- È sempre più difficile distinguere gli utenti in base a indirizzi IP e sottoreti
- È possibile:
  - associare porte di apparati a VLAN
  - associare label MPLS a TAG VLAN
- In questo modo porte diverse di uno stesso switch possono trovarsi su due reti virtuali distinte
  - la distinzione si mantiene sul backbone

Segregazione fra comunità

- Le comunità comunicano in punti definiti
  - dove si consente il traffico fra VLAN o LSP
- Maggiore segregazione fra comunità
  - controllo delle anomalie e delle “infezioni”
  - alleggerimento dei sistemi di monitoraggio e di sicurezza
  - flessibilità nella gestione di comunità in continua evoluzione
- Attenzione! I protocolli p2p (es VoIP) richiedono comunque il traffico fra comunità

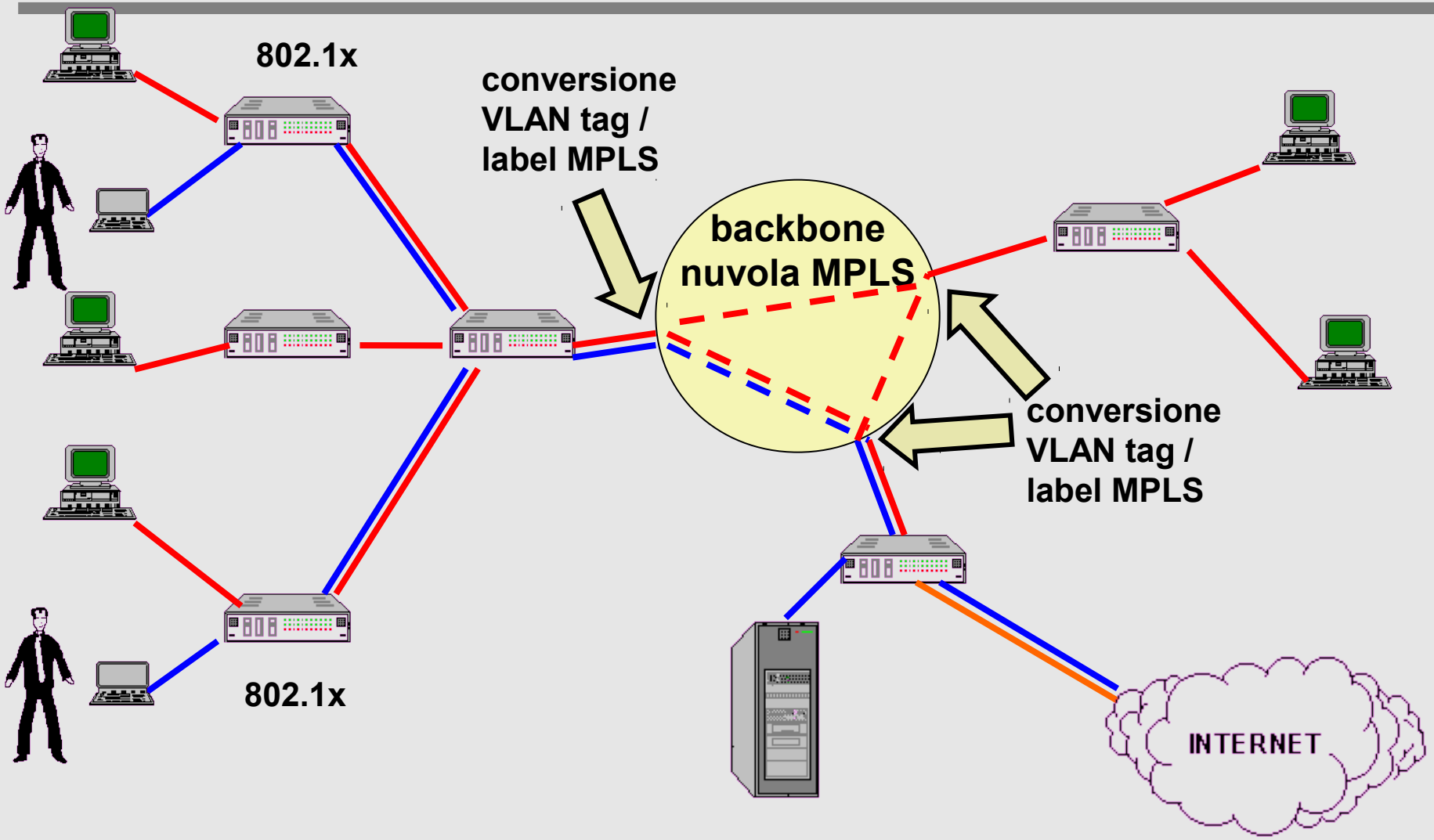
Gestione per comunità



Integrazione con l'Identity Management

- Un uso evoluto di 802.1x permette (permetterà) di associare il meccanismo a utenti anziché a porte
- Auspicabile una buona integrazione con i meccanismi di Identity Management
  - ma i "dettagli implementativi" sono ancora tutt'altro che risolti

Esempio: gestione consulenti



Servizi di remotizzazione

- Permette di condividere fra più servizi un pvc ATM o una frequenza acquistata da un carrier senza rischiare di compromettere il servizio, per attività come:
  - backup centralizzato
  - ridondanza dei siti
  - sistemi di storage centralizzati
- L'uso di due LSP (Layer 3 VPN) presi da due carrier diversi può essere più affidabile (e forse conveniente) di una frequenza da un solo carrier

Integrazione della rete nei processi

- La tecnologia è vantaggiosa per la protezione del traffico e la possibilità di usare VoIP
- Tuttavia, per sfruttarla appieno, è necessario integrare la rete nei processi aziendali:
  - chi disegna i processi deve sapere quali potenzialità offre l'infrastruttura (es. caso di cessione di un ramo di attività)
  - i processi devono poter chiedere alla rete livelli di servizio adeguati

Cosa manca?

- Al momento, la gestione del CoS è fatta essenzialmente in base alle caratteristiche riconoscibili a livello rete (es. indirizzi IP diversi per telefoni IP)
- Serve integrare nelle applicazioni i meccanismi per il CoS
- L'offerta di VPN Layer 3 dei carrier non prevede per ora la gestione di CoS
  - overprovisioning
- La parte 802.1x è in rapida evoluzione

Il passo successivo: VPLS

- Virtual Private LAN Services o anche Transparent LAN Services
- Permettono di virtualizzare un Broadcast Domain Ethernet per mezzo di *pseudo-wire*
- La loro particolarità è la creazione di circuiti punto-multipunto, che permettono di virtualizzare i servizi LAN

I rischi associati

Rischi rispetto a cosa?

- Se la situazione media aziendale è che la rete è incontrollata non sembra che come rischi si possa aggiungere molto…
- Ma se cominciamo a fare affidamento sulla disponibilità della risorsa rete, allora dobbiamo assicurarci che i livelli di servizio siano garantiti

Criticità: la saturazione

- Bisogna verificare che i sistemi non possano saturare in modo illegittimo la rete di traffico ad alta priorità
- Allo stesso modo, dobbiamo verificare che i sistemi di una VLAN non impediscano il traffico di un'altra VLAN
  - questi problemi sono critici solo in periferia, perché i meccanismi disponibili permettono di gestire correttamente il problema sui nodi centrali;
  - in periferia apparati economici od obsoleti possono non essere all'altezza (migrazione per passi)

Criticità: gli apparati

- Gli apparati coinvolti divengono componenti importanti dell'offerta di servizio;
  - devono quindi essere configurati e gestiti in modo sicuro anche in periferia
  - non aggiunge niente rispetto alle esigenze di controllo date dal Wi-Fi e da 802.1x
  - gli apparati che gestiscono traffico MPLS sono "visibili" a livello IP solo per la gestione

Criticità: gli apparati del carrier

- Se ci si affida ad un carrier, dobbiamo considerare che i suoi apparati saranno utilizzati anche per altro traffico (di altri clienti, Internet…)
- Potenzialmente questi apparati possono essere:
  - soggetti a errori di configurazione che rendano accessibile a terzi il traffico
  - soggetti ad attacchi, ad es. di DoS, anche da Internet
  - difficile ipotizzare di poter auditare il carrier
  - uno SLA ci “protegge” almeno per quanto riguarda i DoS

Criticità: i protocolli di segnalazione

- Gli LSP vengono realizzati e gestiti grazie a protocolli di segnalazione (RSVP-TE)
- Eventuali attacchi a questi protocolli possono bloccare/manipolare gli LSP
- C’è ancora poca letteratura
  - idealmente dovrebbero essere protetti dal traffico interno agli lsp

Criticità: la propagazione degli attacchi LAN based all'intera rete

- Rendere trasparente l'infrastruttura può voler dire permettere agli attacchi LAN di propagarsi sull'intera rete (es. MAC spoofing?)
- Attacchi tipici dei contesti switchati potrebbero essere efficaci sugli apparati (es. CAM flooding)
  - le configurazioni non sono comunque attaccate a questo livello
  - se gli apparati gestiscono bene VLAN e MPLS, gli effetti sono confinati
  - può esserci un impatto sulle prestazioni e quindi sulla disponibilità, anche in funzione dell'implementazione
- C'è ancora poca letteratura

Criticità: la compatibilità

- Si tratta di un settore in rapida evoluzione
- Molti protocolli non sono ancora standard
  - draft dell'IETF (es. per VPLS, un draft indica LDP per la segnalazione, un altro BGP)
  - protocolli proprietari (es. evoluzioni di Rapid Spanning Tree Protocol)
- La compatibilità fra apparati sulle funzionalità di base di solito c'è
  - ma le funzionalità non standard spesso servono

Supporto alla sicurezza di rete

- I meccanismi di virtualizzazione aiutano a separare contesti diversi, a segregare il traffico e a definire i punti in cui i diversi contesti scambiano traffico
- Questo semplifica il lavoro sia agli strumenti di filtraggio (firewall) sia a quelli di rilevamento (es. IDS)

Gestione e monitoraggio

- È importante il monitoraggio del traffico alla ricerca di anomalie che possono indicare:
  - il rischio di perdita di disponibilità
  - errori di configurazione
  - variazioni nel traffico legittimo
  - attacchi
- La rete deve segnalare in modo efficace eventuali guasti
  - i meccanismi riescono a rendere trasparenti i guasti… anche troppo
  - servono strumenti che permettano di gestire la diagnostica allo stesso livello della virtualizzazione

Gestione delle configurazioni

- I meccanismi di provisioning sono particolarmente importanti
  - devono essere protetti (ssh?)
  - devono permettere di “disegnare” in modo efficace le comunità sull’infrastruttura di rete
  - uniformità: non solo problemi “multivendor” ma anche per un singolo vendor, specialmente in seguito ad acquisizioni
    - tendenza per i carrier: strumenti fatti in casa basati su XML
    - difficile per ora utilizzare strumenti “generici”

Conclusioni

- I meccanismi di virtualizzazione delle reti offrono molte opportunità ed alcuni nuovi rischi
- In questo contesto, gli aspetti di offerta di servizio, gestione e sicurezza non sono separabili
- La sicurezza non è un costo aggiuntivo, perché è semplicemente parte di una gestione efficiente ed efficace